Aritmética modular

AMD – Grado en Ingeniería Informática

Objetivos

Al finalizar este tema tendréis que:

- Saber qué es $\mathbb{Z}_n$.
- Saber operar en $\mathbb{Z}_n$.
- Calcular el inverso en $\mathbb{Z}_n$, con $n \in \mathbb{N}$ pequeño, a "ojo".
- Calcular inversos en $\mathbb{Z}_n$ aplicando el Algoritmo de Euclides extendido.
- Saber resolver ecuaciones diofánticas
- Resolver problemas usando el Teorema chino de los restos

El conjunto $\mathbb{Z}_n$

Definición

Sea n un número natural mayor que 1. El conjunto $\mathbb{Z}_n$ es el conjunto de todos los números naturales del 0 a $n-1$, es decir,

$$\boxed{\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}}$$

Siguiendo el mismo razonamiendo que con el reloj (visto en el aula), vamos a ver a continuación cómo podemos representar un número cualquiera de $\mathbb{Z}$ en un número particular de $\mathbb{Z}_n$.

El conjunto $\mathbb{Z}_n$

Definición

Sean $n > 1$ y $a \in \mathbb{Z}$. Si $a = q \cdot n + r$, entonces r es el representante de a en $\mathbb{Z}_n$. Diremos que "a es igual a r módulo n", o que "a es congruente a r módulo n". Se escribe así: $a \equiv r \pmod{n}$

Ejemplo

En $\mathbb{Z}_n$ los números iguales a 0 son los múltiplos de n.

Consecuenta directa de la definición de "representante":

Sean $n > 1$ y $a, b \in \mathbb{Z}$. Entonces

$$a \equiv b \ (mod\ n) \Leftrightarrow a \text{ y } b \text{ tienen el mismo resto al dividirlos por } n.$$

El conjunto $\mathbb{Z}_n$

Pero para ver la igualdad $\mathbb{Z}_n$, no hay que calcular restos por separado; basta aplicar el siguiente resultado.

Criterio para saber si dos números son iguales en $\mathbb{Z}_n$

Sea $n \in \mathbb{N}$ mayor que 1. Dados $a, b \in \mathbb{Z}$, se tiene que

$$a \equiv b \ (mod \ n) \text{ si y sólo si } a - b \text{ es múltiplo de } n.$$

Ejemplos

- $21 \equiv 9 \pmod 4$ porque $21 - 9 = 12$ es un múltiplo de 4.
- $9 \equiv 0 \pmod 3$ porque $9 - 0 = 9$ es un múltiplo de 3.
- $14 \equiv 1 \pmod{13}$ porque $14 - 1 = 13$ es un múltiplo de 13.
- $2 \equiv$ -3 $\pmod 5$ porque $2 - (-3) = 5$ es un múltiplo de 5.
- En $\mathbb{Z}_2$, todos los pares son igual a 0 y todos los impares igual a 1.
- En $\mathbb{Z}_3$, todo número es igual a 0 ó a 1 ó a 2. Si cogemos por ejemplo el 44, como $44 = 14 \cdot 3 + 2$, $44 \equiv 2 \pmod 3$ y 2 es representante de 44.

Operaciones $\mathbb{Z}_n$: suma y producto

En $\mathbb{Z}_n$ podemos **sumar** sin problemas. Es decir, dos números a y b se suman igual en $\mathbb{Z}$ que en $\mathbb{Z}_n$. Por ejemplo $1258 + 8548 = 9806 \equiv 1$ es una operación correcta en $\mathbb{Z}_5$.

PERO en $\mathbb{Z}_n$ todo número es igual a otro menor que n, su representante, por lo que no tiene sentido trabajar con números mayores que n.

Siguiendo con el ejemplo, $1258 \equiv 3$ y $8548 \equiv 3$, por lo que para hallar un representante de la suma, lo mejor es

$$1258 + 8548 \equiv 3 + 3 \equiv 6 \equiv 1 \pmod 5.$$

Observad que $9806 \equiv 1 \pmod 5$ y por eso hemos dicho que se puede operar "sin problemas": el resultado no varía si trabajas con representantes o no.

En $\mathbb{Z}_n$ también podemos **multiplicar** "sin problemas" e igual que antes, debemos operar con los representantes. Siguiendo con el ejemplo, elegid vosotros mismo qué método es mejor para hallar el representante de una multiplicación:

$$1258 \cdot 8548 = 3205384 \equiv 4 \pmod 5$$

ó

$$1258 \cdot 8548 \equiv 3 \cdot 3 = 9 \equiv 4 \pmod 5$$

Operaciones $\mathbb{Z}_n$: suma y producto

Ejemplo

Calculemos en $\mathbb{Z}_6$ lo siguiente:

$$342 \cdot 453 + 123 \cdot 1987.$$

Como $342 \equiv 0$, $453 \equiv 3$, $123 \equiv 3$ y $1987 \equiv 0 \pmod 6$, se tiene que

$$342 \cdot 453 + 123 \cdot 1987 \equiv 0 \cdot 3 + 3 \cdot 1 = 3$$

Diferencias con $\mathbb{Z}$

Es sencillo ver que **la suma y el producto** son asociativas y conmutativas; existe el 0 y el 1 y el producto es distributivo respecto a la suma:
$a \cdot (b + c) = (a \cdot\ b) + (a \cdot c)$.

Pero puede haber sorpresas:

- ⋆ En $\mathbb{Z}_6$ nos encontramos con cosas "curiosas": Dos números, el 2 y el 3, que no son 0 pero que al multiplicarlos da 0: $2 \cdot 3 = 6 \equiv 0 \pmod 6$
- ⋆ ¿En $\mathbb{Z}_5$ pasa esto? Prueba a ver que te encuentras.

Esto nos lleva a la siguiente definición:

Definición

En $\mathbb{Z}_n$ un elemento $a \not\equiv 0 \pmod n$ se dice:

Divisor de 0 si existe $b \not\equiv 0$ con $a \cdot b \equiv 0 \pmod n$.

Invertible si existe $b \not\equiv 0$ con $a \cdot b \equiv 1 \pmod n$. El número b se llama el inverso de a en $\mathbb{Z}_n$ y lo denotaremos por a^{-1}.

Si $a \cdot b \equiv 1$, NO SE DEBE ESCRIBIR $b = \frac{1}{a}$

Inversos y divisores de 0 en $\mathbb{Z}_n$

En las definiciones anteriores, observad que si $a \cdot b = 0$, ambos son divisores de 0; y si $b = a^{-1}$, entonces $a = b^{-1}$. Obviamente el inverso es único.

Ejemplos

1. El 2 y 3 son divisores de 0 en $\mathbb{Z}_6$.
2. En $\mathbb{Z}_{24}$ tenemos:
   - $3 \cdot 8 = 24 \equiv 0$,
   - $3 \cdot 16 = 48 \equiv 0$.

   Con lo cual 3,8 y 16 son divisores de 0.
3. En $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, veamos que tenemos:
   - Respecto al 1: el inverso de 1 es 1.
   - Respecto al 2: $2 \cdot 3 = 6 \equiv 1$ por lo que $3 = 2^{-1}$
   - Respecto al 3: $2 = 3^{-1}$
   - Respecto al 4: si tiene inverso, tendrá que ser el mismo porque ya no nos quedan candidatos diferetes: $4 \cdot 4 = 16 \equiv 1$, por lo que $4 = 4^{-1}$.

Inversos y divisores de 0 en $\mathbb{Z}_n$

El siguiente resultado da el método para encontrar los invertibles y los divisores de 0.

Teorema

Sea $a \not\equiv 0 \in \mathbb{Z}_n$.

(I) a es divisor de $0 \Leftrightarrow \mathrm{mcd}(a, n) \neq 1$.

(II) a es invertible $\Leftrightarrow \mathrm{mcd}(a, n) = 1$.

Así,

- si $d = \mathrm{mcd}(a, n) \neq 1$, y $b = \frac{n}{d}$, tenemos que $a \cdot b \equiv 0 \pmod{n}$.
- si $\mathrm{mcd}(a, n) = 1$, entonces sabemos que existen x e y tal que

$$a \cdot x + n \cdot y = 1.$$

Viendo esta igualdad en $\mathbb{Z}_n$, obtenemos

$$a \cdot x \equiv 1 (mod\ n),$$

por lo que $x = a^{-1}$.

Conclusión:

El algoritmo extendido de Euclides nos permite calcular inversos en $\mathbb{Z}_n$.

Algoritmo extendido de Euclides para el cálculo de inversos

Ejemplo

Vamos a calcular el inverso de 11 en $\mathbb{Z}_{20}$. Para ellos aplicamos el algoritmo extendido de Euclides:

$$\begin{aligned} 20 &= 1\cdot 11 + 9. \\ 11 &= 1\cdot 9 + 2. \\ 9 &= 4\cdot 2 + 1. \\ 2 &= 2\cdot 1. \end{aligned}$$

Por tanto $1 = \text{mcd}(20,9)$. Ahora sustituimos de abajo a arriba los restos:

$$1 = 9 - 4\cdot \underline{2} = 9 - 4\cdot(11-9) \ = 5\cdot \underline{9} - 4\cdot 11 = 5\cdot(20-11) - 4\cdot 11 = 5\cdot 20 - 9\cdot 11.$$

Pasando a $\mathbb{Z}_{20}$ tendremos:

$$1 \equiv 5\cdot 20 - 9\cdot 11 \equiv 5\cdot 0 - 9\cdot 11 \equiv -9\cdot 11$$

Por lo tanto, $11^{-1} = -9$ y observad que $-9 \equiv 11$ en $\mathbb{Z}_{20}$.

$\mathbb{Z}_n$ con n primo

Una consecuencia del teorema de la transparencia 9 es que si n es primo,todo elemento **no nulo** de $\mathbb{Z}_n$ tiene inverso.

Observad que para todo $a \neq 0$ en $\mathbb{Z}$, al ser n primo se verifica que:

$$\begin{cases} mcd(a, n) = n & \text{si } a \text{ es múltiplo de } n, \\ mcd(a, n) = 1 & \text{si no.} \end{cases}$$

Con lo cual, para todo $a \not\equiv 0$, se tiene que $\text{mcd}(a, n) = 1$ y por lo tanto a es invertible.

Ecuaciones diofánticas

Queremos encontrar todas las soluciones enteras de la ecuación

$$ax + by = c$$

con a, b y c enteros
Para ello:

- Calculamos $d = mcd(a, b)$. Si d no divide a c la ecuación no tiene soluciones enteras
- En otro caso, la ecuación siempre tiene solución (no única)

Método de resolución (primera forma)

- Simplificamos la ecuación dividiendo por d. La ecuación resultante $a'x + b'y = c'$ cumple que a' y b' no tienen factores comunes
- Pasamos a $Z_{b'}$ aquí la ecuación es $a'x \equiv c'$ en $Z_{b'}$. Llamando a'' al inverso de a' en $Z_{b'}$ tenemos que $x = c' \cdot a''$ en $Z_{b'}$, es decir $x = c' \cdot a'' + r \cdot b'$ para algún valor entero de r
- Pasamos a $Z_{a'}$ aquí la ecuación es $b'y \equiv c'$ en $Z_{a'}$. Llamando b'' al inverso de b' en $Z_{b'}$ de b' tenemos que $y = c' \cdot b''$ en $Z_{a'}$, es decir $y = c' \cdot b'' + s \cdot a'$ para algún valor entero de s
- Sustituimos en la ecuación

$$a'x + b'y = c'$$

$$a'(c' \cdot a'' + r \cdot b') + b'(c' \cdot b'' + s \cdot a') = c'$$

$$r + s = \frac{c' - a'c'a'' - b'c'b''}{a' + b'}$$

- Despejando, $s = r - \frac{c' - a'c'a'' - b'c'b''}{a' + b'}$
- Las soluciones quedan como:

$$x = c' \cdot a'' + r \cdot b'$$

$$y = c' \cdot b'' + s \cdot a'$$

con r cualquier número entero y $s = r - \frac{c' - a'c'a'' - b'c'b''}{a' + b'}$

Método de resolución (segunda forma)

- Simplificamos la ecuación dividiendo por d. La ecuación resultante $a'x + b'y = c'$ cumple que a' y b' no tienen factores comunes
- Usando el algoritmo de Euclides extendido puedo encontrar números r y s de modo que $a'r + b's = 1$
- Mutiplicando por c' obtengo

$$a'r \cdot c' + b's \cdot c' = c'$$

  por tanto $x = r \cdot c'$, $y = s \cdot c'$ es una solución
- Las demás soluciones son de la forma

$$x = r \cdot c' + k \cdot b'$$

$$y = s \cdot c' - k \cdot a'$$

  para cualquier valor entero k que cojamos

Teorema chino de los restos

Queremos resolver el sistema de congruencias

$$x \equiv a_1 (mod n_1)$$

.....

$$x \equiv a_k (mod n_k)$$

Con $n_1, \cdots, n_k$ de modo que para cualquier par de ellos $mcd(n_i, n_j) = 1$

- Este sistema tiene siempre solución (no única)
- Para calcular una solución
  - Para cada índice i construir q_i como el producto de todos los $n's$ menos n_i (por ejemplo, $q_1 = n_2 \cdot n_3 \cdot \cdots \cdot n_k$)
  - q_i es invertible en Z_{n_i}. Calcula h_i su inverso en Z_{n_i}
  - Una solución es

$$x_0 = a_1 \cdot q_1 \cdot h_1 + a_2 \cdot q_2 \cdot h_2 + \cdots + a_k \cdot q_k \cdot h_k$$

- La solución general es

$$x = x_0 + r \cdot n_1 \cdot n_2 \cdot \cdots \cdot n_k$$

Para cualquier valor entero de r