El Anillo de Enteros Módulo n

Alan Reyes-Figueroa

Teoría de Números (Aula 10) 16.agosto.2022

Ya mencionamos que la congruencia módulo n, induce una relación de equivalencia sobre $\mathbb{Z}$. De hecho, mostramos que dos enteros $a, b \in \mathbb{Z}$ son congruentes módulo n si, y sólo si, dejan el mismo residuo r al dividirse dentro de n. Así, las clases de equivalencia módulo n son de la forma $n\mathbb{Z} + r$, con $0 \leq r < n$.

Esto muestra que hay exactamente n clases de equivalencia, que podemos denotarlas como

$$n\mathbb{Z} + 0, \quad n\mathbb{Z} + 1, \quad n\mathbb{Z} + 2, \quad \ldots, \quad n\mathbb{Z} + (n-1).$$

Si $\sim$ denota la relación de congruencia módulo n, entonces el cociente,

$$\mathbb{Z}/\sim \quad = \{\text{clases de equivalencia módulo } n\} = \{n\mathbb{Z} + r,\ 0 \leq r < n\},$$

posee una estructura de anillo, heredada a partir de $\mathbb{Z}$.

Denotamos este cociente por $\mathbb{Z}/n\mathbb{Z}$, (también se denota por $\mathbb{Z}/(n)$, $\mathbb{Z}/n$, $\mathbb{Z}_n$). $\mathbb{Z}/n\mathbb{Z}$ será llamado el **anillo de enteros módulo** n.

El Anillo $\mathbb{Z}/n\mathbb{Z}$

Como recordarán de sus cursos de álgebra, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ posee una estructura de anillo, con las operaciones

$$(n\mathbb{Z}+a)+(n\mathbb{Z}+b) = n\mathbb{Z}+(a+b \pmod n), \qquad (n\mathbb{Z}+a)\cdot(n\mathbb{Z}+b) = n\mathbb{Z}+(ab \pmod n).$$

En ocasiones, es más simple representar la clase $n\mathbb{Z}+r$ por su residuo $\bar{r}$. Las operaciones anteriores resultan

$$\bar{a}+\bar{b} = \overline{a+b}, \qquad \bar{a}\cdot\bar{b} = \overline{ab}.$$

Ejemplo: $\mathbb{Z}/6\mathbb{Z}$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

El Anillo $\mathbb{Z}/n\mathbb{Z}$

En general, $\mathbb{Z}/n\mathbb{Z}$ es un anillo conmutativo con unidad, esto es, es conmutativo, posee elemento neutro aditivo $\bar{0} = n\mathbb{Z}$, y posee un elemento identidad multiplicativo $\bar{1} = n\mathbb{Z} + 1$.

Sin embargo, en general no todo los elementos de $\mathbb{Z}/n\mathbb{Z}$ son invertibles.

Proposición

Sea $a, n \in \mathbb{Z}$, $n > 1$. Existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$ si, y sólo si, $(a, n) = 1$. En otras palabras, a es invertible módulo n, si y sólo si, es primo relativo con n.

Prueba: Por el coroloario al Lema de Bézout, tenemos la siguiente cadena de equivalencias:

$$\begin{aligned} ab \equiv 1 \pmod{n} &\iff n \mid ab - 1 \\ &\iff ab - 1 = nk \iff ab - nk = 1 \\ &\iff (a, n) = 1. \quad \square \end{aligned}$$

Diremos entonces que a es **invertible módulo** n, cuando $(a, n) = 1$. En ese caso, existe

$b \in \mathbb{Z}$ tal que $ab \equiv 1$, y diremos que $b \pmod{n}$ es el **inverso módulo** n de a.

Este inverso es único (módulo n), pues si $ab \equiv 1, ab' \equiv 1 \pmod{n}$, entonces

$$b \equiv b \cdot 1 \equiv b(ab') \equiv (ba)b' \equiv (1)b' \equiv b' \pmod{n}.$$

Así, el inverso está bien definido, y tenemos que $\bar{a} \cdot \bar{1} = \bar{1} \;\Rightarrow\; \bar{a}^{-1} = \bar{b}$.

Definición

*El **grupo de unidades módulo** n, denotado por $(\mathbb{Z}/n\mathbb{Z})^*$ o por $U(n)$, se define como*

$$U(n) = (\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \; (a, n) = 1\}.$$

Obs! Note que $U(n)$ es un grupo multiplicativo: si $\bar{a}, \bar{a'} \in U(n)$, existen $b, b' \in \mathbb{Z}$ tales que $ab \equiv 1 \pmod{n}$ y $a'b' \equiv 1 \pmod{n}$. Luego, $(aa')(bb') \equiv (ab)(a'b') \equiv 1 \cdot 1 \equiv 1 \pmod{n}$, y se tiene que $\overline{aa'} \in U(n)$.

Ejemplo El grupo de unidades módulo 15, $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ tiene la estructura

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{7}$	$\bar{8}$	$\bar{11}$	$\bar{13}$	$\bar{14}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{14}$	$\bar{1}$	$\bar{7}$	$\bar{11}$	$\bar{13}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{1}$	$\bar{13}$	$\bar{2}$	$\bar{14}$	$\bar{7}$	$\bar{11}$
$\bar{7}$	$\bar{7}$	$\bar{14}$	$\bar{13}$	$\bar{4}$	$\bar{11}$	$\bar{2}$	$\bar{1}$	$\bar{8}$
$\bar{8}$	$\bar{8}$	$\bar{1}$	$\bar{2}$	$\bar{11}$	$\bar{4}$	$\bar{13}$	$\bar{14}$	$\bar{7}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{14}$	$\bar{2}$	$\bar{13}$	$\bar{1}$	$\bar{8}$	$\bar{4}$
$\bar{13}$	$\bar{13}$	$\bar{11}$	$\bar{7}$	$\bar{1}$	$\bar{14}$	$\bar{8}$	$\bar{4}$	$\bar{2}$
$\bar{14}$	$\bar{14}$	$\bar{13}$	$\bar{11}$	$\bar{8}$	$\bar{7}$	$\bar{4}$	$\bar{2}$	$\bar{1}$

Propiedad

El anillo $\mathbb{Z}/n\mathbb{Z}$ es un cuerpo, si y sólo si, $n = p$ es primo. En ese caso $U(n) = (\mathbb{Z}/p\mathbb{Z})^*$.

El Anillo $\mathbb{Z}/n\mathbb{Z}$

Prueba: ($\Leftarrow$) Si $n = p$ es primo, entonces $(a, p) = 1$, para todo $1 \leq a < p$. Así, todo elemento $a \neq \bar{0}$ en $\mathbb{Z}/p\mathbb{Z}$ es invertible, y $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo de números.

($\Rightarrow$) Si $\mathbb{Z}/n\mathbb{Z}$ es cuerpo, todo elemento $a \neq \bar{0}$ es invertible, y $(a, n) = 1$, para todo $1 \leq a < n$. Pero esto es equivalente a n ser primo. $\square$

Teorema ("Sueño de todo estudiante")

Sea p primo. Entonces, para cualesquiera $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$, vale

$$(\bar{a} + \bar{b})^p \equiv \bar{a}^p + \bar{b}^p \pmod{p}.$$

Prueba: Si $0 < k < p$, entonces $\binom{p}{k} = \frac{p!}{k!(p-k)!} \equiv 0 \pmod{p}$, pues hay un factor p en el numerador queno puede cancelarse con nada en el denominador. Del Teorema de Binomio, tenemos

$$(a + b)^p = \sum_{0 \leq k \leq p} \binom{p}{k} a^k b^{p-k} \equiv a^p + b^p \pmod{p}. \quad \square$$

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Veremos una primera aplicación de los inversos multiplicativos módulo n.

Lema

Si p es primo, entonces las únicas soluciones de $x^2 \equiv 1 \pmod{p}$ son $\bar{1}$ y $\overline{-1}$. En particular, si $x \in U(p) - \{\pm\bar{1}\}$, entonces $x^{-1} \not\equiv x \pmod{p}$.

<u>Prueba</u>:

$$\begin{aligned} x^2 \equiv 1 \pmod{p} \quad &\Longleftrightarrow \quad p \mid x^2 - 1 = (x-1)(x+1) \\ &\Longleftrightarrow \quad p \mid (x-1) \text{ ó } p \mid (x+1) \\ &\Longleftrightarrow \quad x \equiv 1 \pmod{p} \text{ ó } x \equiv -1 \pmod{p}. \end{aligned}$$

La segunda afirmación es inmediata a partir del hecho $1 \equiv x^2 \;\Leftrightarrow\; x^{-1} \equiv x \pmod{p}$. $\square$

Teorema (Teorema de Wilson)

Sea $n > 1$. Entonces, $n \mid (n-1)! + 1$ si, y sólo si, n es primo. Más precisamente

$$(n-1)! \equiv \begin{cases} -1 \pmod{n}, & \text{si } n \text{ es primo;} \\ 0 \pmod{n}, & n \text{ compuesto, } n \neq 4. \end{cases}$$

UNIVERSIDAD DEL VALLE DE GUATEMALA

<u>Prueba</u>: Si n es conpuesto, pero no es cuadrado de un primo, podemos escribir $n = ab$, con $1 < a < b < n$. En este caso, tanto a y b son factores de $(n-1)!$, y tendríamos que $(n-1)! \equiv 0 \pmod{n}$.

Si $n = p^2$, con p primo, $p > 2$, entonces p y $2p$ son factores de $(n-1)!$, y de nuevo $(n-1)! \equiv 0 \pmod{n}$.
Esto muestra que para todo $n \neq 4$, compuesto, se tiene que $(n-1)! \equiv 0 \pmod{n}$.

Si $n > 2$ es primo, podemos escribir $(n-1)! = 2 \cdot 3 \cdot \ldots (n-1)$. Por el lema anterior, los números $2, 3, \ldots, n-2$, no son su propio inverso, y podemos agruparlos en pares (inversos entre sí), sobrando únicamente el termino $n-1$ el cual es su propio inverso módulo n. Así

$$(n-1)! \equiv 1 \cdot 2 \cdot 3 \ldots \cdot (n-1) \equiv \prod_i (a_i a_i^{-1}) \cdot (n-1) \equiv \prod_i (1) \cdot (n-1) \equiv -1 \pmod{n}.$$

El caso $n = 2$ se verifica de forma difecta: $(2-1)! = 1! \equiv 1 \equiv -1 \pmod{2}$. $\square$

Teorema (Teorema de Wolstenhölme)

Sea $p > 3$ un número primo. Entonces el numerador de $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1}$, es divisible por p^2.

Prueba: Sumando en pares "extremos", obtenemos

$$\sum_{1\leq i<p} \frac{1}{i} = \sum_{i=1}^{(p-1)/2} \left(\frac{1}{i} + \frac{1}{p-i}\right) = \sum_{i=1}^{(p-1)/2} \frac{p}{i(p-i)} = p \sum_{i=1}^{(p-1)/2} \frac{1}{i(p-i)}.$$

El mmc de los números 1 a $p-1$ no es divisible por p. Basta entonces mostrar que el numerador de la última suma es divisible entre p, o equivalentemente, como $p \nmid (p-1)!$, debemos mostrar que el entero

$$S = \sum_{i=1}^{(p-1)/2} \frac{(p-1)!}{i(p-i)},$$

es un múltiplo entre p.

El Anillo $\mathbb{Z}/n\mathbb{Z}$

Para $1 \leq i \leq p-1$, denotamos por r_i el inverso de i módulo p, o sea, $ir_i \equiv 1 \pmod{p}$. Observe que $r_{p-i} \equiv -r_i \pmod{p}$, así

$$S \equiv \sum_{i=1}^{(p-1)/2} \frac{(p-1)!}{i(p-i)}\, ir_i\,(p-i)r_{p-i} \equiv \sum_{i=1}^{(p-1)/2} (p-1)!\, r_i r_{p-i} \equiv \sum_{i=1}^{(p-1)/2} (-1)(-r_i^2) \equiv \sum_{i=1}^{(p-1)/2} r_i^2 \pmod{p},$$

por el Teorema de Wilson.

Los r_i son congruentes a uno de los números $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$, de modo que r_i^2 es congruente a alguno de los números $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. Afirmamos que todos estos cuadrados aparecen en la suma. Si $r_i^2 r_j^2 \pmod{p}$, entonces $p \mid (r_i^2 - r_j^2) = (r_i - r_j)(r_i + r_j)$. Esto implica que $r_i \equiv \pm r_j \pmod{p}$. Multiplicando por ij, tenemos que $j \equiv \pm i \pmod{p} \Rightarrow i = j$, pues $1 \leq i, j \leq \frac{p-1}{2}$.

Portanto, $S \equiv \sum_{i=1}^{(p-1)/2} i^2 \equiv \frac{p(p^2-1)}{24} \equiv 0 \pmod{p}$, pues siendo $p > 3$, se tiene que $(p, 24) = 1$, y el resultado sigue. $\square$

El Anillo $\mathbb{Z}/n\mathbb{Z}$

El Teorema de Wilson produce resultados interesantes sobre los coeficientes binomiales.

Suponga que $h, k \in \mathbb{Z}^+$ son enteros positivos, con $h + k = p - 1$, p primo. Entonces

$$h!k! \equiv (-1)^h(p-1)(p-2)\cdots(p-h)k! \equiv (-1)^k(p-1)! \equiv (-1)^{k+1} \pmod{p},$$

por el Teorema de Wilson. De ahí que

$$\begin{aligned} h!k!\binom{p-1}{k} \equiv (p-1)! \pmod{p} \quad &\Longleftrightarrow \quad (-1)^{k+1}\binom{p-1}{k} \equiv -1 \pmod{p} \\ &\Longleftrightarrow \quad \binom{p-1}{k} \equiv (-1)^k \pmod{p}. \end{aligned}$$

Propiedad

Si $p > 3$ es primo, entonces $p^3 \mid \binom{2p}{p} - 2$.

Primeramente, recordamos algunas identidades de los coeicientes binomiales. Para todo $1 \leq i \leq p-1$, tenemos

$$\binom{p}{i} = \frac{p}{i}\binom{p-1}{i-1}.$$

De ahí,

$$\binom{2p}{p} = \binom{p}{0}^2 + \binom{p}{1}^2 + \ldots + \binom{p}{p}^2,$$

pues podemos elegir p objetos de entre $2p$ escogiendo i de ellos de entre los primeros p, y los $p-i$ restantes entre los últimos p, luego

$$\binom{2p}{p} = \sum_{i=0}^{p}\binom{p}{i}\binom{p}{p-i} = \sum_{i=0}^{p}\binom{p}{i}^2.$$

Usando estas identidades,

$$\binom{2p}{p} - 2 = \sum_{i=1}^{p-1}\frac{p^2}{i^2}\binom{p-1}{i-1}^2 = p^2\sum_{i=1}^{p-1}\frac{1}{i^2}\binom{p-1}{i-1}^2.$$

Observe que $\binom{p}{i} = p!i!(p-i)!$ es un múltiplo de p, para $1i \leq p-1$, pues el denominador de esta fracción no es divisíble entre p. Así, $\frac{1}{i^2}\binom{p-1}{i-1}^2 = \frac{1}{p^2}\binom{p}{i}^2$ es entero y portanto la suma

$$\sum_{i=1}^{p-1} \frac{1}{i^2}\binom{p-1}{i-1}^2 \in \mathbb{Z}.$$

Debemos mostrar ahora que es un múltiplo de p. Para ello, observe que cada $1 \leq i \leq p-1$ es invertible módulo p. Sea r_i el inverso de $i \pmod p$, tal que $1 \leq r_i p$, y $ir_i \equiv 1 \pmod p$. Debido a la unicidad del inverso, los r_i, $i = 1, 2, \ldots, p-1$ forman un sistema completo de invertíbles, esto es, son una permutación de $1, 2, \ldots, p-1$.

Como $\binom{p-1}{i-1} \equiv (-1)^{i-1} \pmod p$, entonces

$$\sum_{i=1}^{p-1} \frac{1}{i^2}\binom{p-1}{i-1}^2 \equiv \sum_{i=1}^{p-1} \frac{(ir_i)^2}{i^2}\binom{p-1}{i-1}^2 \pmod p,$$

de modo que

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \binom{p-1}{i-1}^2 \equiv \sum_{i=1}^{p-1} r_i^2 \binom{p-1}{i-1}^2 \equiv \sum_{i=1}^{p-1} r_i^2 (-1)^{2(i-1)} \equiv \sum_{i=1}^{p-1} r_i^2 \equiv \sum_{i=1}^{p-1} i^2 \pmod{p}.$$

Por otro lado, la suma

$$\sum_{i=1}^{p-1} i^2 = \frac{p(p-1)(2p-1)}{6},$$

es un múltiplo de p, ya que $(6,p) = 1$. (observe que $p > 3 \;\Rightarrow\; p \equiv 1, 5 \pmod{6}$)

Esto muestra que

$$p \mid \binom{2p}{p} - 2.$$