Lectura 2: Divisibilidad

2.1. Conceptos básicos

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. Esta aproximación de listar absolutamente todos los resultados será abandonada de a poco e intercambiada por argumentos intuitivos. Sin embargo, cada argumento intuitivo debe ser respaldado por un argumento adecuado y a pesar que se dejarán de proveer muchos de ellos, se invita a intentar probar esos resultados que no le parezcan inmediatos. Con esto en mente, comencemos a plantear algunos resultados básicos de un área de la matemática conocida como «Teoría de Números».

Definición 2.1. 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 «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

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

de esta forma podemos 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

[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 los llamados racionales, el número $12/3 = 4$ mientras que $7/3$ resulta un número que no es entero que podríamos denominar *puramente racional*. Explicaremos esto futuras lecturas.

operación inversa, podría ser problemático. Es por eso, que se invita a desvincularlos y darse cuenta que el concepto de divisibilidad es en realidad un predicado no una operación entre números enteros.

De forma similar, podemos preguntarnos en que casos a divide a 1. Esto se traduce en la existencia de 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 2.2. 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 en* $\mathbb{Z}$.

No es difícil notar que, si un entero posee un inverso multiplicativo, entonces este es único (ejercicio 2.4). Sin embargo, los números que poseen inversos multiplicativos, o en nuestra terminología, las unidades, no presentan diversidad en $\mathbb{Z}$.

Lema 2.1. *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. Supongamos que, en efecto, existe un entero q que satisface $aq = 1$. Comencemos notando es imposible tener $a = 0$. En efecto, si éste fuera el caso sabemos que para todo entero q, se tendría que $aq = 0$, de esta forma debemos concluir que $a \neq 0$. 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 $q = 1$, $a = aq = 1$ lo cual contradice nuestra suposición. En resumen $a > 1$ y $q > 1$ por lo que $aq > 1$ lo cual es imposible pues por hipótesis $aq = 1$, lo que nos obliga concluir que $a \leq 1$. Con un argumento similar podemos descartar $a < -1$, obteniendo así $-1 \leq a \leq 1$. 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 2.2. *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 2.3. *Para cualesquiera enteros a y b*

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

Demostración. Notemos primero que $a1 = a$, 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 $a \neq 0$, debemos tener 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. No debe ser difícil notar que si limitamos la relación a $\mathbb{N}$, la relación resulta, en efecto, una *relación de orden en* $\mathbb{N}$.

Teorema 2.4. *Sean a y b enteros cualquiera y sean u y v unidades de $\mathbb{Z}$. Entonces, a es divisor de b si y sólo si $u \cdot a$ es divisor de $v \cdot b$.*

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 $\mathbb{Z}$.

2.2. Divisibilidad en la estructura de $\mathbb{Z}$

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 $-8 < -2$. En este punto esto no debe parecer algo extraño, basta considerar sólo las propiedades del orden. Exploraremos ahora el caso general.

Definición 2.3. 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 2.4 evitando la terminología de unidades.

Lema 2.5. *Para enteros cualquiera a y b, $a|b$ si y sólo si $|a| \mid |b|$.*

Este lema, expresa una forma para evitar cualquier referencia a los signos en $\mathbb{Z}$. Esto quiere decir que la divisibilidad es un concepto intrínseco a los números, posteriormente veremos como capturar los elementos esenciales de la divisibilidad. De cualquier forma, tenemos ahora los materiales necesarios para explorar el caso general que buscábamos.

Teorema 2.6. *Para números a y b, ambos distintos de 0, si $a|b$, entonces $|a| \leq |b|$.*

Demostración. Considerando el lema 2.5 podemos afirmar que $|a| \mid |b|$ o, siguiendo su definición, existe un entero q de forma que

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

Proveeremos un argumento que clasifique a q con lo que derivará el resultado buscado. 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 lo siguiente

$$|a| \leq q|a| = |b|,$$

la cual resulta la desigualdad que buscamos. ■

El teorema anterior establece la relación que guardan las relaciones de divisibilidad y la de orden en los enteros. Se requiere por supuesto, un concepto intermedio, el de valor absoluto, y aunque sus propiedades nunca se exploraron, el lector debe estar ya familiarizado con éste.

Exploremos ahora la relación que guarda 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 notando que el $i+1$-ésimo elemento de la lista, a_{i+1}, se puede expresar

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

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 la suma de una cantidad fija de 3, 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 2.7. *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. ■

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 las condiciones requeridas resultan más débiles. La prueba, sin embargo, es tan sencilla que ya hemos hecho uso del resultado en algunas pruebas. Es indispensable, sin embargo, explorarla, ésta se deja como ejercicio (2.9).

Teorema 2.8. *Sean a, b y d enteros cualquiera. Si $d \mid a$, entonces $d \mid ab$.*

Podemos desprender de inmediato un corolario de los teoremas 2.7 y 2.8 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 2.9. *Sean a, b y d enteros cualquiera. Si $d \mid a$ y $d \mid b$, entonces $d \mid sa + tb$, para cualesquiera enteros s y t.*

Podemos explorar 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 2.4. 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 2.10. *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 2.9 podemos concluir que si d divide a ambos, a y b, d debe dividir a cualquier combinación lineal de estos, lo que garantiza la suficiencia. Basta entonces probar la necesidad.

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. Esto prueba la necesidad. ■

Volvemos ahora a nuestra pregunta del párrafo anterior. Dados dos números, se puede expresar cualquier otro como la combinación lineal de esos dos. El teorema responde que 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 2.11. *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 2.10 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. ■

2.3. Teorema de la división

Esta sección pretende proveer los pormenores de un resultado con el nos hemos enfrentado en muchas ocasiones durante nuestra educación: 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 obejetivo dar una respuesta parcial.

Lema 2.12. *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 $b \geq 1$, y para cualquier $n > a$ se tiene

$$nb \geq n > a$$

y en consecuencia $n \notin Q$. En otras palabras, si $n \in Q$, entonces $n \leq a$. Esto prueba nuestra afirmación.

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 $q = \text{máx}\, Q$ 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 $r - b \geq 0$ y

$$r - b = a - qb - b = a - (q + 1)b$$

y debemos debemos concluir que

$$a - (q + 1)b \geq 0,$$

lo cual implica que $q + 1 \in Q$. Siendo que q el máximo del conjunto Q, lo anterior es por supuesto una contradicción y en consecuencia $r < b$ como afirmamos. ■

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 2.13 (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 2.5. 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 2.12 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

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

y vernos tentados concluir que el residuo de dividir -9 entre -2 es -1, pero como indica el teorema, el residuo debe ser no negativo. En realidad es fácil resolver esto:

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

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 positivos.

Consideremos ahora que sucede cuando $a = -12$ y $b = 7$. 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 en consecuencia

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

lo que exhibe el cociente y el residuo de la división que buscamos.

Estos dos ejemplos deben de dar una idea que los casos negativos se pueden resolver usando el valor absoluto y el lema 2.12. Esto se probará en el ejercicio 2.13.

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 2.11 y 2.12 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 (basta escribir el significado de todos los términos, ¡hazlo!).

Proposición 2.14. *Para cualesquiera números, a es múltiplo de b si y sólo si el residuo que resulta de dividir a entre b es 0.*

2.4. 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 2.6. 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, 1. Además, si d es un divisor común de estos números, debe satisfacer $|d| \leq |a|$ y $|d| \leq |b|$ (teorema 2.6), o en otras palabras

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

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

Es quizá importante notar que los enteros involucrados bien pueden ser 0, en cuyo caso el único divisor común que poseen es precisamente 0 por lo que

$$(a, 0) = (0, a) = 0.$$

Por otro lado, como muestra el ejercicio 2.14, es de poca importancia estudiar un caso general en los enteros y en muchas ocasiones bastará explorar únicamente los casos $a > 0$ y $b > 0$.

Teorema 2.15 (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*

$$(a, b) = as + bt.$$

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.,

$$I = \{ax + by \mid x, y \in \mathbb{Z}\}.$$

Debemos notar que $-a, a \in I$ lo que nos lleva a concluir que I contiene al menos un elemento positivo. Tomamos entonces $P \subset I$ como el conjunto de enteros positivos que pertenecen a I, el cual sabemos es no vacío y por el principio de buen orden tiene un 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. Usaremos el hecho que, al d un elemento de I, deben existir enteros s y t de forma que

$$d = as + bt.$$

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

$$a = qd + r.$$

Vamos a descartar la posibilidad que $r > 0$ usando contradicción. 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 entra en contradicción con definir d como el mínimo del conjunto P. Debemos entonces concluir que $r = 0$ o en otras palabras que $d \mid a$. Un argumento análogo sirve para concluir que $d \mid b$ y en consecuencia d es un divisor común de a y b.

Finalmente, si c es cualquier otro divisor común de a y b, de acuerdo al corolario 2.9, c divide a cualquier combinación lineal y en consecuencia $c \mid d$, esto a su vez implica que $c \leq |c| \leq d$. Debemos entonces concluir que, en efecto, d es el máximo común divisor. ■

Corolario 2.16. *Un entero no negativo d que sea divisor común de a y b es el máximo común divisor si y sólo si para cualquier divisor común de a y b, se tiene c | e.*

Demostración. La prueba de la necesidad está contenida en el último párrafo de la prueba del teorema pues si fuera $(a, b) = sa + tb$ como se describe ahí, cualquier divisor común de a y b dividiría a (a, b) al ser éste una combinación lineal de los números involucrados.

Ahora, 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 $(a, b) \mid e$ lo que nos lleva a concluir que $(a, b) = |(a, b)| \leq e$. Por otro lado, $e \leq (a, b)$ por la definición de máximo común divisor y en consecuencia $e = (a, b)$ como buscamos. ■

El corolario anterior no otorga una nueva caracterización del máximo común divisor que elimina cualquier mención al orden. Habrá que tener cuidado, 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. En realidad, el corolario tiene una consecuencia que pasa muchas veces desapercibida: El máximo común divisor no puede ser negativo.

En la siguiente sección exploraremos un método para calcular el cociente y el residuo al efectuar la división y el mismo método nos permitirá dar solución a la identidad de Bézout.

2.5. Algorimo de Euclides

Una forma de encontrar el máximo común divisor de dos números es listar todos los divisores de ambos. Por ejemplo, consideremos los números 20 y 15, por un lado los divisores de 10 resultan ser 1, 2, 4, 5, 10 y 20, mientras los de 15 son 1, 3, 4, 5 y 15. En ese caso los divisores comunes resultan 1, 4 y 5 de los cuales el máximo es 5. En ese caso $(20, 15) = 5$. Parece no ser difícil encontrar el máximo común divisor a través de este método, sin embargo si consideramos números mucho más grandes, la tarea se vuelve mucho más tediosa. Por inocente que parezca discutir acerca de cuan complejo resulta este último algoritmo resulta algo más profundo. De manera histórica, estos resultados detonaron una fructífera área en matemáticas que en el siglo pasado sufrió un crecimiento exponencial con el surgimiento de las ciencias de la computación. Discutiremos uno de estos algoritmos, sin embargo será una discusión muy superficial. El algoritmo en cuestión es una modificación de otro propuesto por Euclides, el cual nos permite realizar el cálculo del máximo común divisor de dos números.

Definiremos ahora una sucesión de enteros no negativos, pensando ésta como una función[2] de $\mathbb{N}$ en $\mathbb{Z}$. Procedemos entonces: Para dos números cualquiera a y $b \neq 0$, definimos q_1 y r_1 como el cociente y el residuo de dividir a entre b, i.e.,

$$a = q_1 b + r_1$$

con $0 \leq r_1 < b$. Si $r_1 \neq 0$, entonces podemos ahora aplicar el teorema de la división sobre b y r_1 obteniendo así q_2 y r_2 como el cociente y el residuo de la división de b entre r_1, i.e.,

$$b = q_2 r_1 + r_2.$$

De nueva cuenta si $r_2 \neq 0$ podemos volver a efectuar el mismo proceso y continuar repitiéndolo si es posible. Si en algún punto, alguno de los residuos $r_k = 0$, la sucesión dejará de estar definida

[2] Ésta es una de la instancias en la cual es conveniente definir funciones parciales. Las funciones parciales juegan un rol importante en la teoría de computabilidad y complejidad pues son éstas las que se evalúan computables.

en adelante al ser imposible efectuar la división con un denominador 0. Lo anterior es suficiente para definir las funciones $q, r\colon \mathbb{N} \to \mathbb{Z}$ de forma que

$$r_k < r_{k-1}$$

y

$$r_{k-2} = q_k r_{k-1} + r_k$$

siempre que r_k esté definida. Debemos preguntarnos entonces cuándo están los números q_k y r_k definidos. Que estos números estén definidos para todo k en $\mathbb{N}$, depende en tener $r_k \neq 0$ para todo k. Por otro lado, tenemos que $0 \leq r_k$ por lo que el conjunto

$$\{r_1, r_2, \dots r_k, \dots\}$$

al ser un subconjunto de números naturales posee, por el principio de buen orden, un mínimo. Supongamos que r_m es dicho mínimo. Afirmamos que ese mínimo debe ser 0. En efecto, si $r_m \neq 0$, entonces podemos efectuar una vez más la división y obtener que $r_{m+1} < r_m$. Lo que es una contradicción con asumir que r_m es el mínimo. Entonces $r_m = 0$ y en consecuencia la secuencia no está definida en ningún sucesor de algún m. No sólo eso, que uno de los residuos esté obligado a ser 0, nos permite describir de la siguiente manera el proceso:

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \\
r_{n-1} &= q_n r_n.
\end{aligned}$$

Quizá esta descripción no parece tener importancia alguna, pero no debemos dejarnos engañar, en realidad el máximo común divisor en este punto ha sido calculado satisfactoriamente. El siguiente lema nos llevará al porqué.

Lema 2.17. *Para enteros a, b, q y r que satisfagan $a = qb + r$, se tiene que $(a, b) = (b, r)$.*

Demostración. Vamos a probar que un número d es un divisor común de a y b si y sólo si es un divisor común de b y r. Si este fuera el caso, los conjuntos de divisores comunes coinciden y en consecuencia los máximos de cada conjunto.

Es realidad sencillo, sólo debemos notar dos cosas. Primero que r es una combinación lineal de a y b y segundo que a es una combinación lineal de b y r. Por esta razón, si por un lado d es un divisor común de a y b, debe ser divisor también de r; de manera similar, si d es un divisor de b y r, debe serlo también de a. Esto prueba el enunciado que se afirmo en el primer párrafo y de su discusión sigue el resultado. ■

El lema anterior nos permite usar la descripción que hemos usado para concluir lo siguiente

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n.$$

Esta afirmación es precisamente la que buscamos. Aplicar el teorema de la división repetidas veces sobre dos números hasta encontrar el residuo 0, deriva en encontrar también el máximo común

divisor de dos números. No es difícil pensar lo anterior como un un programa de algún lenguaje de programación, por ejemplo *C*, y un con poco de motivación se puede proveer una implementación de este algoritmo.

Presentamos ahora un problema asociado: Resolver algunas interesantes ecuaciones con soluciones enteras. Podemos preguntarnos si es posible encontrar enteros x y y que satisfagan

$$ax + by = c.$$

A las ecuaciones de este tipo se les conoce como ecuaciones *diofantinas* o *diofánticas*, nombre que reciben por aparecer como problemas en el obra *Arithmetica* de Diofanto de Alejandría. En este caso, dichas ecuaciones son de carácter lineal, pero en general pueden ser mucho más complicadas, tan complicadas que existe un famoso teorema, resultado de los trabajos de Yuri Matiyasevich, Julia Robinson y Martin Davis que afirma imposible la existencia de un método general para resolver estas ecuaciones. Por fortuna, el caso lineal es particularmente sencillo y el algoritmo de Euclides es capaz de dar las soluciones si es que las hay.

Ahora debe notarse que la forma de una ecuación diofántica tiene similitud con la identidad de Bézout. En efecto, si podemos encontrar enteros s y t de forma que

$$sa + tb = d$$

y si $d|c$, entonces la ecuación

$$ax + by = c$$

tiene solución (solución será un múltiplo de los enteros entregados por la identidad de Bézout). El recíproco también es cierto: si la ecuación diofántica

$$ax + by = c$$

tiene solución, entonces el máximo común divisor de a y b debe dividir a c al resultar c una combinación lineal. La discusión en ese párrafo provee un argumento suficiente para afirmar el siguiente resultado.

Proposición 2.18. *Una ecuación diofántica lineal $ax + by = c$ tiene solución si y sólo si el entero c es un múltiplo del máximo común divisor de a y b.*

Si observamos la discusión, entonces se vuelve sencillo resolver una ecuación diofántica lineal si conocemos los valores indicados por la identidad de Bézout. De manera sorprendente conocemos ya un método que nos permite dar una expresión para ésta. Consideremos de nueva cuenta los cocientes y residuos del algoritmo de Euclides, es una simple observación que r_1 es una combinación lineal de a y b, r_2 una combinación lineal de b y r_1, r_3 una combinación lineal de r_1 y r_2 y así sucesivamente hasta llegar a r_n que es el último residuo que es distinto de 0. Por el ejercicio 2.11, r_n es una combinación lineal de a y b pero si nos detenemos para analizar la prueba, esta muestra como obtener r_n de manera explícita como una combinación lineal. Por ejemplo, en caso que tengamos

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 \end{aligned}$$

se debe tener

$$r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = -q_2 a + (1 + q_1 q_2)b$$

por lo que lo único necesario para saber los valores que indica la identidad de Bézout son los cocientes del algoritmo de Euclides. Este procedimiento no es difícil imaginarlo en el caso general y esa es la intención del ejercicio 2.16. Además, junto a la proposición 2.18, esta descripción también es capaz de dar solución a las ecuaciones del ejercicio 2.17.

En resumen, determinar las soluciones de una ecuación diofántica $ax + by = c$ basta seguir los siguientes pasos:

1. Usando el algoritmo de Euclides calcular el máximo común divisor de a y b.
2. Verificar si d divide a c. Si no lo hace, la ecuación no tiene solución, por el contrario si lo hace, usar los valores de los cocientes para calcular el máximo común divisor como combinación lineal de a y b obteniendo un par de enteros r y s.
3. Como c es múltiplo de d, los enteros r y s se usarán para calcular los valores x y y que dan solución a la ecuación.

Ejercicios

Ejercicio 2.1. Encuentra todos los divisores de 16 y 25.

Ejercicio 2.2. Demuestra que para cualquier entero a, debemos tener $a \mid 0$.

Ejercicio 2.3. Demuestra que para cualquier entero a, debemos tener $1 \mid a$.

Ejercicio 2.4. Suponga que R es un dominio entero. Se dice que un elemento a tiene inverso multiplicativo si existe b en R de forma que $ab = 1$. Demuestra que si c es cualquier otro elemento de R que satisface $ac = 1$, entonces $b = c$. En otras palabras, muestra que los inversos multiplicativos, si existen, son únicos.

Ejercicio 2.5. Encuentra un entero que no sea combinación lineal de 30 y 70.

Ejercicio 2.6. 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 2.7. Prueba que si c es combinación lineal de a y b entonces cualquier múltiplo de c también lo es.

Ejercicio 2.8. 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 2.9. Prueba el teorema 2.8.

Ejercicio 2.10. Vamos a proveer una generalización del corolario 2.11. 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 2.19. *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 2.11. Muestra que el conjunto de tres enteros consecutivos posee un múltiplo de 3.

Ejercicio 2.12. Muestra que el conjunto de m enteros consecutivos posee un múltiplo de m.

Ejercicio 2.13. Para proveer la demostración del teorema 2.13, considera los siguientes casos y utiliza el lema 2.12 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 2.14. Muestra que para cualesquiera dos enteros

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

Ejercicio 2.15. Asume que $d = sa + tb$ es una combinación lineal de a y b. Muestra que existe una cantidad infinita de parejas (s_k, t_k) de forma que

$$d = s_k a + t_k b.$$

Ejercicio 2.16. Utilizando el algoritmo de Euclides expresa como combinación lineal el máximo común divisor de los siguientes números.

1. 228 y 348
2. 15 y 21
3. $2n + 1$ y $4n$, para $n \geq 1$.

Ejercicio 2.17. Determina cuales de las siguientes ecuaciones diofánticas tienen solución y encuentra la solución si la tienen usando el algoritmo de Euclides.

1. $35x + 17y = 14$
2. $1242x + 1476y = 49$
3. $15x + 21y = 10$

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.

Las notas anteriores juegan algunas veces a ser un simple resumen de lo que otros autores han presentado, otras menos a reinterpretarlo y en una cantidad ínfima de ocasiones intentan pobremente aumentalo. El único objectivo real al que sirven, es preparar el curso de Álgebra Superior II impartido en la carrera de Actuaría de la FES Acatlán. Su versión es, en consecuencia, susceptible a errores gramaticales, imprecisiones técnicas y cambios constantes.