



Divisibilidad

Emilio Toscano Oneto

1 Definiciones y Resultados

La divisibilidad es una de las propiedades más fundamentales de la Teoría de Números y es un área que tiene enfoque en el conjunto de los enteros. A lo largo de las notas al mencionar un número entero, nos referiremos a aquellos números de la colección $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ y cuando se mencionen a los números naturales, hacemos referencia a la colección de números $\mathbb{N} = \{1, 2, 3, \dots\}$.

Definición 1.1. Si a y b son enteros, decimos que a divide a b (escrito también como $a \mid b$), si es posible encontrar un entero x tal que $ax = b$.

Escribiremos $a \nmid b$ para decir que a no divide a b . Podemos además notar que la definición también se vale para números enteros negativos, como por ejemplo, el 2 divide al -4 , pues $2(-2) = -4$. Será de gran importancia reconocer que las aclaraciones

- a divide a b
- a es divisor de b
- a es factor de b
- b es múltiplo de a y
- b es divisible entre a ,

son todas equivalentes entre sí.

Nota 1.2. Diremos que un entero a es un número par si $2 \mid a$. Con esta definición, vemos que el 0 es un número par, pues $2(0) = 0$ y más aún, podremos decir que el 0 divide al 0, pues existen enteros x de tal manera que $0x = 0$. En base a lo anterior, diremos que a es un entero impar si $2 \nmid a$.

Proposición 1.3. Algunas propiedades básicas de la división son:

- (i) Para todo entero a , se cumple que $a \mid a$.
- (ii) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
- (iii) Es posible que $a \mid b$, pero $b \nmid a$.
- (iv) Para a y b enteros, $a \mid b$ y $b \mid a$ si y sólo si $a = b$ ó $a = -b$.
- (v) Si $a \mid b$ pero $a \nmid c$, entonces $a \nmid b + c$.
- (vi) Si $a \mid b$, entonces $-a \mid b$.

Demostración de Proposición 1.3 : (i) En efecto, tomando a $x = 1$, siempre se cumple que $ax = a$ y por lo tanto $a \mid a$.

(ii) Si $a \mid b$ y $b \mid c$, entonces existen enteros x y y tales que $ax = b$ y $by = c$, entonces $axy = by = c$, por lo tanto $a \mid c$.

(iii) Como ejemplo podemos tomar a $a = 1$ y $b = 2$.

(iv) Si $a \mid b$ y $b \mid a$, existen enteros x y y tales que $ax = b$ y $by = a$, por lo tanto $axy = by = a$, de donde $xy = 1$ por ser entero y así $x = y = 1$ o bien $x = y = -1$ y de ambos casos se sigue que $a = b$ ó $a = -b$. Si $a = b$ ó $a = -b$, se tiene que $a(1) = b$, por lo que $a \mid b$ y a su vez $b(-1) = a$, de donde $b \mid a$.

(v) Si $a \mid b$ pero $a \nmid c$, entonces existe un entero d tal que $ad = b$ y para cualquier entero n se tiene que $an \neq c$. En particular tomando al número $n = m - d$ con m algún entero arbitrario, se sigue que $a(m - d) \neq c$, es decir, $am \neq ad + c = b + c$ y así $a \nmid b + c$.

(vi) Si $a \mid b$, entonces existe k entero tal que $ak = b$ y así tomando a $n = -k$, se tiene que n es entero y además $ak = a(-n) = (-a)n = b$, por lo tanto $-a \mid b$. ■

Ejemplo 1.4. Para a y b , enteros positivos, si $a \mid b$, entonces $a \leq b$. Para ello, puesto que son positivos, se tiene que $a, b > 0$ y además existe un entero k tal que $ak = b$, entonces por lo anterior, $k > 0$ y por ser entero, $k \geq 1$, entonces $a \leq ak = b$.

Ejemplo 1.5. Para c un entero distinto de 0, entonces $a \mid b$ si y sólo si $ac \mid bc$.

Si $a \mid b$, entonces hay algún entero n tal que $an = b$. Está ecuación es equivalente a $c(an) = c(b)$, pues $c \neq 0$, y así $(ac)n = bc$, lo cual por definición implica que $ac \mid bc$ y se obtiene la equivalencia.

Proposición 1.6. Para a, b y c enteros, tenemos que $a \mid b$ y $b \mid c$ si y sólo si $a \mid bx + cy$ para cualesquiera enteros x y y .

Demostración de Proposición 1.6 : Supongamos que $a \mid b$ y $a \mid c$. Entonces existen enteros d y e tales que $ad = b$ y $ae = c$, por lo que si x y y son enteros cualesquiera, se sigue que $a(dx + ey) = adx + aey = bx + cy$, por lo tanto $a \mid bx + cy$.

Supongamos ahora que $a \mid bx + cy$ para cualquier par de enteros x y y . Como cualquier pareja x y y cumplen lo anterior, podemos tomar $x = 0$ y $y = 1$ y observar que $a \mid c$, pues $b(0) + c(1) = c$ y cuando tomamos $x = 1$ y $y = 1$ se obtiene que $a \mid b$. ■

Corolario 1.7. Si b, c y d son enteros que satisfacen la ecuación $b + c = d$ y a es otro entero que divide a dos de ellos, entonces divide al tercero.

Definición 1.8. Decimos que un entero a es combinación lineal de los enteros b y c , si existen dos enteros x y y que satisfacen la ecuación $bx + cy = a$.

Ejemplo 1.9. Podemos escribir a 19 como combinación lineal de 3 y 5. Para ello basta con considerar a $x = 3$ y $y = 2$ para observar que $3x + 5y = 19$.

Proposición 1.10. Sean a, b enteros cualesquiera y d un divisor del número natural n , entonces $a^d - b^d \mid a^n - b^n$

Demostración de Proposición 1.10 : Si d es divisor de n , entonces existe un entero k tal que $dk = n$ y así

$$(a^d - b^d)(a^{d(k-1)} + a^{d(k-2)}b^d + \dots + a^d b^{d(k-2)} + b^{d(k-1)}) = (a^n - b^n).$$

Los detalles de esta factorización queda como ejercicio moral para el lector. ■

Ejemplo 1.11. Considera al número $987^6 - 123^6$. Puesto que $6 = 2 \cdot 3$, entonces los números $987^2 - 123^2$ y $987^3 - 123^3$ lo dividen.

Demuestra que $13 \mid 89^{50} - 76^{50}$. Por la Proposición 1.10, se tiene que el entero $89 - 76 = 13$ divide a $89^{50} - 76^{50}$, pues $d = 1$ es divisor de $n = 50$.

Definición 1.12. Decimos que p es número primo cuando los únicos números enteros que lo dividen son ± 1 y $\pm p$.

A pesar de que esta definición se da de manera general para enteros positivos y negativos, aquí cada vez que se haga referencia a un número primo se supondrá que son positivos a no ser que se mencione lo contrario.

Ejemplo 1.13. Entre los números del 1 al 10, los únicos primos que hay son 2, 3, 5 y 7, pues en casos como 6, 8, 10, se tiene que 2 los divide y por tanto no cumplen la definición de número primo. El 1 no se considera primo, pues para serlo necesita tener exactamente 2 divisores (salvo el signo). Por el mismo motivo, el 0 tampoco es primo.

Ejemplo 1.14. Demuestra que los enteros 1573, 157573, 15757573, ... no son primos.

Consideremos el caso para 15757573, el caso general es analogo (puedes intentar escribirlo como ejercicio). Notemos que

$$\begin{aligned} 15757573 &= 15757573 + (157573 - 157573) + (1573 - 1573) \\ &= (15757573 - 157573) + (157573 - 1573) + 1573 \\ &= 15,600,000 + 156,000 + 1573. \end{aligned}$$

En particular $156 = 13 \cdot 12$, mientras que $1573 = 13 \cdot 11^2$, por lo tanto, 13 divide a cada sumando y luego $13 \mid 15757573$.

Definición 1.15. Decimos que un entero a es compuesto si a es producto de al menos 2 primos (no necesariamente distintos).

Ejemplo 1.16. Los números 12, 25, 77 y 42920 son todos números compuestos, pues los podemos escribir como $12 = 2 \cdot 2 \cdot 3$, $25 = 5 \cdot 5$, $77 = 7 \cdot 11$ y $42920 = 4292 \cdot 2 \cdot 5$. Es decir, se pueden escribir como producto de 2 primos ó más.

Teorema 1.17. (Teorema Fundamental de la Aritmética) Todo entero n distinto de 0 y ± 1 es producto de números primos.

Demostración de Teorema 1.17 : Sea n un entero positivo, si n es primo, terminamos (pues se puede como producto de un solo primo). Si n no es primo, entonces $n = ab$ para enteros positivos a, b menores a n , si a y b son primos, acabamos, si alguno de ellos no lo es, podemos escribirlo como producto de enteros más chicos, y así sucesivamente. Este procedimiento debe de acabar en algún punto, pues los números se vuelven más chicos y son positivos, por lo que en dicho punto se tendrá a n como producto de primos. Para el caso en el que n es un entero negativo, podemos considerar a $-n$ (pues es positivo) y repetir el mismo procedimiento. ■

Este Teorema en su versión completa garantiza que dicho producto de primos es único salvo el orden de los factores y el signo, lo cual será de alta utilidad en futuros resultados. Más aún, cuando se descompone a un entero a como producto de primos, a esa descomposición la llamaremos *descomposición canónica* del número y usualmente al escribirla se ordenan los primos de menor a mayor.

Ejemplo 1.18. Si el producto de 3 números distintos, mayores a 1 da como resultado 100. ¿Cuáles son esos enteros?

Por el Teorema 1.17, se puede observar que $100 = 2^2 \cdot 5^2$, de donde las posibles combinaciones con 3 números con producto igual a 100 (sin incluir al 1 como factor), son

$$\begin{aligned} 4 \cdot 5 \cdot 5 \\ 2 \cdot 2 \cdot 25 \\ 2 \cdot 5 \cdot 10 \end{aligned}$$

De donde la única combinación con factores distintos es la última y así los enteros que buscamos son 2, 5 y 10.

Ejemplo 1.19. La descomposición canónica de los números 30, 24 y 108 esta dada por

$$\begin{aligned} 30 &= 2 \cdot 3 \cdot 5 \\ 24 &= 2^3 \cdot 3 \\ 108 &= 2^2 \cdot 3^3. \end{aligned}$$

Ejemplo 1.20. Encuentra todos los primos p tales que $p \mid 3^4 + 2^4 + 6^2$.

Notemos que

$$\begin{aligned} 3^4 + 2^4 + 6^2 &= (3^4 + 2(6^2) + 2^4) - 6^2 = (3^2 + 2^2)^2 - 6^2 \\ &= (3^2 + 2^2 - 6)(3^2 + 2^2 + 6) = 7 \cdot 19 \end{aligned}$$

Por lo tanto, si p es un primo que divide al número, entonces $p = 7$ ó $p = 19$.

Proposición 1.21. Si p es un primo y a, b son enteros tales que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.

Demostración de Proposición 1.21 : Supongamos que p no divide a a ni a b . Cuando esto sucede, entonces p no es parte de la descomposición canónica de a y b , por lo tanto, p no es parte de la descomposición canónica de ab , lo cual contradice que $p \mid ab$ y así p divide a alguno de los dos números. ■

Notemos la importancia de que p sea primo de la proposición anterior, pues si fuese compuesto, existen casos en los que el resultado anterior no se cumple.

Ejemplo 1.22. Considerando al entero 36, es claro que 6 lo divide, sin embargo, $18 = 4 \cdot 9$, pero 6 no divide ni al 4 ni al 9.

Para 12, es claro que 2 lo divide y además $12 = 2 \cdot 6 = 3 \cdot 4 = 1 \cdot 12$, vemos que en todos los casos 2 divide a alguno de los factores.

Ejemplo 1.23. Sean p y q números primos distintos mayores a 2, demuestra que si $p \mid q^2 + q$, entonces $p < q$.

Puesto que $q^2 + q = (q + 1)q$, entonces si $p \mid (q + 1)q$, se sigue que $p \mid q$ ó $p \mid q + 1$. El primer caso es imposible por definición de número primo y necesariamente $p \mid q + 1$. De lo anterior, se tiene que $p \leq q + 1$, si $p = q + 1$, entonces como $q > 2$, se sigue que $q + 1$ debe de ser par lo cual contradice que p es un primo mayor que 2 y $p < q + 1$. El entero más grande que es menor a $q + 1$ es precisamente q , sin embargo, $p \neq q$ y así $p < q$ como se quería demostrar.

Teorema 1.24. Existen infinitos números primos.

Demostración de Teorema 1.24 : Supongamos que no es así y que existen exactamente k primos distintos a los cuales denotaremos por p_1, p_2, \dots, p_k . Al considerar al entero $p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$, por el inciso (v) de la Proposición 1.3, este número no es múltiplo de ninguno de los primos p_1, \dots, p_k y además tampoco es primo (de lo contrario contradice que solo hay k primos), por lo que existe un entero a menor a $p_1 \cdot \dots \cdot p_k + 1$ que lo divide y más aún, a no es ninguno de los primos p_1, \dots, p_k , por lo que la descomposición canónica de a no incluye a ningún primo, lo cual implica que $a = 1$ y así los únicos divisores de $p_1 \cdot \dots \cdot p_k + 1$ menores a él es el 1, lo cual implica que es primo y se llega a una contradicción. Por lo tanto, existen infinitos primos. ■

Proposición 1.25. Sea a un entero y $a = p_1^{q_1} \cdot p_2^{q_2} \cdot \dots \cdot p_k^{q_k}$ su descomposición canónica, entonces si $b \mid a$, el entero b es de la forma $b = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$ con $0 \leq r_j \leq q_j$ para $j = 1, 2, \dots, k$.

La demostración queda como ejercicio moral para el lector. *Hint:* La validez del resultado se da gracias al inciso (ii) de la Proposición 1.3.

Ejemplo 1.26. Sea $a = 540$, y $b = 18$, se verifica que

$$a = 540 = 2^2 \cdot 3^3 \cdot 5, \text{ y además } b \mid a \text{ donde } b = 2 \cdot 3^3 \cdot 5^0$$

Para ello, recordar que para x un número distinto de 0, se cumple que $x^0 = 1$.

2 Criterios de Divisibilidad

En este siguiente apartado se mostrarán ciertas condiciones que un número entero necesita para garantizar que es múltiplo de algún otro entero a los cuales llamaremos criterios de divisibilidad y se presentará la demostración de un solo criterio, ya que la demostración de las demás son muy similares.

Lema 2.1. *Un entero a es divisible entre 2 si y sólo si, la última cifra de a es múltiplo de 2.*

Lema 2.2. *El entero a es múltiplo de 3 si y sólo si la suma de las cifras de a es múltiplo de 3.*

Lema 2.3. *El entero a es divisible entre 4 si y sólo si las últimas dos cifras de a es un múltiplo de 4.*

Lema 2.4. *Un entero a es múltiplo de 5 si y sólo si a termina en 0 ó 5.*

Lema 2.5. *Un entero a es múltiplo de 6 si y sólo si a es múltiplo de 2 y de 3.*

Lema 2.6. *El entero a es divisible entre 8 si y sólo si las últimas tres cifras de a son múltiplo de 8.*

Lema 2.7. *El entero a es múltiplo de 9 si y sólo si la suma de las cifras de a es múltiplo de 9.*

Lema 2.8. *Un entero a es múltiplo de 10 si y sólo si a termina en 0.*

Lema 2.9. *Un entero a es múltiplo de 11 si y sólo si la diferencia de la suma de las cifras en posición impar de a menos la suma de las cifras en posición par de a es divisible por 11.*

Ejemplo 2.10. *Sea el entero 1386 usando solo los criterios de divisibilidad se pueden hacer las siguientes observaciones:*

1. 1386 es múltiplo de 2, pues el número termina en 6.
2. 1386 es múltiplo de 9, pues $1 + 3 + 8 + 6 = 18$ y 18 es múltiplo de 9 (y también de 3, por lo que 3 también lo divide).
3. De las dos observaciones anteriores, 1386 es múltiplo de 6.
4. 1386 no es múltiplo de 4, pues $4(21) < 86 < 4(22)$, es decir, 4 no divide a 86 y por tanto tampoco a 1386.
5. 1386 no es divisible entre 5, pues el número en cuestión no termina en 0 ni en 5.
6. 1386 es múltiplo de 11, pues $(1 + 8) - (3 + 6) = 9 - 9 = 0$ el cual es múltiplo de 11.

Demostración de Lema 2.7 : Sea a algún entero positivo, podemos escribir a a en su representación decimal y así

$$a = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10a_1 + a_0.$$

Donde n es un entero no negativo y los números a_0, a_1, \dots, a_{n-1} son enteros entre el 0 y el 9, mientras que a_n está entre 1 y 9. Puesto que $10 = 1 + 9$, se observa que

$$\begin{aligned} a &= (9 + 1)10^{n-1}a_n + (9 + 1)10^{n-2}a_{n-1} + \dots + (9 + 1)a_1 + a_0 \\ &= (9 \cdot 10^{n-1}a_n + 10^{n-1}a_n) + \dots + (9a_1 + a_1) + a_0 \\ &= 9(10^{n-1}a_n + \dots + a_1) + (10^{n-1}a_n + \dots + 10a_2) + a_1 + a_0 \\ &= \dots = 9(10^{n-1}a_n + \dots + a_1 + 10^{n-2}a_n + \dots + a_n) + (a_n + a_{n-1} + \dots + a_1 + a_0). \end{aligned}$$

Es decir, al repetir el truco de la primera igualdad n veces, entonces se tiene un múltiplo de 9 junto la suma de las cifras de 9 y así a es múltiplo de 9 solo cuando $a_n + \dots + a_0$ es divisible entre 9. En el caso de a un entero negativo, basta con considerar a $-a$ y luego cambiar el signo. ■

El Lema 2.5 se puede pensar incluso como resultado inmediato de los criterios del 2 y del 3. De hecho, a partir de estos criterios se pueden deducir criterios para números más grandes y a continuación se presentan algunos de ellos.

Corolario 2.11. *Un entero n es múltiplo de 12 si y sólo si n es múltiplo de 3 y 4.*

Corolario 2.12. *Un entero n es múltiplo de 10^m para m entero positivo, si y sólo si las últimas m cifras de n son todas 0.*

Corolario 2.13. *El entero n es múltiplo de 36 si y sólo si n es múltiplo de 4 y de 9.*

Nota 2.14. *Es importante tener cuidado al combinar criterios para crear otro, pues no siempre es verdadero. Por ejemplo, uno podría deducir que un número n es múltiplo de 8 si y sólo si n es múltiplo de 2 y de 4, lo cual no es cierto, pues 36 es múltiplo de 2 y de 4, pero 8 no lo divide. ¿Puedes deducir que condiciones se necesitan para crear otro criterio?*

3 Ejercicios

La siguiente lista de ejercicios propuestos no siguen ningún orden de dificultad particular.

Ejercicio 3.1. Demuestra los siguientes enunciados:

- (i) La suma de dos números pares es también un número par.
- (ii) La suma de un número impar con un par, es un número impar.
- (iii) La suma de dos números impares es un número par.
- (iv) El producto de un número par con cualquier otro entero es otro número par.

Ejercicio 3.2. Demuestra que no se puede escribir a ningún número impar como combinación lineal de 6 y 8.

Ejercicio 3.3. Determina si 7 divide a $371^4 - 41^4$. Justifica tu respuesta.

Ejercicio 3.4. Sea n un entero. Demuestra que $24 \mid n(n+1)(n+3)(n+4)$.

Ejercicio 3.5. Encuentra todos los primos $p > q$ tales que $p+q$ y $p-q$ son números primos también.

Ejercicio 3.6. ¿Será posible escribir al 100 como combinación lineal de 12 y 18? Justifica tu respuesta.

Ejercicio 3.7. Sea N un dígito, considera al número

$$M = \underbrace{2022N2022N\dots2022N}_{5 \cdot 2022}.$$

Encuentra todos los valores de N tales que M es múltiplo de 7 y demuestra que siempre es múltiplo de 33.

Ejercicio 3.8. ¿Cuál es el factor primo más grande de $3^{12} - 1$?

Ejercicio 3.9. Usa la Proposición 1.10 para demostrar que si n es un natural impar, entonces $a+b \mid a^n + b^n$.

Ejercicio 3.10. Sea a un entero que satisface la ecuación $5^{2022} + a = 4^{1011}$, demuestra que $3 \mid a$.

Ejercicio 3.11. Encuentra una lista de 5 números primos distintos, tales que la diferencia entre cualesquiera dos términos consecutivos de la lista sea 6 y demuestra que esta lista es única.

Ejercicio 3.12. Demuestra que para x y y enteros positivos, entonces $19^x - 5^y$ es múltiplo de 7 si y sólo si $x - y + 1$ es múltiplo de 7 ó cuando $x = y$.

Ejercicio 3.13. Encuentra todos los primos p tal que exista a entero que cumpla que $p \mid a^2 + 1$, $p \mid a^3 + 1$ y $p \mid a^4 + 1$.

Ejercicio 3.14. Encuentra todos los primos p, q, r tales que $p > q > r$ y que cumplen que $p - q$, $q - r$ y $p - r$ son primos.

Ejercicio 3.15. Demuestra el criterio de divisibilidad del 11.

Ejercicio 3.16. Si se forma al entero N juntando a los números del 19 al 93 de la siguiente forma

$$N = 19202123\dots919293.$$

Encuentra la máxima potencia de 3 que divide a N .

Ejercicio 3.17. ¿Entre qué números del 1 al 12 es divisible $\frac{10^{601}-10}{9}$?

Ejercicio 3.18. Demuestra que si $3 \nmid n$, entonces $3 \mid n^2 - 1$ para n entero.

Ejercicio 3.19. Considera al entero positivo

$$\underbrace{123123123\dots123123^2}_{300} - 41^2.$$

Demuestra que es múltiplo de 328.

Ejercicio 3.20. Sea p algún número primo, y d el producto de todos los primos menores o iguales a p . Determina si $d + 1$ es primo y justifica tu respuesta.

Ejercicio 3.21. Para cualesquiera enteros n y $m > 1$, demuestra que existe k entre 0 y $n - 1$, tal que $n - k$ es múltiplo de m .

Ejercicio 3.22. Encuentra todos los primos positivos p para los cuales el número $p^2 + 77$ tiene exactamente 5 divisores.

Ejercicio 3.23. Demuestra que un entero n es múltiplo de 2^m con m entero positivo, si y sólo si las últimas m cifras de n es múltiplo de 2^m

Ejercicio 3.24. Encuentra un criterio de divisibilidad para 1001 que sea práctico.

Ejercicio 3.25. Sean a, b, c, d y n enteros positivos y p un primo tales que $p \mid a^c - b^d$, entonces $p \mid a^{cn} - b^{dn}$.

Ejercicio 3.26. Probar que para cualquier entero positivo n , se tiene que

$$(n^3 - n)(5^{8n+4} + 3^{4n+2})$$

es múltiplo de 3804. (Hint: utiliza el problema anterior)

Ejercicio 3.27. ¿Existen enteros positivos n para los cuales el número $n!$ termine en exactamente 5 ceros? (Recordar que $n! = 1 \times 2 \times 3 \times \dots \times (n - 1) \times n$.)

Ejercicio 3.28. En una fila para la entrada al teatro, hay 10240 personas. El vendedor decide atender uno no, uno sí, uno no, etc. A aquellos que no atiende se regresan al final de la fila (uno por uno, en orden). ¿En qué lugar estaba inicialmente formado el último cliente que atienden?

Ejercicio 3.29. Sean p y q primos tales que $p < q$. Demuestra que $pq \nmid p^2 + pq + 6q - 1$.

Ejercicio 3.30. ¿Para cuántos enteros n del 1 al 10 000 se tiene que $2^n - n^2$ es múltiplo de 5?