Aritmética Modular

Ezra Guerrero Alvarez

31 de diciembre del 2022

1 Introducción

Para simplificar el trabajo de lidiar con relaciones de divisibilidad, introducimos la aritmética modular. A través de este folleto, denotamos por $m \perp n$ que los enteros m y n son coprimos.

2 Congruencia Modular

Decimos que dos enteros a, b son congruentes módulo m si y solo si $m \mid a - b$. En tal caso, escribimos

$$a \equiv b \pmod{m}.$$

Notemos que $m \mid n$ si y solo si $n \equiv 0 \pmod{m}$. La clave de estas congruencias es que se comportan muy parecido a la igualdad.

Lema 1: Propiedades de la Congruencia Modular

- (Reflexividad) $a \equiv a \pmod{m}$.
- (Simetría) $a \equiv b \pmod{m}$ si y solo si $b \equiv a \pmod{m}$.
- (Transitividad) Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$.
- (Aritmética) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a + c \equiv b + d \pmod{m}$ y $ac \equiv bd \pmod{m}$.
- (División) Si $an \equiv bn \pmod{m}$, entonces $a \equiv b \pmod{\frac{m}{\gcd(m,n)}}$. En particular, si $m \perp n$, $an \equiv bn \pmod{m}$ implica $a \equiv b \pmod{m}$.

Ejercicio 1. Demuestra estas propiedades.

La propiedad de multiplicación es particularmente útil, pues nos dice que si $a \equiv b \pmod{m}$, entonces $a^n \equiv b^n \pmod{m}$ para todo n entero positivo. Esto nos permite simplificar muchos cálculos. Por ejemplo, notamos que $(m-1)^2 \equiv (-1)^2 \equiv 1 \pmod{m}$ sin tener que expandir ninguna expresión.

3 Primos

Cuando nuestro módulo es primo, trabajar con aritmética modular es muy conveniente. La explicación matemática tras esto es que los enteros módulo p forman lo que se conoce como un campo o cuerpo. Piensen que un campo es una estructura matemática que se comporta como los reales o los racionales. En este sentido, veremos que la aritmética módulo un primo es muy parecida.

La propiedad más importante de tener un módulo primo se ve con el siguiente lema:

Lema 2: Inversos módulo p

Sea p un primo y a un entero tal que $p \nmid a$. Entonces, existe un entero x tal que $ax \equiv 1 \pmod{p}$. Llamamos a x un inverso módulo p de a. Además, si x, x' son inversos módulo p de a, entonces $x \equiv x' \pmod{p}$. Usualmente denotamos a el inverso módulo p de a entre 0 y p como a^{-1}.

Demostración. Como $p \nmid a$ y p es primo, sigue que $p \perp a$. Entonces, por el Lema de Bezout, existen enteros x, y tales que $ax + py = 1$. Viendo esta expresión módulo p, vemos que

$$1 \equiv ax + py \equiv ax \pmod{p}$$

y x es un inverso módulo p de a. Ahora, supongamos que x, x' son dos inversos módulo p de a. Entonces,

$$x \equiv x \cdot 1 \equiv x \cdot ax' \equiv xa \cdot x' \equiv 1 \cdot x' \equiv x' \pmod{p},$$

como deseábamos demostrar. ■

Corolario. (Propiedad del Producto Nulo) Si $ab \equiv 0 \pmod{p}$, entonces $a \equiv 0 \pmod{p}$ o $b \equiv 0 \pmod{p}$.

Observemos que el lema anterior no se cumple si p no es primo. Por ejemplo, no existe un x tal que $2x \equiv 1 \pmod{4}$, y podemos verificar esto rápidamente por paridad. Además, ¡la Propiedad del Producto Nulo ya no tiene porque cumplirse! Por ejemplo, $2 \cdot 3 \equiv 0 \pmod{6}$ pero ni 2 ni 3 son congruentes a $0 \pmod{6}$.

Ahora, veamos uno de los resultados más importantes de la teoría de números:

Teorema 1: Pequeño Teorema de Fermat

Sea p un primo y a un entero. Se cumple que

$$a^p \equiv a \pmod{p}.$$

Demostración. Basta demostrarlo para $a \in \{0, 1, \ldots, p-1\}$. Si $a = 0$ esto es claramente cierto. Entonces, supongamos que $a > 0$, tal que $a \perp p$. Consideremos los números $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$. Notemos que hay exactamente $p-1$ de ellos. Además, si $a \cdot i \equiv a \cdot j \pmod{p}$, como $a \perp p$, podemos multiplicar por a^{-1} ambos lados y obtener $i \equiv j \pmod{p}$. Como $0 < i, j < p$, seguiría que $i = j$. Entonces, Estos $p-1$ números son distintos por parejas módulo p. Por ende, al reducir módulo p, formarán una permutación de $1, 2, \ldots, p-1$. Entonces, si los multiplicamos todos, vemos que

$$a^{p-1}(p-1)! \equiv a \cdot 1 \cdot a \cdot 2 \cdots a \cdot (p-1) \equiv 1 \cdot 2 \cdots (p-1) \equiv (p-1)! \pmod{p}.$$

Ahora, como $p \nmid (p-1)!$, sabemos que tiene un inverso módulo p. Multiplicando por el inverso de $(p-1)!$, encontramos que $a^{p-1} \equiv 1 \pmod{p}$. Esto implica el resultado. ■

Como vemos en la demostración anterior, multiplicar por el inverso se siente idéntico a dividir. Podemos formalizar esta idea y traer los racionales al mundo de la aritmética modular. Es *clave* que estaremos trabajando con un módulo primo en lo que sigue.

Denotamos al inverso módulo p de x por $\frac{1}{x}$. De esta manera, $\frac{x}{y}$ representa el entero tal que $y \cdot \frac{x}{y} \equiv x \pmod{p}$.

Lema 3: Los inversos se comportan como racionales

Con la notación anterior,

$$\frac{a}{b} + \frac{c}{d} \equiv \frac{ad + bc}{bd} \pmod{p}.$$

Demostración. Deseamos demostrar que $\frac{a}{b} + \frac{c}{d}$ es el entero tal que si lo multiplicamos por bd obtenemos $ad + bc$. Para esto, consideremos el producto $bd\left(\frac{a}{b} + \frac{c}{d}\right)$. Por la propiedad distributiva y definición de inversos, vemos que este producto es igual a

$$bd \cdot \frac{a}{b} + bd \cdot \frac{c}{d} = ad + bc,$$

tal como buscábamos demostrar. ■

Este lema nos permite tratar a los inversos tal como si fueran fracciones sin perdida de rigor.

4 Conclusión

La aritmética modular es una herramienta muy poderosa para lidiar con problemas de teoría de números. Cualquier entero positivo como módulo puede resultar útil, pero cuando utilizamos un número primo, ganamos estructura extra de la cual nos podemos aprovechar.