Divisibilidad

Ezra Guerrero Alvarez

30 de diciembre del 2022

1 Introducción

La teoría de números es un área muy estudiada y divertida de la matemática. Concierne el estudio de los enteros y porque se comportan como observamos y lleva a resultados muy profundos y sorprendentemente aplicables. Por ello, es crucial comenzar con buenos fundamentos de esta área tan importante.

2 Los naturales y divisibilidad

Todos estamos familiarizados con el conjunto de los números naturales:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Estos forman las bases de todo lo que haremos con teoría de números. Nos permiten sumar, multiplicar, contar, etc. De manera importante, tienen un orden asignado, en particular $0 < 1 < 2 < \ldots$. Naturalmente, extendemos los naturales a los enteros

$$\mathbb{Z} = \mathbb{N} \cup \{-1, -2, -3, \ldots\}.$$

Estos nos permiten restar al igual que sumar. Ahora, podemos introducir uno de los conceptos más importantes de toda la teoría de números: la divisibilidad.

Definición 1: Divisibilidad

Sean m, n enteros. Decimos que n es divisible entre m, o que m divide a n si existe un entero k tal que $n = km$. A n se le llama un múltiplo de m y a m un divisor o factor de n.

Cuando m divide a n, escribimos $m \mid n$ (leído "m divide a n"). Algunas propiedades básicas de la divisibilidad son las siguientes:

- Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.
- Si $a \mid b$ y $b \neq 0$ entonces $|a| \leq |b|$.
- Se cumple que $a \mid b$ si y solo si $ac \mid bc$.
- Si $a \mid b$ y $a \mid c$ entonces $a \mid bx + cy$ para todo par de enteros (x, y).

Ejercicio 1. Demuestre todas estas propiedades.

Ahora, no siempre va a ser el caso que $m \mid n$. Sin embargo, podemos emplear una generalización de la división para obtener un resultado sumamente útil para cualquier par de enteros positivos:

Lema 1: Algoritmo de la División

Sean m y n dos enteros positivos. Existe un **único** par de enteros no-negativos (q, r) tal que

$$n = m \cdot q + r$$

y $0 \leq r < m$.

Demostración. Demostramos que tal pareja existe. Si $n < m$, entonces podemos escoger $(q, r) = (0, n)$. De lo contrario, supongamos que $n \geq m$. Ahora bien, por el ordenamiento de los naturales, sabemos que existe un q tal que $mq \leq n$ y $m(q+1) > n$. Entonces, podemos escoger $(q, r) = (q, n - mq)$, pues la segunda desigualdad implica que $n - mq < m$. ■

Ejercicio 2. Demuestre que esta pareja es única.

Ahora, a veces nos interesa cuando dos números comparten divisores. Para m, n enteros positivos, llamamos d un divisor común de m y n si $d \mid m$ y $d \mid n$. Notemos que 1 siempre es un divisor común.

Definición 2: Máximo Común Divisor

Definimos $\gcd(m, n)$ como el máximo divisor común de m y n. Si $\gcd(m, n) = 1$, decimos que m y n son coprimos o primos relativos y escribimos $m \perp n$.
Nota: ¡¡La notación $m \perp n$ no es estándar!! Asegúrense de definir como la están usando para así evitar problemas.

Ejercicio 3. Sea d un divisor común de m y n. Demuestra que $d \mid \gcd(m, n)$.

Una forma muy útil de encontrar el máximo común divisor de dos números es el siguiente algoritmo:

Lema 2: Algoritmo de Euclides

Dados dos enteros positivos $m > n$, el siguiente algoritmo crea una secuencia de enteros no negativos $a_0, a_1, \ldots$:
Sean $a_0 = m$ y $a_1 = n$. Para $k \geq 2$,

$$\begin{cases} \text{Si } a_{k-1} = 0, & \text{entonces el algoritmo termina.} \\ \text{De lo contrario,} & a_k \text{ es el residuo al dividir } a_{k-2} \text{ por } a_{k-1}. \end{cases}$$

Este algoritmo siempre termina y el penúltimo término de la secuencia (el último que no es 0) es igual a $\gcd(m, n)$.

Demostración. Demostramos que $a_0 > a_1 > a_2 > \ldots$. Como los a_i son enteros no negativos, esta secuencia no puede decrecer por siempre, así que eventualmente tenemos un r tal que $a_{r+1} = 0$. Procedemos por inducción. Primero, notemos que $m > n$, así que $a_0 > a_1$. Este es nuestro caso base. Ahora, supongamos que $a_0 > a_1 > \ldots > a_k$. Tenemos que a_{k+1} es el residuo al dividir a_{k-1} por a_k. Por el algoritmo de la división sabemos que $a_{k+1} < a_k$, así que $a_0 > \ldots > a_k$. Esto concluye la inducción.
Ahora, como $a_{r+1} = 0$, sabemos que $a_r \mid a_{r-1}$. Ahora, como $a_{r-2} = q \cdot a_{r-1} + a_r$ por el algoritmo de la división, vemos que $a_r \mid a_{r-2}$ también. Continuando de esta manera, observamos que $a_r \mid a_{r-3}, \ldots, a_1, a_0$. Ahora, supongamos que d es un divisor común de m y n. Notemos que $d \mid a_2$. De hecho, podemos ver que $d \mid a_k$ para todo k en la secuencia. Entonces, $d \mid a_r$. Entonces, vemos que $\gcd(m, n) \mid a_r$. Sin embargo, a_r es un divisor común de m y n, así que $a_r \mid \gcd(m, n)$. Sigue que $a_r = \gcd(m, n)$, como buscábamos demostrar. ■

Ejercicio 4. Demuestra que existen enteros x y y tales que $a_r = mx + ny$.

Lema 3: Lema de Bezout

El máximo común divisor de m y n es el mínimo elemento positivo del conjunto

$$\{mx + ny \mid x, y \in \mathbb{Z}\}.$$

Demostración. Sea d un elemento positivo del conjunto. Como $\gcd(m,n) \mid m, n$ sabemos que $\gcd(m,n) \mid d$, así que $\gcd(m,n) \leq d$. Ahora, como $\gcd(m,n)$ pertenece al conjunto, sigue que debe ser el mínimo elemento positivo que le pertenece. ■

3 Irreducibles y Primos

3.1 Irreducibles

Llamamos a un entero positivo p *irreducible* si y solo si tiene exactamente dos divisores positivos. Talvez están más acostumbrados a llamar a estos números primos, pero olviden su experiencia previa por el momento. De hecho, el nombre ”irreducible” tiene mucho más sentido con esta definición.

Lema 4: Siempre hay un factor irreducible

Para todo entero positivo $n > 1$, existe un irreducible p tal que $p \mid n$.

Demostración. Es crucial que $n \neq 1$. Procedemos por inducción fuerte. Nuestro caso base es $n = 2$, el cual es irreducible. Ahora, supongamos que para todo $1 < n < k$ existe un irreducible p tal que $p \mid n$. Si k es irreducible terminamos. De lo contrario, por definición debe tener exactamente un divisor o al menos tres. Notemos que 1 y k siempre dividen k. Como $k > 1$, estos son distintos, entonces k tiene al menos tres factores. Sea n uno de ellos. Como $n \mid k$, tenemos $n \leq k$. Además, $n \neq 1, k$ así que $1 < n < k$. Por la hipótesis inductiva sigue que n tiene un divisor irreducible p. Pero entonces $p \mid n \mid k$ es un divisor irreducible de k. Esto concluye la inducción. ■

Ejercicio 5. Demuestre que todo entero positivo mayor a 1 tiene un divisor irreducible p con $p \leq \sqrt{n}$.

Ejercicio 6. Demuestre que existen infinitos enteros positivos irreducibles.

Podemos combinar nuestro conocimiento de irreducibles y el Lema de Bezout. Sea p un irreducible y a un entero tal que $p \nmid a$. ¿Cuáles factores pueden compartir p y a? Como p es irreducible, solo pueden ser 1 y p. Sin embargo, como $p \nmid a$, sabemos que p no es un divisor de a. Por ende, p y a solo comparten uno como factor, así que son coprimos. Como $p \perp a$, el Lema de Bezout nos indica que existen eneteros x, y tales que $px + ay = 1$.

3.2 Primos

Talvez se preguntarán porque no hemos definido los números anteriores como primos. El motivo es el siguiente:

Definición 3: Primos

Un entero positivo $p > 1$ es primo si y solo si se cumple que $p \mid ab$ implica que $p \mid a$ o $p \mid b$.

Esta es la definición de un número primo y es una propiedad que *nunca* se les debe olvidar. ¿Porqué entonces estamos acostumbrados a definir los primos como irreducibles?

Ejercicio 7. Demuestra que p es irreducible si y solo si es primo.

Teorema 1: Teorema Fundamental de la Aritmética

Para todo entero $n > 1$ existe un único conjunto de primos $\{p_1, p_2, \ldots, p_\omega\}$ y secuencia de enteros positivos $\alpha_1, \alpha_2, \ldots, \alpha_\omega$ tal que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\omega^{\alpha_\omega}.$$

De manera equivalente, si $p_1, p_2, \ldots$ es la secuencia creciente de primos, entonces para todo entero $n > 1$ existe una única secuencia infinita de enteros no negativos $\alpha_1, \alpha_2, \ldots$ tal que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

4 Conclusión

Es esencial tener estas herramientas básicas de teoría de números en mente, pues son estos fundamentos los cuales nos llevan a todos los resultados importantes y a resolver problemas. Todos los lemas mencionados son de suma importancia y un estudio de la teoría de números no estaría completo sin estar cómodos con estos conceptos primeros.