Representación de números

Clase 25

IIC 1253

Prof. Cristian Riveros

Congruencia modular (pendiente clase anterior)

Definición

Sea $m \in \mathbb{Z}$ con $m > 0$.

Para todo $a, b \in \mathbb{Z}$ diremos que a es **congruente** con b **módulo** m si:

$$a \equiv b \pmod{m} \qquad \text{si, y solo si,} \qquad m \mid (a - b)$$

Ejemplo

- $15 \equiv 45 \pmod{6}$? ✓
- $-7 \equiv -11 \pmod{4}$? ✓

Congruencia modular (pendiente clase anterior)

Definición

Sea $m \in \mathbb{Z}$ con $m > 0$.

Para todo $a, b \in \mathbb{Z}$ diremos que a es **congruente** con b **módulo** m si:

$$a \equiv b \pmod{m} \qquad \text{si, y solo si,} \qquad m \mid (a - b)$$

Para $m \in \mathbb{Z}$, la relación $a \equiv b \pmod{m}$ es una **relación de equivalencia**.

Proposición

Para todo $a, b, m \in \mathbb{Z}$ con $m > 0$, las siguientes condiciones son equivalentes:

1. $a \equiv b \pmod{m}$
2. $a = b + m \cdot s$ para algún $s \in \mathbb{Z}$.
3. $(a \bmod m) = (b \bmod m)$

Suma y multiplicación de congruencia modular

Si $7 \equiv 13 \pmod 6$ y $2 \equiv 8 \pmod 6$, ¿es verdad que:

$$\begin{aligned} 7+2 &\equiv 13+8 \pmod 6 \quad ? \\ 7\cdot 2 &\equiv 13\cdot 8 \pmod 6 \quad ? \end{aligned}$$

Suma y multiplicación de congruencia modular

Proposición

Para todo $m > 0$, si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces:

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ a \cdot c &\equiv b \cdot d \pmod{m} \end{aligned}$$

Demostración

Supongamos que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$.
Por la proposición anterior, tenemos que existe $r, s \in \mathbb{Z}$ tal que:

$$a = b + m \cdot r \qquad \text{y} \qquad c = d + m \cdot s$$

Sumando y multiplicando ambas igualdades, tenemos que:

$$\begin{aligned} a + c &= b + d + m \cdot (r + s) && \Rightarrow \quad a + c \equiv b + d \pmod{m} \\ a \cdot c &= (b + m \cdot r)(d + m \cdot s) && \\ &= b \cdot d + m \cdot (bs + rd + rms) && \Rightarrow \quad a \cdot c \equiv b \cdot d \pmod{m} \end{aligned}$$

$\square$

Suma y multiplicación de congruencia modular

Proposición

Para todo $m > 0$, si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces:

$$\begin{aligned} a + c &\equiv b + d \pmod{m} \\ a \cdot c &\equiv b \cdot d \pmod{m} \end{aligned}$$

Corolario

Para todo $a, b, m \in \mathbb{Z}$ con $m > 0$, se tiene que:

$$\begin{aligned} (a + b) \bmod m &= ((a \bmod m) + (b \bmod m)) \bmod m \\ (a \cdot b) \bmod m &= ((a \bmod m) \cdot (b \bmod m)) \bmod m \end{aligned}$$

Demostración: ejercicio.

Aritmética módulo m

Definición

Para $m > 0$, sea $\mathbb{Z}_m = \{0, \ldots, m-1\}$.
Para todo $a, b \in \mathbb{Z}_m$, definimos las operaciones $+_m$ y $\cdot_m$ como:

$$\begin{aligned} a +_m b &= (a+b) \bmod m \\ a \cdot_m b &= (a \cdot b) \bmod m \end{aligned}$$

¿cuáles son los valores de?

- $7 +_{11} 9 \;=\; 5$
- $7 \cdot_{11} 9 \;=\; 8$

¿han usado estas operaciones antes?

¿qué propiedades cumple la aritmética modular?

Propiedades

Para todo $a, b, c \in \mathbb{Z}_m$, se cumple que:

Clausura: $a +_m b \in \mathbb{Z}_m$ y $a \cdot_m b \in \mathbb{Z}_m$.

Conmutatividad: $a +_m b = b +_m a$
$a \cdot_m b = b \cdot_m a$

Asociatividad: $a +_m (b +_m c) = (a +_m b) +_m c$
$a \cdot_m (b \cdot_m c) = (a \cdot_m b) \cdot_m c$

Identidad: $a +_m 0 = a$
$a \cdot_m 1 = 1$

Inverso (aditivo): Si $a \neq 0$, entonces existe $a' \in \mathbb{Z}_m$ tal que $a +_m a' = 0$

Distributividad: $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

¿qué propiedad falta?

Outline

Representación de números

Outline

Representación de números

Teorema

Sea $b > 1$. Si $n \in \mathbb{N} - \{0\}$, entonces se puede escribir de forma única como:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_1 b + a_0 = \sum_{i=0}^{k-1} a_i b^i$$

- $k \geq 1$,
- $a_0, \ldots, a_{k-1}$ menor que b $\quad (a_i < b) \quad$ y
- $a_{k-1} \neq 0$.

¿cuál es la representación de 123?

con $b = 10$: $\quad 123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$

con $b = 2$: $\quad 123 = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$

con $b = 8$: $\quad 123 = 1 \cdot 8^2 + 7 \cdot 8^1 + 3 \cdot 8^0$

Demostración: por inducción fuerte

$$P(n) \ := \quad n \ = \ \sum_{i=0}^{k-1} a_i b^i$$

1. $P(1): \quad 1 = 1 \cdot b^0$ ✓

2. Suponemos que $P(n')$ se cumple para todo $n' < n$ y dem. $P(n)$:
   - Existe un único par $m, r \in \mathbb{Z}$ con $0 \leq r < b$ tal que: $n \ = \ m \cdot b + r$.
   - Como $m < n$ (¿por qué?), entonces por hipótesis de inducción:
   $$m \ = \ \sum_{i=0}^{k-1} a_i b^i \quad k \geq 1,\ a_i < b \text{ y } a_{k-1} \neq 0.$$
   - Reemplazando m tenemos que:
   $$n \ = \ \left(\sum_{i=0}^{k-1} a_i b^i \right) \cdot b + r \ = \ \sum_{i=0}^{k-1} a_i b^{i+1} + r$$
   - Definiendo $a'_0 = r$ y $a'_{i+1} = a_i$ para $0 \leq i \leq k$, tenemos que:
   $$n \ = \ a'_k b^k + a'_{k-1} b^{k-1} + \ldots + a'_1 b + a'_0$$
   con $k + 1 \geq 1,\ a'_i < b$ y $a'_k \neq 0$. $\square$

Representación de números

Teorema

Sea $b > 1$. Si $n \in \mathbb{N}$, entonces se puede escribir de forma única como:

$$n \; = \; a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \ldots + a_1 b + a_0 \; = \; \sum_{i=0}^{k-1} a_i b^i$$

- $k \geq 1$,
- $a_0, \ldots, a_{k-1}$ menor que $b \quad (a_i < b) \quad$ y
- $a_{k-1} \neq 0$.

Desde ahora, decimos que la representación de ***n* en base *b*** es la secuencia:

$$(n)_b \; = \; a_{k-1} \ldots a_1 a_0$$

Ejemplo

$$(123)_{10} = 123 \qquad (123)_2 = 1111011 \qquad (123)_8 = 173$$

¿cómo encontramos la representación de n en base b?

Para $n \in \mathbb{N} - \{0\}$ y $b > 1$, deseamos encontrar los coeficientes $a_i < b$ tal que:

$$n \;=\; a_{k-1}b^{k-1} + \ldots + a_1 b + a_0$$

Sabemos que $n \;=\; q \cdot b + r$ para algún único par $q, r \in \mathbb{N}$ con $r < b$.

¿qué es q y r en la representación de n en base b?

Proposición

Para un $n \in \mathbb{N} - \{0\}$ y $b > 1$, si $(n)_b = a_{k-1} \ldots a_1 a_0$ y $n = q \cdot b + r$, entonces:

$$\begin{aligned} r &= a_0 \\ (q)_b &= a_{k-1} \ldots a_1 \end{aligned}$$

Demostración: ejercicio.

¿cómo encontramos la representación de n en base b?

Ejemplo

Para escribir 39 en base 2:

$$\begin{aligned} 39 &= 19 \cdot 2 + 1 \\ 19 &= 9 \cdot 2 + 1 \\ 9 &= 4 \cdot 2 + 1 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 1 \cdot 2 + 0 \\ 1 &= 0 \cdot 2 + 1 \end{aligned}$$

Por lo tanto, $(39)_2 = 100111$.

Para escribir 39 en base 5:

$$\begin{aligned} 39 &= 7 \cdot 5 + 4 \\ 7 &= 1 \cdot 5 + 2 \\ 1 &= 0 \cdot 5 + 1 \end{aligned}$$

Por lo tanto, $(39)_5 = 124$.

Algoritmo para conversión de base

Algoritmo

input : Número $n \in \mathbb{N} - \{0\}$, base $b \geq 2$
output: Una secuencia $(n)_b = a_{k-1} \dots a_1 a_0$

Function `ConversiónBase` *(n, b)*

$q := n$

$k := 0$

while $q \neq 0$ **do**

$a_k := q \bmod b$

$q := q \operatorname{div} b$

$k := k + 1$

return $a_{k-1} \dots a_1 a_0$

¿cuál es el tiempo del algoritmo en términos de n?

¿cuál es el tamaño de $(n)_b$ con respecto a n?

Suponga que $|(n)_b| = k$.

- Como n tiene k dígitos en base b, entonces:

$$b^{k-1} \quad \leq \quad n \quad \leq \quad b^k - 1$$

- Despejando k, tenemos que:

$$\log_b(n+1) \quad \leq \quad k \quad \leq \quad \log_b(n) + 1$$

- Como k es un valor entero:

$$\lceil \log_b(n+1) \rceil \quad \leq \quad k \quad \leq \quad \lfloor \log_b(n) + 1 \rfloor$$

Teorema

Para todo $n \in \mathbb{N}$ y $b \geq 2$, se cumple que $|(n)_b| = \lceil \log_b(n+1) \rceil$.

Por lo tanto, $|(n)_b| \in \mathcal{O}(\log(n))$.

Representación y división de números

¿cómo sabemos que un número es divisible por 3?

$$
\begin{aligned}
n \bmod 3 &= (a_k \cdot 10^k + \ldots + a_1 \cdot 10 + a_0) \bmod 3 \\
&= \big((a_k \cdot 10^k) \bmod 3 + \ldots + (a_1 \cdot 10) \bmod 3 + a_0 \bmod 3\big) \bmod 3 \\
&= \big((a_k \cdot 1) \bmod 3 + \ldots + (a_1 \cdot 1) \bmod 3 + a_0 \bmod 3\big) \bmod 3 \\
&= \big(a_k + \ldots + a_1 + a_0\big) \bmod 3
\end{aligned}
$$

Demuestre reglas para 4, 9, ...