Teoría de números

Clase 21

IIC 1253

Prof. Cristian Riveros

Outline

División

Congruencia modular

Outline

División

Congruencia modular

División

Sea $\mathbb{Z}$ el conjunto de todos los enteros.

Definición

Para $a, b \in \mathbb{Z}$ con $a \neq 0$,
diremos que a **divide** b si existe $q \in \mathbb{Z}$ tal que $a \cdot q = b$.

$$a \mid b \quad \text{si, y solo si,} \quad \exists q \in \mathbb{Z}.\ a \cdot q = b$$

Ejemplos

- $5 \mid 45$?
- $12 \mid 34$? (en este caso, anotamos $12 \nmid 34$)
- $25 \mid 0$?

Si $a \mid b$, diremos que
a es un **divisor** de b o que b es un **multiplo** de a.

División

Proposición

Para $a, b, c \in \mathbb{Z}$ con $a \neq 0$:

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

Demostración

Supongamos que $a \mid b$ y $a \mid c$.

- $a \mid b$ entonces $a \cdot q = b$ para algún $q \in \mathbb{Z}$.
- $a \mid c$ entonces $a \cdot q' = c$ para algún $q' \in \mathbb{Z}$.

Si sumamos ambas igualdades tenemos que:

$$\begin{aligned} a \cdot q + a \cdot q' &= b + c \\ a \cdot (q + q') &= b + c \end{aligned}$$

Por lo tanto, $a \mid (b + c)$.

División

Proposición

Para $a, b, c \in \mathbb{Z}$ con $a \neq 0$:

1. Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$.
2. Si $a \mid b$, entonces $a \mid (b \cdot c)$ para todo $c \in \mathbb{Z}$.
3. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

Demuestre 2. y 3.

Corolario

Si $a \mid b$ y $a \mid c$, entonces $a \mid (n \cdot b + m \cdot c)$ para todo $n, m \in \mathbb{Z}$.

División con resto

Por el "*algoritmo de división con resto*"
sabemos que siempre existe $q, r \in \mathbb{Z}$ con $0 \leq r < a$ tal que: $a \cdot q + r = b$.

Teorema

Sea $a, b \in \mathbb{Z}$ con $a > 0$.
Entonces existen un único par $q, r \in \mathbb{Z}$ con $0 \leq r < a$ tal que:

$$a \cdot q + r \quad = \quad b$$

Demostración

Suponga (por contradicción) que existe $(q', r') \neq (q, r)$ con $0 \leq r' < a$:

$$b \quad = \quad a \cdot q + r \quad = \quad a \cdot q' + r' \quad \text{, entonces} \quad a \cdot (q - q') = r' - r$$

1. Si $r = r'$, entonces $q = q'$. ¡contradicción!
2. Si $r < r' < a$, entonces $a > r' - r = a \cdot (q - q') > 0$. ¡contradicción! (?)
3. Si $r' < r < a$, entonces $a > r - r' = a \cdot (q' - q) > 0$. ¡contradicción! (?)

$\square$

División con resto

Por el "*algoritmo de división con resto*"
sabemos que siempre existe $q, r \in \mathbb{Z}$ con $0 \leq r < a$ tal que: $a \cdot q + r = b$.

Teorema

Sea $a, b \in \mathbb{Z}$ con $a > 0$.
Entonces existen un único par $q, r \in \mathbb{Z}$ con $0 \leq r < a$ tal que:

$$a \cdot q + r \quad = \quad b$$

Definición

Desde ahora, si $a \cdot q + r = b$ entonces anotaremos:

$$\begin{aligned} b \textbf{ div } a &= q \\ b \textbf{ mod } a &= r \end{aligned}$$

Ejemplo

$42 \textbf{ div } 13 = 3$ $\quad$ $42 \textbf{ mod } 13 = 3$ $\quad$ $-12 \textbf{ div } 9 = -2$ $\quad$ $-12 \textbf{ mod } 9 = 6$

División con resto

Por el "*algoritmo de división con resto*"
sabemos que siempre existe $q, r \in \mathbb{Z}$ con $0 \leq r < a$ tal que: $a \cdot q + r = b$.

Teorema

Sea $a, b \in \mathbb{Z}$ con $a > 0$.
Entonces existen un único par $q, r \in \mathbb{Z}$ con $0 \leq r < a$ tal que:

$$a \cdot q + r = b$$

Definición

Desde ahora, si $a \cdot q + r = b$ entonces anotaremos:

$$\begin{aligned} b \textbf{ div } a &= q \\ b \textbf{ mod } a &= r \end{aligned}$$

Demuestre que $a \mid b$ si, y solo si, $b \textbf{ mod } a = 0$.

Outline

División

Congruencia modular

Congruencia modular

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

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:

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

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. $(a \textbf{ mod } m) = (b \textbf{ mod } m)$

Demostración: ejercicio.

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:

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

Suma y multiplicación de congruencia modular

Proposición

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

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

Corolario

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

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

Demostración: ejercicio.

Aritmética módulo m

Definición

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

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

¿han usado estas operaciones antes?

¿cuáles son los valores de?

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

¿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?