Práctica 6 , Segunda parte (Ejercicios 11 al 20)

Resolución del Ejercicio 13

- Analicemos si (2,1024) son congruentes módulo 3:

$$2 \equiv 1024 \ mod(3) \Leftrightarrow 3/(2-1024)$$

es decir, por definición, de divisibilidad tenemos:

$$existe \ k \in Z \ tal \ que \ (2-1024) = 3k$$

$$-1022 = 3k$$

pero

$$\frac{-1022}{3} = k \notin Z$$

Conclusión: podemos entonces concluir, que $2 \neq 1024 \ mod(3)$.

- Analicemos si (101,512) son congruentes módulo 3:

$$101 \equiv 512 \ mod(3) \Leftrightarrow 3/(101-512)$$

es decir, por definición, de divisibilidad tenemos:

$$existe \ h \in Z \ tal \ que \ (101-512) = 3h$$

$$-411 = 3h$$

Luego

$$\frac{-411}{3} = h$$

$$-137 = h$$

Como existe $h = -137 \in Z$ tal que (101-512)=-411=3.(-137)

Conclusión: podemos entonces concluir, que $101 \equiv 512 \ mod(3)$.

- Se deja de tarea, analizar si (1501,1348) son congruentes mod(3).

Resolución del Ejercicio 14

- Busco $m \in Z$ tal que $5 \equiv 4 \ mod(m)$

  es decir, por definición de congruencia:

$$existe \ k \in Z \ tal \ que \ (5-4) = mk$$

$$1 = mk$$

  luego

  $m = k = 1$ ó $m = k = -1$

  Conclusión: Los valores que puede tomar m son: $m \in \{-1, 1\}$.

- Busco $m \in Z$ tal que $3 \equiv -3 \ mod(m)$

  es decir, por definición de congruencia:

$$existe \ h \in Z \ tal \ que \ (3-(-3)) = mh$$

$$6 = mh \ (1)$$

también , podemos escribirlo:

$$\frac{6}{m} = h \in Z \ (2)$$

Luego para saber los valores que puede tomar m (mirando (1) ó en forma equivalente podemos mirar (2)), consiredamos:

$$6 = 6 \cdot 1 = (-6) \cdot (-1) = 2 \cdot 3 = (-2) \cdot (-3)$$

Finalmente, tenemos que $m = \pm 1, \pm 2, \pm 3, \pm 6$

Conclusión: Los valores que puede tomar m son:

$$m \in \{-1, 1, -2, 2, -3, 3, -6, 6\}$$

- se deja de tarea, el análisis de los casos:

$$1 \equiv 0 \ mod(m)$$

$$1197 \equiv 286 \ mod(m)$$

Resolución del Ejercicio 16

Sean a, b, c y $n \in Z$

Resolución del inciso c

$$a \equiv b \; mod(n) \wedge b \equiv c \; mod(n) \Rightarrow a \equiv c \; mod(n)$$

Para comenzar, tenemos como dato lo siguiente:

- $a \equiv b \; mod(n)$, es decir, por definición de congruencia, tenemos:

$$existe \; k \in Z \; tal \; que \; a - b = nk \; (1)$$

- $b \equiv c \; mod(n)$, es decir, por definición de congruencia, tenemos:

$$existe \; h \in Z \; tal \; que \; b - c = nh \; (2)$$

- Queremos probar:

$$a \equiv c \; mod(n)$$

  es decir, por definición de congruencia, tenemos:

$$existe \; t \in Z \; tal \; que \; a - c = nt$$

Comencemos:

si sumamos (1) + (2) obtenemos:

$$(a - b) + (b - c) = nk + nh$$

Luego, realizamos calculos y llegamos a:

$$(a - c) = n(k + h)$$

luego por propiedades de números enteros (suma es cerrada) $(k + h) = t \in Z$

$$(a - c) = nt$$

por definición de congruencia, nos queda:

$$a \equiv c \; mod(n)$$

como queríamos probar.

Resolución del inciso f

$$a \equiv 0 \; mod(n) \Leftrightarrow n/a$$

es lo mismo que escribir:

$$\forall a \in Z \, (a \equiv 0 \; mod(n) \Rightarrow n/a \;(1) \wedge n/a \Rightarrow a \equiv 0 \; mod(n) \;(2))$$

Comencemos demostrando $a \equiv 0 \; mod(n) \Rightarrow n/a$ (1):

$$a \equiv 0 \; mod(n)$$

por definición de congruencia

$$existe \; h \in Z \; tal \; que \; a - 0 = nh$$

$$existe \; h \in Z \; tal \; que \; a = nh$$

por definición de divisibilidad

$$n/a$$

por lo tanto queda probado (1).

Demostremos $n/a \Rightarrow a \equiv 0 \; mod(n)$ (2):

$$n/a$$

por definición de divisibilidad

$$existe\ w \in Z\ tal\ que\ a = nw$$

por propiedad del neutro en la suma de números enteros:

$$existe\ h \in Z\ tal\ que\ a - 0 = nh$$

por definición de congruencia llegamos:

$$a \equiv 0\ mod(n)$$

por lo tanto queda probado (2).

Finalmente, por (1) y (2) queda demostrado.

Resolución del Ejercicio 17

Sea $m \in Z$ m es un número impar, es decir, existe $k \in Z$ tal que $m = 2k + 1$ (1).

Queremos probar: $m^2 \equiv 1\ mod(4)$, es decir, por definición de congruencia sería:

exite $t \in Z$ talque:

$$m^2 - 1 = 4t$$

Comencemos:

$$m^2 - 1 \underbrace{=}_{(1)} (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4(k^2 + k) \underbrace{=}_{(2)} 4t$$

(pues llamando $(k^2+k) = t \in Z$ (2) (por propiedad suma y producto cerrado en Z)).

Finalmente, llegamos:

$$m^2 - 1 = 4t$$

por definición de congruencia, nos queda:

$$m^2 \equiv 1\ mod(4)$$

que es a lo que queríamos llegar.

Resolución del Ejercicio 19

Recordemos (ver teoría de congruencias pg 6-7, las definiciones y propiedades de las operaciones de suma y producto en el conjunto de clases de equivalecias módulo m, Z_m): sean x, $y \in Z$

- Suma: $\overline{x} + \overline{y} = \overline{x+y}$
- Producto: $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

Comencemos: $\overline{3} + \overline{1} =?$

aplicamos la suma y tenemos:

$$\overline{3} + \overline{1} = \overline{3+1} = \overline{4}$$

luego vamos a resolverlo usando la propiedad demostrada en el ejercicio 18:

Propiedad: todo número es congruente, módulo m, con el resto de su división por m.

Entonces:

Caso 1: $m = 4$, y como $\overline{4}$ hay que realizar la división entre ambos, luego, por el algoritmo de la división de enteros, tenemos:

$$4 = 4 \cdot 1 + 0$$

el cociente es 1 y el resto es 0.

(recordar que el resto $0 \leq r < |4| = 4$, luego los resto posibles son: $r \in \{0, 1, 2, 3\}$).

concluimos entonces:

$$\overline{3} + \overline{1} = \overline{3 + 1} = \overline{4} = 0$$

Caso 2: $m = 5$, y como $\overline{4}$, pero como $4 < 5$
(recordar que el resto $0 \leq r < |5| = 5$, luego los resto posibles son: $r \in \{0, 1, 2, 3, 4\}$).

concluimos entonces:

$$\overline{3} + \overline{1} = \overline{3 + 1} = \overline{4} = 4$$

Veamos: $\overline{40} \cdot \overline{3} = ?$

aplicamos el producto y tenemos:

$$\overline{40} \cdot \overline{3} = \overline{40 \cdot 3} = \overline{120}$$

luego vamos a resolverlo usando la propiedad demostrada en el ejercicio 18:

Propiedad: todo número es congruente, módulo m, con el resto de su división por m.

Entonces:

Caso 1: $m = 4$, y como $\overline{120}$ hay que realizar la división entre ambos, luego, por el algoritmo de la división de enteros, tenemos:

$$120 = 4 \cdot 30 + 0$$

el cociente es 30 y el resto es 0.

(recordar que el resto $0 \leq r < |4| = 4$, luego los resto posibles son: $r \in \{0, 1, 2, 3\}$).

concluimos entonces:

$$\overline{40} \cdot \overline{3} = \overline{40 \cdot 3} = \overline{120} = 0$$

Caso 2: $m = 5$, y como $\overline{120}$ hay que realizar la división entre ambos, luego, por el algoritmo de la división de enteros, tenemos:

$$120 = 5 \cdot 24 + 0$$

el cociente es 24 y el resto es 0.

(recordar que el resto $0 \leq r < |5| = 5$, luego los resto posibles son: $r \in \{0, 1, 2, 3, 4\}$).

concluimos entonces:

$$\overline{40} \cdot \overline{3} = \overline{40 \cdot 3} = \overline{120} = 0$$

Se deja de tarea, completar tanto con $m = 4$ como con $m = 5$ los casos:

$$\overline{5} + \overline{9}$$

$$(\overline{3} + \overline{2}) \cdot (\overline{6} \cdot \overline{8})$$