Lectura 3: Divisibilidad II

3.1. Factorización única

Comenzaremos esta sección describiendo una importante clasificación numérica. Mostraremos su importancia y sus propiedades, la más relevante de todas exhibe que estos números son, bajo cierta óptica, la estructura fundamental detrás de los enteros.

Definición 3.1. Decimos que un entero $p > 1$ es *un número primo* si sus únicos divisores son 1 y p.

A simple vista no parecerían tener mucha importancia estos números, sin embargo son la piedra angular de los enteros. Consideremos por ejemplo un número a que no sea primo, en se caso éste debe admitir un divisor distinto de 1 y de a. Esto quiere decir que existe un entero b que satisface $1 < b < a$ y $a = bc$ para algún otro número c. Este otro número c es por supuesto otro divisor de a por lo que $1 \leq c \leq a$, sin embargo es imposible que $c = 1$ o $c = a$ (en esos caso sería $a < a$). Esto indica de alguna manera que a se puede descomponer en los factores b y c. Usemos esto para formular un lema y una definición

Lema 3.1. *Si un número entero $a > 1$ no es primo, entonces existen números $1 < b < a$ y $1 < c < a$ tales que*

$$a = bc$$

.

Definición 3.2. Un número que no es primo, se dice *compuesto*.

Ahora, podríamos aplicar el tratamiento del lema 3.1 a los números b y c, los números resultantes decrecen y en algún punto esta descomposición involucrará únicamente números primos. Este argumento intuitivo se puede formalizar sin mucho problema.

Teorema 3.2. *Para cualquier entero $a > 1$ existen primos $p_1, p_2, \ldots p_{k-1}$ y p_k de forma que*

$$a = p_1 \cdots p_k.$$

En otras palabras, a se puede expresar como el producto de primos.

Demostración. Usaremos inducción fuerte sobre el enunciado «a se puede expresar como el producto de primos». El caso base será $a = 2$ y como 2 es primo, entonces se puede expresar como el producto de primos. Supongamos entonces que cualquier entero menor que a se puede expresar como el producto de primos. Si a es primo, entonces no hay nada que probar y el resultado sigue. Si por otro lado a es compuesto, entonces se puede expresar como $a = bc$ para algunos enteros $1 < b < a$ y $1 < c < a$ y por hipótesis de inducción, debemos tener

$$b = p_1 \ldots p_k$$

y

$$c = q_1 \dots q_l$$

para algunos primos $p_1, \dots, p_k, q_1, \dots, q_{l-1}$ y q_l; en ese caso tenemos que

$$a = p_1 \dots p_k q_1 \dots q_l$$

y en consecuencia a se puede expresar como el producto de primos.

Por inducción, el párrafo anterior indica que cualquier entero $a > 1$ se puede expresar como el producto de primos como deseábamos. ■

Vamos a dar ejemplos de esta factorización que hemos tratado únicamente en abstracto:

$$42 = 2 \cdot 3 \cdot 7,$$

$$36 = 2 \cdot 2 \cdot 3 \cdot 3,$$

$$15,400 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7 \cdot 11.$$

Estos ejemplos nos permiten observar un par de situaciones, la primera es que los factores que forman la expresión pueden estar repetidos, la segunda es las expresiones no dependen del orden sin embargo la enumeración de los factores parece depender del orden, por lo que nos veríamos obligados que las factorizaciones no son únicas. Pero al ser el producto conmutativo, no tendría sentido imponer una diferencia entre la expresión $2 \cdot 3$ y la expresión $3 \cdot 2$. Si se aprecia con cuidado, hemos usado la palabra factorización de manera libre, pero la observación anterior nos instiga a definir esta expresión de manera que nos sea útil.

Definición 3.3. Por *una factorización prima de un entero positivo a*, entenderemos un conjunto formado por números primos $p_1, p_2, \dots p_k$ de forma que $a = p_1 p_2 \dots p_k$.

Esta definición nos permite afirmar las factorizaciones primas de 42, $2 \cdot 3 \cdot 7$ y $7 \cdot 3 \cdot 2$, son la misma en virtud de que los conjuntos $\{2, 3, 7\}$ y $\{7, 3, 2\}$ coinciden. En general, esto nos permite afirmar que cambiar el orden de los factores, no cambia la factorización. Esto es algo que deseábamos y que nos permite volver a explorar la pregunta, ¿son las factorizaciones primas únicas? La respuesta a este hecho la entrega el importante *teorema fundamental de la aritmética* (teorema 3.5).

Lema 3.3 (Euclides)**.** *Si p es un número primo y $p|ab$, entonces $p|a$ o $p|b$. De manera más general, si $p|a_1 \dots a_n$, entonces p divide a alguno de los números a_i para $1 \leq i \leq n$.*

Demostración. Si $p \mid a$, entonces el resultado es inmediato, supongamos entonces que $p \nmid a$. Debemos notar que al ser p primo, cualquier divisor común de p y a es o 1 o p pero por hipótesis $p \nmid a$ por lo que debemos concluir que el único divisor común entre a y p es 1. Así, debemos concluir que $(p, a) = 1$.

Como $(p, a) = 1$, la identidad de Bézout garantiza la existencia de enteros s y t de forma que

$$sp + ta = 1,$$

en ese caso debemos tener que

$$b = sbp + tab.$$

De esta forma hemos expresado b como una combinación lineal de p y ab. Por otro lado, $p \mid p$ y por hipótesis $p \mid ab$, por lo que p debe dividir a cualquier combinación lineal de estos números, en particular $p \mid b$. Esto es lo que buscábamos. La segunda parte de la prueba se presenta al resolver el ejercicio 3.3. ■

Corolario 3.4. *Si un entero $m > 1$ satisface que, $m \mid ab$ siempre implica que $m|a$ o $m|b$, entonces m es primo.*

Demostración. Usaremos contraposición para mostrar que si m es compuesto, entonces no sigue necesariamente que m divida un producto implica que divide a alguno de sus factores.

Supongamos que m es compuesto y que $m = ab$ para algunos enteros $1 < a, b < m$. En ese caso, tenemos que $m \mid ab$, pero si $m \mid a$ o $m \mid b$, entonces $m \leq a$ o $m \leq b$ lo cual contradice las desigualdades que definen a a y b. Entonces, si m es compuesto, es falso que $m \mid ab$ implica $m \mid a$ o $m \mid b$. Por contraposición, el resultado que buscamos sigue. ■

Teorema 3.5. *Cualquier entero $a > 1$ posee una factorización prima única.*

Demostración. En el teorema 3.2 se ha probado que a tiene una factorización prima. Supongamos entonces que $a = p_1 \dots p_k$ y $a = q_1 \dots q_l$ son factorizaciones primas de a, en otras palabras

$$p_1 \dots p_k = q_1 \dots q_l.$$

Debemos mostrar para todo k y para todo l, que el conjunto formado por los números $p_1, \dots, p_{k-1}$ y p_k coincide con el formado por los números $q_1, \dots, q_l$ y q_l. Usaremos inducción sobre k para probar el enunciado anterior.

Para $k = 1$, debemos suponer $p_1 = q_1 \dots q_l$. En ese caso, $k = l = 1$ y $p_1 = q_1$, en otro caso p_1 sería el producto de primos en contradicción con ser éste primo. Por lo tanto, como los conjuntos de factores coinciden, las factorizaciones primas son iguales.

Supongamos para un natural k, que las factorizaciones coinciden siempre que su producto coincida. Si $p_1 \dots p_k p_{k+1} = q_1 \dots q_l$, entonces $p_1 \mid q_1 \dots q_l$ y, por el lema de Euclides, p_1 debe dividir alguno de los factores q_j, en otras palabras $p_1 = 1$ o $p_1 = q_j$ por ser q_j un número primo, pero p_1 es también un número primo y por tanto $p_1 \neq 1$, por lo que nos vemos obligados a concluir que $p_1 = q_j$ para algún $1 \leq j \leq l$. Esto nos permite afirmar que

$$p_1 \dots p_k = q_1 \dots q_{j-1} p_1 q_{j+1} \dots q_l$$

y por la ley de cancelación del producto, esto implica que

$$p_2 \dots p_k = q_1 \dots q_{j-1} q_{j+1} \dots q_l.$$

Con la igualdad anterior, la hipótesis de inducción nos permite garantizar que

$$\{p_1, \dots, p_k\} = \{q_1, \dots, q_{j-1} q_{j+1} \dots q_l\}$$

lo cual implica a su vez que

$$\{p_1, \dots, p_k\} = \{q_1, \dots, q_l\},$$

i.e., las factorizaciones primas coinciden, como buscábamos.

Por inducción, la afirmación realizada en el primer párrafo sigue y ésta indica solamente que no pueden existir dos factorizaciones primas distintas, lo que prueba el resultado. ■

Podemos arreglar un poco la expresión de un número como el producto de números primos, aglutinando los factores comunes con una notación exponencial.

Corolario 3.6. *Para $a > 1$, existe un único conjunto de primos distintos entre sí $p_1, \ldots, p_{k-1}$ y p_k, y números naturales $m_1, \ldots, m_{k-1}$ y m_k de forma que*

$$a = p_1^{m_1} \ldots p_k^{m_k}.$$

Este último resultado contiene una expresión que nos permite representar un entero de manera única a través de primos. No sólo eso, podemos ver que cualquier entero $a \neq \pm 1$ se puede expresar como

$$a = u p_1^{m_1} \ldots p_k^{m_k},$$

donde $u = \pm 1$. Este es el significado que nos permite afirmar que los primos son el bloque fundamental en el conjunto de los enteros, pues los enteros se pueden representar de manera única por un conjunto de números primos. Por último presentaremos un interesante resultado de la existencia una factorización única.

Teorema 3.7. *El conjunto de los números primos es infinito.*

Demostración. Para probar el resultado, procedemos por contradicción, i.e., supongamos que el conjunto de los números primos es finito, sean entonces $p_1, \ldots, p_{k-1}$ y p_k todos primos distintos y los únicos que hay. Definimos ahora el entero

$$m = p_1 \ldots p_k + 1,$$

el cual al ser mayor que 1, por lo que se puede expresar como un producto de primos. Tomemos q como el menor de los factores primos m; como el número de primos es finito, q debe dividir también a $p_1 \ldots p_k$, al ser uno de los elementos en esa lista y en consecuencia q es también divisor de la diferencia $m - p_1 \ldots p_k = 1$, lo cual resulta imposible pues $q > 1$. Así, el conjunto de los números primos no es finito. ■

3.2. Primos, divisores máximos y múltiplos mínimos

Hemos establecido un importante resultado que contiene una potente estructura en los naturales, debemos ahora vincularlo con los conceptos que hemos establecido. Primero, debemos notar que el teorema fundamental de la aritmética, implica que cada entero con $|a| \neq 1$ admite un divisor primo. Así, es relevante preguntarnos que relación guarda el máximo común divisor con la expresión prima de dos números.

Desarrollemos un par de ejemplos primero. Consideremos los números 550 y 154, no es difícil verificar que

$$1100 = 11 \cdot 2^2 \cdot 5^2$$

y

$$616 = 2^3 \cdot 11 \cdot 7$$

para poder comparar sus expresiones de manera más sencilla, debemos tener un conjunto común de factores que se encuentren ordenados. En este caso, es sencillo ver que la secuencia

$$2, 5, 7, 11$$

describe el conjunto de todos los factores involucrados. Podemos entonces expresar 1100 y 616 como producto de ellos:

$$1100 = 2^2 \cdot 5^2 \cdot 7^0 \cdot 11^1$$

$$616 = 2^3 \cdot 5^0 \cdot 7^1 \cdot 11^1.$$

Ahora, tampoco es complicado notar que

$$(1100, 616) = 44 = 2^2 5^0 7^0 \cdot 11^1.$$

Una comparación cuidadosa de los factores en el máximo común divisor nos da un método sencillo de como se han obtenido los exponentes.

Intentemos generalizar el procedimiento descrito en el párrafo anterior. Primero, para enteros a y b podemos expresar

$$a = q_1^{i_1} \dots q_k^{i_{k_1}}$$

y de igual forma

$$b = r_1^{j_1} \dots r_k^{j_{k_2}}.$$

En ese caso, el conjunto

$$S = \{q_1, \dots, q_{k_1}, r_1, \dots, r_{k_2}\}$$

está formado por números primos, el cual podemos describir como

$$S = \{p_1, \dots, p_k\}$$

tomando $p_1 < \dots < p_k$. Esto nos permitirá expresar

$$a = p_1^{m_1} \dots p_k^{m_k}$$

y de igual forma

$$b = p_1^{n_1} \dots p_k^{n_k}.$$

Con estas expresiones podemos realizar un análisis de lo que sucede respecto a los exponentes de los factores primos cuando un número divide a otro.

Lema 3.8. *Sean $p_1, \dots, p_{k-1}$ y p_k números primos, $m_1, \dots m_k, n_1, \dots n_{k-1}$ y n_k números naturales cualquiera, y sean por último $a = p_1^{m_1} \dots p_k^{m_k}$ y $b = p_1^{n_1} \dots p_k^{n_k}$. Entonces $a \mid b$ si y sólo si $m_i \leq n_i$ para todo $1 \leq i \leq k$.*

Demostración. Comencemos suponiendo que $m_i \leq n_i$. En ese caso podemos simplemente definir $l_i = n_i - m_i$ y eligiendo

$$q = p_1^{l_1} \dots p_k^{l_k}$$

tenemos que $b = qa$.

Supongamos ahora que $a \mid b$, en ese caso existe un entero q de forma que $b = qa$; ese entero q debe poseer una factorización prima que se puede expresar ubicando naturales $l_1, \dots, l_{k-1}$ y l_k de forma que $q = p_1^{l_k} \dots p_k^{l_k}$ lo que implica a su vez que

$$p_1^{n_1} \dots p_k^{n_k} = b = qa = p_1^{m_1 + l_1} \dots p_k^{m_k + l_k},$$

al ser las factorizaciones primas únicas, la anterior igualdad implica que $n_i = m_i + l_i$ para toda $1 \leq i \leq k$. Además, tenemos garantía que $l_i \geq 0$, con lo que podemos concluir que $n_i - m_i \geq 0$. En otras palabras $m_i \geq n_i$ como afirma el resultado. ∎

Proposición 3.9. *Sean $p_1, \ldots, p_{k-1}$ y p_k números primos, $m_1, \ldots m_k, n_1, \ldots n_{k-1}$ y n_k números naturales cualquiera, y sean por último $a = p_1^{m_1} \ldots p_k^{m_k}$ y $b = p_1^{n_1} \ldots p_k^{n_k}$. Entonces, si se elige $l_i = \text{mín}\{m_i, n_i\}$,*

$$(a, b) = p_1^{l_1} \ldots p_k^{l_k}.$$

Demostración. Debemos notar primero que el número

$$d = p_1^{l_1} \ldots p_k^{l_k}$$

es un divisor común de a y b, esto es consecuencia del lema pues por hipótesis, $l_i \leq m_i$ y también $l_i \leq n_i$ para todo $1 \leq i \leq k$.

Ahora, podemos expresar el máximo común divisor encontrando naturales $t_1, \ldots, t_{k-1}$ y t_k, para escribir

$$(a, b) = p_1^{t_1} \ldots p_k^{t_k}.$$

Como en particular $d \mid a$ y $d \mid b$, de acuerdo al lema anterior $t_i \leq m_i$ y $t_i \leq n_i$ para toda $1 \leq i \leq k$, esto implica que $t_i \leq \text{mín}\{m_i, n_i\} = l_i$. Además, d es un divisor común, por lo que $d \mid (a, b)$ y de acuerdo al lema, esto deriva en tener que $l_i \leq t_i$, lo que prueba $t_i = l_i$ y así $(a, b) = d$ que es precisamente lo que afirma la proposición. ∎

Podemos llevar esto más lejos. Una pregunta que podemos hacer es indagar el significado de tomar no el mínimo, como lo hace la anterior proposición, sino el máximo. Para responder la pregunta, presentamos ahora el concepto dual del máximo común divisor: el mínimo común múltiplo.

Definición 3.4. Un número c se dice *un múltiplo común de los enteros a y b* si es un múltiplo de ambos. El mínimo común múltiplo se denotará como $[a, b]$.

Con este lenguaje es posible enunciar un resultado análogo a la proposición 3.9. La prueba resulta análoga y es un ejercicio excelente recrearla usando paso a paso el lema 3.8 (ejercicio 3.4).

Proposición 3.10. *Sean $p_1, \ldots, p_{k-1}$ y p_k números primos, $m_1, \ldots m_k, n_1, \ldots n_{k-1}$ y n_k números naturales cualquiera, y sean por último $a = p_1^{m_1} \ldots p_k^{m_k}$ y $b = p_1^{n_1} \ldots p_k^{n_k}$. Entonces, si se elige $l_i = \text{máx}\{m_i, n_i\}$,*

$$[a, b] = p_1^{l_1} \ldots p_k^{l_k}.$$

Las proposiciones 3.9 y 3.9 tienen una conclusión muy natural que de hecho describirá el mínimo común múltiplo en términos del máximo común divisor y hará que la teoría que hemos estado desarrollando resulte igual de relevante para este concepto. Sin embargo, se puede proveer una prueba independiente del teorema (quizá más sencilla desde el punto de vista de la manipulación algebraica correspondiente). Con la suficiente motivación uno debe ser capaz de encontrarla.

Teorema 3.11. *Para enteros cualquiera a y b, se tiene que*

$$ab = (a, b)[a, b].$$

Esta identidad resulta importante, pues el concepto de mínimo común múltiplo fue recién introducido y no conocemos mucho acerca de éste y menos de como calcularlo. Lo interesante, al menos desde el punto de vista del cómputo del número, es que cualquier método que se use para calcular el máximo común divisor, provee una forma muy sencilla para calcular el mínimo común múltiplo. Esto hace que cuando menos calcularlo sea una menos de nuestras preocupaciones.

3.3. Congruencias módulo m

Comenzaremos describiendo una forma de presentar algunos resultados relacionados con la divisibilidad a través de definir una relación sobre los enteros.

Definición 3.5. Sea $m > 1$ un número natural . Para dos enteros a y b, diremos que *a es congruente con b módulo m* si y sólo si $a - b$ es un múltiplo de m. En símbolos, escribiremos

$$a \equiv b \mod m.$$

Vamos a establecer una convención respecto a las posibles relaciones que resultan para la elección de m. Primero notamos que cualquier número es divisible por 1, por lo que la relación módulo 1 no es muy interesante, ni tampoco la de los números negativos, pues con su parte positiva se puede conseguir el mismo resultado. Es por esta razón que cuando no se especifique, el número m se asumirá $m > 1$ durante esta sección.

Es importante plantearse la razón de ser de este nuevo concepto, uno puede pensar de manera poco acertada que es sólo una nueva forma de hablar acerca de la divisibilidad, pues $a \equiv 0 \mod m$ si y sólo si $m \mid a$. En su lugar, su intención es proveer una notación bastante sugestiva para

$$m \mid a - b,$$

expresión de no debe parecer ajena pues el teorema de la división nos da un caso de esta forma. Veamos cómo.

Proposición 3.12. *Para cada entero $a > 1$, existe un único entero $0 \leq r < m$ tal que*

$$a \equiv r \mod m.$$

Demostración. Como se comentó, esto será resultado del teorema de la división. Dicho teorema, garantiza la existencia de un único par de números q y $0 \leq r < m$ de forma que

$$a = qm + r,$$

en otras palabras $m \mid a - r$ y en consecuencia $a \equiv r \mod m$. Este número debe ser único pues cualquier otro número con la propiedad que buscamos resulta ser simplemente el residuo de la misma división. Esto es lo que afirma el resultado. ■

Esta última proposición es provocativa, a de alguna forma está representado por el residuo de dividirlo entre m, al menos parece contener toda la información necesaria para definir la relación módulo m. De hecho, la proposición nos permite decir que cualquier entero $r + (\text{múltiplo de } m)$ debe ser equivalente a a módulo m. Esta apariencia se confirma en el siguiente resultado.

Proposición 3.13. *Sean a y b enteros y sean también r_1 y r_2 los residuos de dividir a entre m y b entre m respectivamente. Entonces $a \equiv b \mod m$ si y sólo si $r_1 = r_2$.*

Demostración. Muy parecido al caso anterior, escribimos $a = q_1 m + r_1$ y $b = q_2 m + r_2$ donde los residuos satisfacen $0 \leq r_1, r_2 < m$. Ahora, si $r_1 = r_2$, entonces

$$a - q_1 m = b - q_2 m$$

o en otras palabras

$$a - b = (q_1 - q_2)m$$

por lo que $a \equiv b \mod m$.

Si por el contrario $a \equiv b \mod m$, entonces $a - b = km$ para algún k. En ese caso

$$a = km + b = km + q_2 m + r_2 = (k + q_1)m + r_2,$$

como $r_2 < m$, éste debe ser el residuo indicado por el algoritmo de la división, luego $r_1 = r_2$. ■

La proposición anterior puede resultar increíblemente sencilla de probar si se sabe de antemano que la relación módulo resulta una relación de equivalencia. Esto se tendrá oportunidad de probar en el ejercicio 3.10. Toca el turno ahora de verificar algunas propiedades que nos permiten determinar el comportamiento de la relación módulo respecto a la suma y al producto.

Teorema 3.14. *Para cualesquiera enteros a, b, c y d se verifica:*

1. *Si $a \equiv b \mod m$, entonces $ca \equiv cb \mod m$, para todo entero c.*
2. *Si $a \equiv b$ y $c \equiv d \mod m$, entonces $a + c \equiv b + d$ y $ac \equiv bd \mod m$.*

Demostración. Estos resultados son inmediatos de las definiciones y se probará solamente 1. Supongamos con este objetivo que $a \equiv b \mod m$; en ese caso, existe un número k de forma que $a - b = km$. Entonces,

$$ca - cb = c(a - b) = ckm$$

por lo que $m \mid ca - cb$ y como consecuencia de la definición, $ca \equiv cb \mod m$. ■

Hay muchas propiedades que nos permiten cambiar el módulo y dar afirmaciones sin esfuerzo alguno. Una muy interesante está contenida en el siguiente lema.

Lema 3.15. *Para un natural $n > 1$ se tiene que*

1. *Si $n \mid m$ y $a \equiv b \mod m$, entonces $a \equiv b \mod n$.*
2. *Si $a \equiv b \mod m$ y $a \equiv b \mod n$, entonces $a \equiv b \mod [m, n]$.*

Demostración. Para probar 1., sólo es necesario seguir las propiedades de la divisibilidad: Por hipótesis $n \mid m$ y $m \mid a - b$, como la divisibilidad es transitiva, entonces $n \mid a - b$ y en consecuencia $a \equiv b \mod n$.

La prueba de 2., es una simple aplicación del ejercicio 3.7: Por hipótesis $a - b$ es un múltiplo de m y de n, entonces $a - b$ es también múltiplo de $[m, n]$ por lo que $a \equiv b \mod [m, n]$. ■

El principal interés del lema, se encuentra en la expresión decimal de los enteros. Con un poco de observación podemos ver que nuestra forma de escribir cualquier número es una combinación lineal de las potencias de 10, e.g.,

$$134 = 1 \cdot 10^2 + 3 \cdot 10^1 + 4 \cdot 10^0$$

$$7245 = 7 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10^1 + 5 \cdot 10^0,$$

estas combinaciones lineales por supuesto, no admiten más que *dígitos*, i.e., los números $0, 1, \ldots, 8$ y 9. En general, para cualquier entero positivo a, podemos expresarlo como

$$a = a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n$$

donde los números $a_0, \ldots a_{n-1}$ y a_n se les llama los dígitos de a. Presentamos ahora un ejemplo, con tintes de mera curiosidad, a través del cual observaremos como es que el concepto de congruencia se logra transmitir a los dígitos.

Ejemplo. *Un entero a es múltiplo de 9 si y sólo si 9 divide a la suma de sus dígitos.* En efecto, debemos notar primero que $10 \equiv 1 \mod 9$, y según el teorema 3.14, debemos tener $10^n \equiv 1 \mod 9$; bajo el mismo teorema, también podemos expresar

$$\begin{aligned} a &= a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n \\ &\equiv a_1 + \cdots + a_n \mod 9. \end{aligned}$$

En consecuencia, a es divisible por 9 si y sólo si 9 divide a la suma de sus dígitos.

Ejemplo. *Un entero a es un múltiplo de 2 si y sólo si a_0 es un múltiplo de 2.* Debemos notar que $10^n \equiv 0$ mód 2 y en consecuencia

$$\begin{aligned} a &= a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n \\ &\equiv a_0 \mod 2. \end{aligned}$$

Lo que implica que a es múltiplo de 2 si y sólo a_0 es múltiplo de 2.

Un par de casos derivado de estos ejemplos están presenten en los ejercicio 3.12. Estos ejemplos constituyen parte de un interesante grupo de problemas conocidos como *pruebas de sanidad*, una discusión mucho más elaborada puede encontrarse en el capítulo 5 sección C de [Chi95].

La siguiente definición es sólo una conveniencia, es importante notar que no es una operación nueva, ni refiere de forma alguna a los inversos multiplicativos, es sólo una manera de hacer referencia al cociente de una división cuando ésta no presenta residuo. La única razón por la que se introduce es para simplificar algunas expresiones y se debe tratar con sumo cuidado hasta que se comprenda la diferencia.

Definición 3.6. Si $a \mid b$, al único número q tal que $b = qa$ se le denotará por b/a o $\frac{b}{a}$.

Proposición 3.16. *Para un natural $n > 1$ se tiene que:*

1. *Si $na \equiv nb \mod nm$, entonces $a \equiv b \mod m$.*
2. *Si $na \equiv nb \mod m$ y $(m, n) = 1$, entonces $a \equiv b \mod m$.*
3. *Si $na \equiv nb \mod m$, entonces $a \equiv b \mod \frac{m}{(m,n)}$.*

Demostración. Para probar 1., suponemos que $na \equiv nb \mod nm$, lo que por definición significa que $nm \mid na - nb$ o en otras palabras,

$$n(a - b) = n(qm),$$

lo que por ley de cancelación implica que $m \mid a - b$ y consecuencia $a \equiv b \mod m$.

Para probar 2., aparte de suponer que $na \equiv nb \mod m$, debemos notar que $na \equiv nb \mod n$; de acuerdo al lema 3.15, se debe tener que

$$na \equiv nb \mod [m, n],$$

pero como $(m, n) = 1$ y debido al teorema 3.11, debemos tener que $mn = [m, n]$; esto nos lleva directamente a la congruencia

$$na \equiv nb \mod mn$$

y por 1., debemos concluir que

$$a \equiv b \mod m.$$

Para probar 3., usamos la congruencia que se obtuvo en el primer paso del párrafo anterior, i.e.,

$$na \equiv nb \mod [m,n]$$

Ahora, tomamos q como el único entero tal que $m = q(m,n)$, en ese caso tenemos

$$[m,n](m,n) = mn = nq(m,n)$$

y como m y n son enteros > 1, la ley de cancelación garantiza que

$$nq = [m,n],$$

esto se traduce en tener

$$na \equiv nb \mod nq;$$

de nueva cuenta por 1. y como $q = m/(m,n)$,

$$a \equiv b \mod \frac{m}{(m,n)}.$$

■

Hemos desenredado muchas de las propiedades de las congruencias. Sin embargo, hemos de notar que sólo son reformulaciones de los resultados que hemos presentado sobre divisibilidad, que resulta en un lenguaje nuevo para hablar de lo mismo. Entonces, ¿cuál es la ventaja de presentarlo de esta manera? Se podrá notar que el símbolo para la congruencia $\equiv$ guarda similitud con el de igualdad, esto por supuesto no es una coincidencia. La ventaja de presentar los conceptos de divisibilidad a través de congruencias resulta en que podemos plantear ecuaciones, por ejemplo, encontrar los números x tales que

$$x + 2 \equiv 3 \mod 5.$$

En este caso basta notar que estamos buscando números $x \equiv 1 \mod 5$ los cuales, por la proposición 3.12 son aquellos números que tienen residuo 1 al dividir por 5, de manera explícita, las soluciones son el conjunto

$$\{q \cdot 5 + 1 \mid q \in \mathbb{Z}\}.$$

Como podemos ver, las propiedades de congruencia nos permiten resolver de manera sencilla las ecuaciones del tipo $x + a \equiv b \mod m$. Podemos preguntarnos que sucede con las congruencias del tipo

$$ax \equiv b \mod m.$$

Si éstas fueran una igualdad, lo que debemos encontrar es un entero x de forma que $ax = b$, en otras palabras buscamos responder si $a \mid b$. Pero al ser congruencias, lo que buscamos es un entero x de forma que $b = ax + n$, donde n es un múltiplo de m, o de manera equivalente si podemos encontrar enteros x y y de forma que $b = ax + my$. Si traemos de vuelta los conceptos de divisibilidad, sabemos como resolver esas ecuaciones: Como b es una combinación lineal de a y m, entonces las soluciones se pueden garantizar a condición que (a,m) divida a b. Si este es el caso, la identidad de Bézout nos dice como proceder. Ilustremos esto con un par de ejemplos.

Consideremos primero la congruencia

$$3x \equiv 4 \mod 12.$$

En ese caso $(3, 12) = 3$, sin embargo, si suponemos que la congruencia tiene solución, entonces podemos podemos expresar

$$3x - 4 = 12q$$

para algunos x y q enteros. Esto quiere decir que 4 es una combinación lineal de 3 y 12 por lo que debería ser divisible por cualquier divisor común de estos, en particular de 3, pero $3 \nmid 4$ por lo que asumir que tiene solución deriva en contradicción.

Supongamos ahora la congruencia

$$20x \equiv 5 \mod 15,$$

en ese caso $(15, 20) = 5$ el cual es múltiplo de 5 y ocupando la identidad de Bézout podemos expresar $5 = 1 \cdot 20 + (-1) \cdot 15$ y en consecuencia $x = 1$ es una solución para la congruencia que buscamos. Además no es difícil verificar que $x = 4$ es otra posible solución, en realidad cualquier suma de 1 con un múltiplo de 3 es una solución (¡compruébalo!). Vamos a estructurar el procedimiento anterior, primero de una forma limitada, luego de una manera más general.

Teorema 3.17. *Si $(a, m) = 1$, entonces la congruencia*

$$ax + b \equiv 0 \mod m$$

tiene solución. Además, cualesquiera dos soluciones x_1 y x_2 satisfacen

$$x_1 \equiv x_2 \mod m.$$

Demostración. Comencemos notando que al ser $(a, m) = 1$, la identidad de Bézout garantiza la existencia de enteros s y t de forma que

$$sa + tm = 1$$

por lo que debemos tener

$$bsa + btm = b$$

y en consecuencia

$$(-bs)a + b = btm$$

o en términos de congruencias

$$(-bs)a + b \equiv 0 \mod m$$

por lo que elegir $x = -bs$ resulta una solución de la congruencia.

Para probar la segunda parte supongamos que dos números x_1 y x_2 son soluciones de la congruencia, i.e.,

$$ax_1 \equiv -b \mod m$$
$$ax_2 \equiv -b \mod m$$

Por ser la relación transitiva y simétrica, debemos tener que

$$ax_1 \equiv ax_2 \mod m$$

y como $(a, m) = 1$, el lema 3.16 implica que

$$x_1 \equiv x_2 \mod m.$$

■

Teorema 3.18. *La congruencia*

$$ax + b \equiv 0 \mod m$$

tiene solución si b es un múltiplo de (a, m)*. Ademas cualesquiera dos soluciones* x_1 *y* x_2 *satisfacen*

$$x_1 \equiv x_2 \mod \frac{m}{(m, a)}$$

Demostración. La prueba es semejante al caso anterior. Describimos primero $b = q(m, a)$ para algún entero q, enseguida usamos la identidad de Bézout para encontrar los enteros r y s de forma que

$$sa + tm = (a, m)$$

con lo que tenemos

$$qsa + qtm = q(a, m) = b$$

y en consecuencia

$$(-qs)a + b \equiv 0 \mod m.$$

por lo que la congruencia tiene solución en $x = -qs$, garantizando la existencia. La prueba de la segunda parte es muy similar a la del teorema anterior y se obtiene en el ejercicio 3.15. ■

Corolario 3.19. *La congruencia* $ax \equiv 1 \mod m$ *tiene solución si y sólo si* $(a, m) = 1$*.*

Por último, notamos que podemos tener de igual forma sistemas de congruencias y mientras sean lineales, éstas siempre tienen solución. De hecho, problemas que involucran congruencias simultaneas con módulos primos relativos aparecen en antiguos manuscritos Chinos y el método para resolverlos que aparece en éstos, aparece en la prueba del siguiente teorema.

Teorema 3.20 (Teorema chino del residuo)**.** *Si m y n son primos entre sí, entonces las congruencias*

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

tienen una solución común.

Demostración. Comenzamos notando que el teorema 3.17 garantiza que la primer congruencia tiene al menos una solución y cualquier número que podrá expresar como

$$x = a + ym$$

para algún entero y, será de igual forma una solución. Esto quiere decir que si podemos encontrar un entero y de forma que

$$a + ym \equiv b \mod n$$

podremos concluir el resultado que buscamos. Pero podemos escribir la congruencia anterior como

$$my + (a - b) \equiv 0 \mod n$$

y como $(m, n) = 1$, de nueva cuenta el teorema 3.17 garantiza la existencia de un entero con esa propiedad. Así, $x = a + ym$ es una solución común las congruencias. ■

Ejercicios

Ejercicio 3.1. Para un primo p y un entero $a > 1$, muestra que $(p, a) \neq 1$ si y sólo si $p \mid a$.

Ejercicio 3.2. Sea a, b y c números enteros cualquiera. Demuestra que si $c \mid ab$ y $(c, a) = 1$ entonces $c|b$. Sugerencia: Modificar la prueba de uno de los lemas presentados es suficiente. El objetivo es encontrar cuál.

Ejercicio 3.3. Prueba la segunda parte del lema 3.3. Sugerencia: Usa inducción.

Ejercicio 3.4. Prueba la proposición 3.10. Sugerencia: Ajusta la prueba de la proposición 3.9.

Ejercicio 3.5. Demuestra que para enteros m y n, se tiene que $m + n = \text{mín}\{m, n\} + \text{máx}\{m, n\}$.

Ejercicio 3.6. Prueba el teorema 3.11 usando el ejercicio anterior y las proposiciones 3.9 y 3.10.

Ejercicio 3.7. Demuestra que si $m \mid a$ y $n \mid a$ entonces $[m, n] \mid a$. Sugerencia: Una forma sencilla de hacer esto es usar las factorizaciones primas de a, m y n.

Ejercicio 3.8. Si a y b son enteros que dividen a n y tales que $(a, b) = 1$, demuestra que su producto también divide a n.

Ejercicio 3.9. Verifica las siguientes congruencias

1. $1329 \equiv 2 \mod 9$.
2. $182 \equiv 119 \mod 9$.
3. $-3 \equiv 27 \mod 6$.
4. $145 \equiv 2 \mod 13$.

Ejercicio 3.10. Prueba que la relación $\cdot \equiv \cdot \mod m$ es una relación de equivalencia.

Ejercicio 3.11. Termina la demostración del teorema 3.14

Ejercicio 3.12 (Otras pruebas de sanidad). Demuestra que:

1. Un entero a es múltiplo de 3 si y sólo si 3 divide a la suma de sus dígitos.
2. Un entero a es un múltiplo de 5 si y sólo si a_0 es un múltiplo de 5.

Ejercicio 3.13. Muestra que $x \equiv y \mod m$, implica $(x, m) = (y, m)$.

Ejercicio 3.14. Encuentra el menor entero positivo x, si existe, que satisfaga:

1. $16x - 9 \equiv 0 \mod 35$.
2. $200x + 315 \equiv 0 \mod 411$.
3. $6x + 3 \equiv 4 \mod 10$.
4. $(2n + 1)x + 7 \equiv 0 \mod 4n$, para $n > 1$.

Ejercicio 3.15. Termina la prueba del teorema 3.18.

Ejercicio 3.16 (El otro teorema chino del residuo). Sean $m_1, \ldots, m_{k-1}$ y m_k primos relativos en pares, i.e., siempre que $i \neq j$, se tiene $(m_i, m_j) = 1$. Demuestra que las congruencias

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

tienen una solución común.

Ejercicio 3.17. Encuentra una solución común para las siguientes colecciones de congruencias.

1. $x \equiv 0 \mod 7$ y $x \equiv 0 \mod 8$.
2. $x \equiv 3 \mod 17$, $x \equiv 4 \mod 21$. y $x \equiv 5 \mod 25$

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.

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.