Unidad VII: Teoría de números

Teoría de números: Aritmética modular

Clase 19 - Matemáticas Discretas (IIC1253)

Prof. Miguel Romero

Para $a, b \in \mathbb{Z}$, escribimos $a \mid b$ para indicar que a divide a b.

$$a \mid b \iff \text{existe } k \in \mathbb{Z} \text{ tal que } a \cdot k = b.$$

Algunas propiedades:

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

- $1 \mid a$.
- $a \mid 0$.
- Si $a \mid b$, entonces $a \mid -b$, $-a \mid b$ y $-a \mid -b$.
- Si $a \mid b$, entonces $a \mid (b \cdot c)$.
- Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$ y $a \mid (b - c)$.

Teorema:

Para cada $a, b \in \mathbb{Z}$ tal que $b \neq 0$, existen números únicos $p, q \in \mathbb{Z}$ tal que:

$$a = p \cdot b + q \qquad \text{y} \qquad 0 \leq q < |b|$$

Ejemplos:

Para los siguientes números a, b encuentre los números p, q del teorema:

$$12, 3 \qquad 3, 12 \qquad 13, 4 \qquad -13, 4 \qquad 13, -4$$

Corolario:

Para cada $a, b \in \mathbb{Z}$ tal que $b > 0$, existen números únicos $p, q \in \mathbb{Z}$ tal que:

$$a = p \cdot b + q \qquad \text{y} \qquad 0 \leq q < b$$

Sean $a, b \in \mathbb{Z}$ tal que $b \neq 0$.

Hay que demostrar que existen únicos $p, q \in \mathbb{Z}$ tal que

$$a = p \cdot b + q \qquad \text{y} \qquad 0 \leq q < |b|$$

Primero veremos la existencia, y luego la unicidad.

Definamos el siguiente conjunto $S \subseteq \mathbb{N}$:

$$S = \{n \in \mathbb{N} \mid n = a - k \cdot b \text{ para algún } k \in \mathbb{Z}\}.$$

Veamos que $S \neq \varnothing$.

Caso 1: $a \geq 0$.

Tenemos que $a \in \mathbb{N}$ y $a = a - 0 \cdot b$, luego $a \in S$.

Caso 2: $a < 0$ y $b \geq 1$.

Veamos que $a - a \cdot b \in S$. Notar que $a - a \cdot b = a \cdot (1 - b)$.
Como $a < 0$ y $(1 - b) \leq 0$, concluimos que $a \cdot (1 - b) \in \mathbb{N}$.

Caso 3: $a < 0$ y $b \leq -1$.

Veamos que $a - (-a) \cdot b \in S$. Notar que $a - (-a) \cdot b = a \cdot (1 + b)$.
Como $a < 0$ y $(1 + b) \leq 0$, concluimos que $a \cdot (1 + b) \in \mathbb{N}$.

Definamos el siguiente conjunto $S \subseteq \mathbb{N}$:

$$S = \{n \in \mathbb{N} \mid n = a - k \cdot b \text{ para algún } k \in \mathbb{Z}\}.$$

Tenemos que $S \neq \varnothing$.

Por el principio del mínimo, obtenemos que S tiene un menor elemento q.

- Como $q \in S$, existe $p \in \mathbb{Z}$ tal que $q = a - p \cdot b$.
- Es decir: $a = p \cdot b + q$.

Basta demostrar que $0 \leq q < |b|$.

Como $q \in \mathbb{N}$ sabemos que $0 \leq q$. Basta ver que $q < |b|$.

Veamos que $q < |b|$.

Por contradicción, supongamos que $q \geq |b|$.

Caso 1: $b > 0$.

En este caso, tenemos que $|b| = b$, y luego $q \geq b$.

Notar que $q - b \geq 0$. Además, $q - b = a - p \cdot b - b = a - (p + 1) \cdot b$.

Obtenemos que $q - b \in S$.

Esto es una contradicción ya que $q - b < q$ y q es el menor elemento de S.

Veamos que $q < |b|$.

Por contradicción, supongamos que $q \geq |b|$.

Caso 2: $b < 0$.

En este caso, tenemos que $|b| = -b$, y luego $q \geq -b$.

Notar que $q + b \geq 0$. Además, $q + b = a - p \cdot b + b = a - (p-1) \cdot b$.

Obtenemos que $q + b \in S$.

Esto es una contradicción ya que $q + b < q$ y q es el menor elemento de S.

Acabamos de demostrar que existen $p, q \in \mathbb{Z}$ tal que:

$$a = p \cdot b + q \qquad \text{y} \qquad 0 \leq q < |b|$$

Veamos que estos p, q son únicos.

Supongamos que existen r, s tal que $a = r \cdot b + s$ y $0 \leq s < |b|$.

- Vamos a demostrar que $p = r$ y $q = s$.

Tenemos que $(p - r) \cdot b = s - q$. Obtenemos que $b \mid (s - q)$.

Como $0 \leq q < |b|$, sabemos que $-|b| < -q \leq 0$.

Combinando $0 \leq s < |b|$ y $-|b| < -q \leq 0$, obtenemos que $-|b| < s - q < |b|$.

Dado que $b \mid (s - q)$ y $-|b| < s - q < |b|$, concluimos que $s - q = 0$.

Como $(p - r) \cdot b = s - q$ y $b \neq 0$, concluimos que $p - r = 0$.

Obtenemos que $p = r$ y $q = s$.

Sean $a, b \in \mathbb{Z}$ tal que $b \neq 0$.

El teorema anterior nos dice que existen únicos $p, q \in \mathbb{Z}$ tal que:

$$a = p \cdot b + q \qquad \text{y} \qquad 0 \leq q < |b|$$

Notación:

- p es el cociente de la división de a en b.
- q es el **resto de la división de a en b**.

Al resto de la división de a en b también le llamaremos **a módulo b**.

- Escribimos $a \bmod b$.

Observación:

$$a \mid b \quad \Longleftrightarrow \quad b \bmod a = 0$$

División euclideana: cociente y resto

Sean $a, b \in \mathbb{Z}$ tal que $b \neq 0$.

El teorema anterior nos dice que existen únicos $p, q \in \mathbb{Z}$ tal que:

$$a = p \cdot b + q \qquad \text{y} \qquad 0 \leq q < |b|$$

Notación:

- p es el cociente de la división de a en b.
- q es el **resto de la división de a en b**.

Al resto de la división de a en b también le llamaremos **a módulo b**.

- Escribimos $a \bmod b$.

Ejemplos:

$$12 \bmod 2 = 0 \qquad 13 \bmod 2 = 1$$

$$15 \bmod 3 = 0 \qquad -15 \bmod 3 = 0 \qquad 16 \bmod 3 = 1 \qquad -16 \bmod 3 = 2$$

$$16 \bmod -3 = 1 \qquad 3 \bmod 7 = 3 \qquad 33 \bmod -7 = 5$$

Definición:

Sea $n \in \mathbb{Z}$. Para $a, b \in \mathbb{Z}$ definimos:

$$a \equiv_n b \iff n \mid (b - a)$$

Decimos que a y b son **congruentes (o equivalentes) módulo n**.

Ya vimos que $a \equiv_n b$ es una relación de equivalencia:

- $a \equiv_n a$.
- Si $a \equiv_n b$, entonces $b \equiv_n a$.
- Si $a \equiv_n b$ y $b \equiv_n c$, entonces $a \equiv_n c$.

Proposición:

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Demostración ($\Leftarrow$):

Tenemos que a y b se pueden escribir como:

$$\begin{array}{rclr} a & = & p \cdot n + q & 0 \leq q < |n| \\ b & = & r \cdot n + s & 0 \leq s < |n| \end{array}$$

Recordar que $q = a \bmod n$ y $s = b \bmod n$.

Por hipótesis, tenemos que $q = s$.

Restando la segunda ecuación con la primera obtenemos:

$$(b - a) = (r - p) \cdot n$$

Concluimos que $n \mid (b - a)$, es decir, $a \equiv_n b$.

Proposición:

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Demostración ($\Rightarrow$):

Por contrapositivo, supongamos que $a \bmod n \neq b \bmod n$.

Sin pérdida de generalidad, supongamos que $a \bmod n < b \bmod n$.

Tenemos que a y b se pueden escribir como:

$$\begin{array}{rcl@{\qquad\qquad}l} a & = & p \cdot n + q & 0 \leq q < |n| \\ b & = & r \cdot n + s & 0 \leq s < |n| \end{array}$$

Recordar que $q = a \bmod n$ y $s = b \bmod n$. Por hipótesis, tenemos que $q < s$.

Restando la segunda ecuación con la primera obtenemos:

$$(b - a) = (r - p) \cdot n + (s - q)$$

Notar que $1 \leq (s - q) \leq s \leq |n|$. Luego $(b - a) \bmod n = (s - q)$.

Como $(s - q) > 0$, concluimos que $n \nmid (b - a)$, es decir, $a \not\equiv_n b$.

Proposición:

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Corolario:

$a \equiv_n (a \bmod n)$.

Demostración :

Tenemos que:

$$(a \bmod n) = 0 \cdot n + (a \bmod n) \qquad 0 \leq (a \bmod n) < |n|$$

Esto implica que $(a \bmod n) \bmod n = a \bmod n$.

Por la proposición anterior, obtenemos que $a \equiv_n (a \bmod n)$.

Proposición:

Si $a \equiv_n b$ y $c \equiv_n d$, entonces:

$$\begin{aligned} (a + c) &\equiv_n (b + d) \\ (a \cdot c) &\equiv_n (b \cdot d) \end{aligned}$$

Demostración :

Tenemos que $n \mid (b - a)$ y $n \mid (d - c)$.

Es decir, existen $k, \ell \in \mathbb{Z}$ tal que:

$$\begin{aligned} (b - a) &= n \cdot k \\ (d - c) &= n \cdot \ell \end{aligned}$$

Sumando ambas ecuaciones y reordenando obtenemos:

$$(b + d) - (a + c) = n \cdot (k + \ell)$$

Concluimos que $(a + c) \equiv_n (b + d)$.

Proposición:

Si $a \equiv_n b$ y $c \equiv_n d$, entonces:

$$\begin{aligned} (a+c) &\equiv_n (b+d) \\ (a \cdot c) &\equiv_n (b \cdot d) \end{aligned}$$

Demostración :

De las ecuaciones anteriores, obtenemos:

$$\begin{aligned} b &= n \cdot k + a \\ d &= n \cdot \ell + c \end{aligned}$$

Multiplicando ambas ecuaciones:

$$b \cdot d = (n \cdot k + a) \cdot (n \cdot \ell + c) = n^2 \cdot k \cdot \ell + n \cdot k \cdot c + n \cdot \ell \cdot a + a \cdot c$$

Reordenando y factorizando, obtenemos:

$$b \cdot d - a \cdot c = n \cdot (n \cdot k \cdot \ell + k \cdot c + \ell \cdot a)$$

Concluimos que $(a \cdot c) \equiv_n (b \cdot d)$.

Proposición:

Si $a \equiv_n b$ y $c \equiv_n d$, entonces:

$$\begin{aligned}(a + c) &\equiv_n (b + d)\\ (a \cdot c) &\equiv_n (b \cdot d)\end{aligned}$$

Corolario:

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

Ejercicio: Demuestre el corolario.

1. Demuestre que un número $n \in \mathbb{N}$ es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

2. De reglas de división para los números 4 y 8.

3. Calcule $1000^{1000^{1000}} \bmod 17$.