

Propiedades:

- $[a]_m + [b]_m = [a+b]_m$
- $[a]_m \cdot [b]_m = [a \cdot b]_m$
- si $m = p$ (primo) entonces \mathbb{Z}_p es un cuerpo.

↳ Estructura de anillo.

En particular todos sus elementos tienen inverso.

Ejemplo

• En \mathbb{Z}_5 : $[3]_5 \cdot [2]_5 = [3 \cdot 2]_5 = [6]_5 = [1]_5$

Entonces $[3]_5$ es el inverso de $[2]_5$ en módulo 5.

• En \mathbb{Z}_6 : $[3]_6 \cdot [2]_6 = [6]_6 = [0]_6$

Cuando el producto de dos elementos $\neq 0$ sea cero los llamaremos **divisores de cero**.

Ejercicio

$[a]_m$ es inversible si y sólo si $[a]_m$ no es divisor de cero

↳ \Rightarrow

Supongamos que $[a]_m$ es inversible, entonces existe $[b]_m \neq [0]_m$ tal que $[a]_m \cdot [b]_m = [1]_m$.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

Multiplícamos (4) por $[b]_m$:

$$[c]_m = [4]_m \cdot [c]_m = [b]_m \cdot [a]_m [c]_m = [b]_m \cdot [0]_m = [0]_m$$

Llegando a una contradicción ya que $[c]_m = [0]_m \neq [0]_m$
Por tanto $[a]_m$ no puede ser un divisor de cero. \uparrow

Definición.

Llamaremos **congruencia lineal** a una expresión del tipo:

$$ax \equiv b \pmod{m}$$

con $a, b, x \in \mathbb{Z}$ y $m \in \mathbb{N}$. Donde la x es una incógnita.

Ejemplo.

Resolver la congruencia lineal:

$$7x \equiv 2 \pmod{5}$$

Vamos a intentar simplificar los coeficientes:

En \mathbb{Z}_5 , $[7]_5 = [2]_5$, entonces la expresión anterior es equivalente a:

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

Ejemplo:

Resolver: $15x \equiv 4 \pmod{17}$.

$$\boxed{\text{m.c.d.}(15, 17) = 1}$$

Recordamos que $a \equiv b \pmod{m} \Leftrightarrow a - b = k \cdot m$

En nuestro caso:

$$15x - 4 = 17 \cdot k \Leftrightarrow 15x - 17 \cdot k = 4$$

$$\begin{array}{l} \Leftrightarrow \\ \uparrow \\ y = -k \end{array} 15x + 17y = 4$$

Debemos resolver la ec. diofántica $15x + 17y = 4$ y la solución a la congruencia será x .

Resolvemos la ec. diofántica aplicando el algoritmo de Euclides

$$17 = 15 \cdot 1 + 2 \rightarrow 2 = 17 - 15$$

$$15 = 2 \cdot 7 + 1 \rightarrow 1 = 15 - 2 \cdot 7$$

$$2 = 1 \cdot 2 + 0$$

$$\begin{aligned} 1 &= 15 - 2 \cdot 7 = 15 - (17 - 15) \cdot 7 = 15 - 17 \cdot 7 + 15 \cdot 7 = \\ &= 15 \cdot 8 - 17 \cdot 7 \end{aligned}$$

Entonces: $15 \cdot (8) + 17 \cdot (-7) = 1$ por tanto, multiplicando por 4:

$$15 \cdot (32) + 17 \cdot (-28) = 4$$

Luego $x = 32$ es solución de la congruencia.

Debemos dar siempre la solución en el módulo

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Otra forma: Observar que $[15]_{17} = [-2]_{17}$ entonces

$$15x \equiv 4 \pmod{17} \Leftrightarrow -2x \equiv 4 \pmod{17}$$

$$\text{Entonces } [x]_{17} = [-2]_{17} = [15]_{17}.$$

¿ Tiene siempre solución una congruencia lineal?

No:

Resolver $ax \equiv b \pmod{m}$ es equivalente a resolver $ax - b = km \Leftrightarrow ax - m \cdot k = b$ esta ec. diofántica. y tiene solución si y sólo si $\text{m.c.d.}(a, m)$ divide a b .

En caso de tener solución, ¿ cuántas soluciones incongruentes tiene? Tiene $\text{m.c.d.}(a, m)$ soluciones incongruentes.

Ejemplo:

1) $27x \equiv 40 \pmod{15}$

No tiene solución pues $\text{m.c.d.}(27, 15) = 3$
no divide a 40

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

$$78 = 66 \cdot 1 + 12 \rightarrow 12 = 78 - 66$$

$$66 = 12 \cdot 5 + \boxed{6} \rightarrow 6 = 66 - 12 \cdot 5$$

$$12 = 6 \cdot 2 + 0$$

Por tanto $\text{mcd}(66, 78) = 6$ que divide a 12.

Tiene solución y además tiene 6 soluciones incongruentes.

Cuando tengamos más de una solución, para calcularlas todas deberemos considerar la

nueva congruencia lineal de dividir todo por 6

Congruencia

auxiliar: $11x \equiv 2 \pmod{13}$

Importante: Esta

no es equivalente

a la anterior. Solo

la utilizaremos para

poder calcular todas

las soluciones.

Debemos resolver esta ecuación que es equivalente

$$-2x \equiv 2 \pmod{13}$$

Entonces $[x]_{13} = [-1]_{13} \equiv [12]_{13}$ es solución de esta congruencia lineal.

Para obtener las 6 soluciones incongruentes deberemos calcular 6 soluciones consecutivas de la congruencia auxiliar.

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

De forma general para resolver una congruencia lineal primero deberemos comprobar si tiene solución: $\text{mcd}(a, m) \mid b$?

Si la respuesta es afirmativa entonces tendrá $\text{mcd}(a, m)$ soluciones incongruentes. Para calcularlas todas tendremos que construir la congruencia auxiliar resultante de dividir todo por $\text{mcd}(a, m)$ y las soluciones de la inicial se generan a partir de la auxiliar.

SISTEMAS DE CONGRUENCIAS

Proposición

Sean $a, b \in \mathbb{N}$. Entonces:

$$a \cdot b = \text{mcd}(a, b) \cdot \text{MCM}(a, b)$$

$$\text{MCM}(a, b) = \frac{a \cdot b}{\text{mcd}(a, b)}$$

donde $\text{MCM}(a, b)$ es el mínimo común múltiplo.

Ejemplo

[Th. Resto chino]

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70

Cartagena99

$x \equiv 4 \pmod{7} \Leftrightarrow \boxed{x = 4 + 7 \cdot k}$ y sustituimos en la segunda:

$$4 + 7k \equiv 5 \pmod{8} \Leftrightarrow 7k \equiv 1 \pmod{8}$$

Observamos que $7k \equiv 1 \pmod{8}$ tiene solución y es única (ya que $\text{mcd}(7,8)=1$) y además la solución es $[k]_8 = [-1]_8 = [7]_8$.

Entonces $k = 7 + 8 \cdot \ell$ y por tanto

$$\begin{aligned} x &= 4 + 7 \cdot k = 4 + 7(7 + 8\ell) = 4 + 49 + 56\ell = \\ &= 53 + 56\ell. \end{aligned}$$

Es decir $[x]_{56} = [53]_{56}$ es la solución del sistema.

Ejercicio: $[a]_m$ es inversible en \mathbb{Z}_m si y sólo si $\text{mcd}(a, m) = 1$. (primos entre sí)

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, teal-colored font. The '99' is significantly larger and more prominent than the 'Cartagena' part. The text is set against a background of light blue and orange geometric shapes, including a large blue triangle and an orange shape that looks like a stylized '9' or a wave.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP: 689 45 44 70