ARITMETICA MODULAR PARA PRINCIPIANTES EN EL VI CONGRESO DE MATEMATICAS Y GEOGEBRA IBAGUÉ OCTUBRE 7, 8 Y 9 DEL 2014

Si a, b, k Ɛ Z y m Ɛ N entonces

a ≡ b (mod m) $\Leftrightarrow$ a – b es múltiplo de m, es decir a – b = km $\Rightarrow a = b + mk$

Además al dividir a entre m y b entre m dejan el mismo residuo

a ≡ b (mod m) $\Leftrightarrow$ a(mod m) = b(mod m) = residuo

Ejemplo: 21 ≡ 17 (mod 4) $\Rightarrow$ 21 – 17 es múltiplo de 4; 21 ÷ 4 ^ 17 ÷ 4 dejan el mismo residuo 1

Hallar 3 enteros congruentes con 5 (mod 7): x ≡ 5 (mod 7) $\Rightarrow$ x = 5 + 7k, tomando para k valores 1, 5 ^ – 4 tenemos x = 12, 19, – 23 o sea 12 ≡ 5 (mod 7); 19 ≡ 5 (mod 7); – 23 ≡ 5 (mod 7)

PROPIEDADES DE ≡ si a, b, c, d $\in Z$ y m $\in$ N

PROPIEDAD REFLEXIVA a ≡ a (mod m); 7 ≡ 7 (mod 9), en efecto 7 – 7 es múltiplo de 9

SIMÉTRICA si a ≡ b (mod m) $\Leftrightarrow$ b ≡ a (mod m); 12 ≡ 3 (mod 9) $\Rightarrow$ 3 ≡ 12 (mod 9), en efecto 12 – 3 es múltiplo de 9 ^ 3 – 12 es múltiplo de 9

TRANSITIVA si a ≡ b (mod m) ^ b ≡ c (mod m) $\Leftrightarrow$ a ≡ c (mod m); 10 ≡ 7(mod 3) ^ 7 ≡ 1(mod 3) $\Leftrightarrow$ 10 ≡ 1(mod 3)

UNIFORME RESPECTO A LA SUMA: SI a ≡ b (mod m) y c ≡ d (mod m) $\Leftrightarrow$ a + c ≡ b + d (mod m); 10 ≡ 7(mod 3) ^ 7 ≡ 1(mod 3) $\Leftrightarrow$ 10 + 7 ≡ 7 + 1 (mod 3) o sea 17 ≡ 8(mod 3)

UNIFORME RESPECTO AL PRODUCTO: a ≡ b (mod m) y c ≡ d (mod m) $\Leftrightarrow$ a× c ≡ b × d (mod m) 10 ≡ 7(mod 3) ^ 7 ≡ 1(mod 3) $\Leftrightarrow$ 10 × 7 ≡7 × 1 (mod 3) o sea 70 ≡ 7(mod 3)

Si a ≡ b (mod m) $\Rightarrow a^k \equiv b^k (\mathrm{mod}\, m)$**;** a ^ b Ɛ Z y k Ɛ N, la inversa no se cumple siempre; 19 ≡ 2(mod 17) $\Rightarrow$ $19^3 \equiv 2^3$ (mod 17), verificarlo

Si a ≡ b (mod m) $\Rightarrow$ a ≡ b + mk (mod m); 19 ≡ 2 + 17(3) (mod 17); a, b y k son enteros y m natural

EJERCICIO DE APLICACIÓN

Hallar el residuo de dividir 20^{257} entre 7

D/ 20 ≡ – 1 (mod 7) $\Rightarrow$ $20^{257} \equiv (-1)^{257}$ $\Rightarrow 20^{257} \equiv -1$ (mod 7) $\Rightarrow$ $20^{257} \equiv -1 + 7$ (mod 7) $\Rightarrow 20^{257} \equiv$ 6 (mod 7), por lo tanto el residuo es 6

OPERACIONES CON CONGRUENCIAS

SUMA: a (mod m) + b (mod m) = a + b (mod m); 2(mod 5) + 4(mod 5) = 6(mod 5) $\equiv$ 1(mod 5) lo que significa que **2 + 4 = 1 en Z_5**

RESTA: a (mod m) – b (mod m) = a – b (mod m); 2(mod 5) – 4(mod 5) = – 2(mod 5) $\equiv$ 3(mod 5) lo que significa que **2 – 4 = 3 en Z_5**

PRODUCTO: a (mod m) × b (mod m) = a × b (mod m); 2(mod 5) × 4(mod 5) = 8(mod 5) $\equiv$ 3(mod 5) lo que significa que **2 × 4 = 3 en** $\mathbf{Z_5}$

COCIENTE: 3(mod 5) ÷ 4(mod 5) →hay que resolver $\frac{3}{4}$ en Z_5 entonces 3 × 4^{-1} en Z_5 o sea hay que determinar el inverso de 4 (mod 5)

El inverso se puede hallar de varias formas, veamos la siguiente

a × a^{-1} = 1 (mod m) en nuestro caso a = 4 y hallaremos 4^{-1} en Z_5 = {0, 1, 2, 3, 4}

4 × 0 ≡ 0(mod 5)

4 × 1 ≡ 4(mod 5)

4 × 2 ≡ 8(mod 5) ≡ 3(mod 5)

4 × 3 ≡ 12(mod 5) ≡ 2(mod 5)

4 × 4 ≡ 16(mod 5) ≡ 1(mod 5) por lo tanto el inverso de 4(mod 5) es 4

a × a^{-1} ≡1(mod m)

Entonces

3 × 4^{-1} = 3 × 4 (mod 5) ≡ 2 (mod 5) por lo tanto 3(mod 5) ÷ 4(mod 5) = 2 (mod 5) lo que significa que **3 ÷ 4 = 2 en** $\mathbf{Z_5}$

Una forma más sencilla es aplicando la fórmula a^{-1} = $\frac{1+mk}{a}$ donde m es el módulo y a es el número al cual se le hallará el inverso, k Ɛ Z

4^{-1} = $\frac{1+5k}{4}$ para k = 3, 4^{-1} = 4

LA CONGRUENCIA DE EULER

$a^{\phi(m)} \equiv 1(\operatorname{mod} m)$ Siendo (a, m) = 1

$\phi(m)$ Es la cantidad de números Ɛ Z^+ menores o iguales a m que son coprimos con m

Ej. $\phi(4)$, El conjunto de números menores o iguales a cuatro es {1, 2, 3, 4}, de estos los coprimos con 4 son {1, 3}, total 2, por lo tanto $\phi(4)$ = 2

Ej. $\phi(10)$; {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}, Los coprimos con 10 son {1, 3, 7, 9} total 4 por lo tanto $\phi(10)$ = 4

Si p es primo $\phi(p) = p - 1$

Existe un método para calcular $\phi(m)$

Calcular $\phi(200)$

1. Se descompone 200 en sus factores primos 200 = $2^3 \times 5^2$ los factores primos son 2 y 5
2. Se aplica la fórmula $\phi(m)$ = m[1 – 1/p][1 – 1/q], en este caso p = 2 y q = 5

$\phi(200)$ = 200[1 – ½][1 – 1/5] = 200[1/2][4/5] = 80

$\phi(m.n) = \phi(m).\phi(n)$ **Si (m, n) = 1**

Ej. $\phi(15) = \phi(3).\phi(5) = 2 \times 4 = 8$

APLICACIONES DE LA CONGRUENCIA DE EULER

$7^{\phi(15)} \equiv 1(\text{mod}\,15)$, vemos que (7, 15) = 1

$\phi(15)$ = 8 entonces $7^8 \equiv 1(\text{mod}\,15)$ significa que el residuo de dividir 7^8 entre 15 es 1, veámoslo sin aplicar el teorema de Euler

$7^1 \equiv 7$ (mod 15) → $7^2 \equiv 49$ (mod 15) ≡ 4 (mod 15)

$7^4 \equiv 16$ (mod 15) → $7^4 \equiv 1$ (mod 15) →$7^8 \equiv 1$ (mod 15)

Hallar el residuo de dividir 8^{57} entre 11

$8^{\phi(11)} \equiv 1(\text{mod}\,11) \Rightarrow 8^{10} \equiv 1(\text{mod}\,11) \Rightarrow (8^{10})^5 \equiv 1^{50}(\text{mod}\,11) \Rightarrow 8^{50} \equiv 1(\text{mod}\,11)$ Ahora calcularemos lo que falta hallar que es el residuo de dividir 8^7 entre 15.

$8^1 \equiv 8$ (mod 11) → $8^2 \equiv 64$ (mod 11) → $8^2 \equiv 9$ (mod 11) →$8^2 \equiv -2$ (mod 11) → $8^6 \equiv (-2)^3$ (mod 11) → $8^6 \equiv (-2)^3$ (mod 11) → $8^6 \equiv (-8)$ (mod 11) → $8^6 \equiv 3$ (mod 11) → $8^7 \equiv 24$ (mod 11)→ $8^7 \equiv 2$ (mod 11) por lo tanto el residuo es 2

Hallar la cifra de las unidades del desarrollo de 9^{27}

Por Euler $9^{\phi(10)} \equiv 1(\text{mod}\,10) \Rightarrow 9^4 \equiv 1(\text{mod}\,10) \Rightarrow (9^4)^6 \equiv 1^6(\text{mod}\,10)$

$9^{24} \equiv 1(\text{mod}\,10)$

Falta por hallar el residuo de dividir 9^3 entre 10

$9^1 \equiv 9$(mod 10) → $9^2 \equiv 81$ (mod 10) → $9^2 \equiv 1$ (mod 10) → $9^3 \equiv 9$ (mod 10), por lo tanto **la cifra de las unidades es 9**

Hallar las dos últimas cifras del desarrollo de 37^{82}

$37^{\phi(100)} \equiv 1(\text{mod}\,100) \Rightarrow 37^{40} \equiv 1(\text{mod}\,100) \Rightarrow (37^{40})^2 \equiv 1^{80}(\text{mod}\,11) \Rightarrow 37^{80} \equiv 1(\text{mod}\,100)$

Falta calcular el residuo de dividir 37^2 entre 100

$37^1 \equiv 37$ (mod 100) → $37^2 \equiv 1369$ (mod 100) ≡ 69 (mod 100), por lo tanto **las dos últimas cifras son 69**

CONGRUENCIAS LINEALES: ax ≡ b (mod m) es una congruencia lineal y tiene solución para x si b es múltiplo del M.C.D entre a y m que se designa (a, m)

5x ≡ 2 (mod 3) tiene solución ya que 2 es múltiplo de (5, 3) = 1

12x ≡ 3(mod 6) no tiene solución ya que 3 no es múltiplo de (12, 6) = 6

1. Primer método; ax ≡ b (mod m) → ax ≡ b + mk(mod m)
   Si **5x ≡ 2(mod 3)** → 5x ≡ 2 + 3.1 (mod 3) → 5x ≡ 5(mod 3) → x ≡ 1(mod 3) → x = 1 + 3k entonces x = {1, 4, 7,…} para k ≥ 0, k Ɛ Z^+ y x = {–2, – 5, –8,…} para k Ɛ Z^-
2. Segundo método, si ax ≡ b(mod m) → x ≡ a^{-1}.b(mod m)
   5x ≡ 2(mod 3), a^{-1} es el inverso de 2 (mod 3)
   2 × 0 ≡ 0(mod 3); 2 × 1 ≡ 2(mod 3); 2 × 2 ≡ 4(mod 3) → 2 × 2 ≡ 1(mod 3) por lo tanto 2 es el inverso de 2(mod 3) → x ≡ 2 × 2(mod 3) ≡ 4(mod 3) ≡ 1(mod 3) → x = 1 + 3k
3. Tercer método, si ax ≡ b (mod m) → ax – mx ≡ b(mod m)
   5x ≡ 2(mod 3) → 5x – 3x ≡ 2(mod 3) →2x ≡ 2(mod 3) → x ≡ 1(mod 3) → x = 1 + 3k
   Resolver la congruencia 14x ≡ 8(mod 6); 8 es múltiplo de (14, 6) = 2
   Simplificamos por 2 → 7x ≡ 4(mod 3) → hallamos el inverso de 7(mod 3) → $a^{-1} = \frac{1+3k}{a} = \frac{1+3(2)}{7} = 1 \Rightarrow a^{-1} = 1 \therefore x \equiv 1 \times 4(\mathrm{mod}\, 3) \equiv 1(\mathrm{mod}\, 3) \Rightarrow x = 1 + 3k$
   Por el tercer método 7x – 3x ≡ 4(mod 3) → 4x ≡ 4(mod 3) → x ≡ 1(mod 3) → x = 1 + 3k
4. PROBLEMAS DE APLICACIÓN
   Hallar los enteros múltiplos de 7 que al dividirlos por 5 dejen un residuo de 3, entonces:
   7x ≡ 3(mod 5) → 7x – 5x ≡ 3 (mod 5) → 2x ≡ 3(mod 5) → 2x ≡ 3 + 5(mod 5) → 2x ≡ 8(mod 5) ∴ x ≡ 4 (mod 5) ∴ 7x ≡ 28(mod 5) ∴ 7x ≡ 28 + 35 k = {28, 63, 98,…} para k Ɛ Z^+ U {0} y {– 7, – 42, – 77,…} para k Ɛ Z^-

RESOLUCIÓN DE SISTEMAS DE CONGRUENCIAS

Hallar los enteros que al dividirlos por 5 y 8 dejen residuos de 2 y 3 respectivamente

Debemos resolver el sistema

X ≡ 2(mod 5) ^ x ≡ 3(mod 8); veamos las condiciones para que tenga solución son 2 – 3 debe ser múltiplo de (5, 8) = 1

De la primera obtenemos x = 2 + 5k, reemplazamos este valor de x en la segunda congruencia y obtenemos 2 + 5k ≡ 3(mod 8) → 5k ≡ (3 – 2) (mod 8) → 5k ≡ 1(mod 8) → 5k ≡ 1 + 8(3)(mod 8) → 5k ≡ 25(mod 8) → k ≡ 5(mod 8) → k = 5 + 8m, como x = 2 + 5k → x = 2 + 5(5 + 8m) → x = 27 + 40m = {27, 67, 107,…} para m entero positivo y x = {– 13, – 53, – 93,…} para m entero negativo, tener en cuenta que al dividir – 13 entre 5 el cociente es – 3 y el residuo es 2 y al dividir – 13 entre 8 el cociente es – 2 y el residuo 3

Hallar los enteros que al dividirlos por 3, 5 y 7 dejen residuos de 1, 3 y 2 respectivamente

Debemos resolver el sistema

X ≡ 1(mod 3) ^ x ≡ 3(mod 5) ^ x ≡ 2(mod 7); veamos, las condiciones son que 1 – 3 debe ser múltiplo 3, 5) = 1; 3 – 2 múltiplo de (5, 7) = 1; 1 – 2 múltiplo de (3, 7) = 1

De la primera tenemos x = 1 + 3k, reemplazamos este valor en la segunda y obtenemos 1 + 3k ≡ 3(mod 5) → 3k ≡ (3 – 1) (mod 5) → 3k ≡ 2(mod 5) → 3k – 5k ≡ 2(mod 5) → – 2k ≡ 2(mod 5) → k ≡ -1 (mod 5) → k ≡ – 1 + 5 (mod 5) → k = 4 + 5m, pero x = 1 + 3k → x = 1 + 3(4 + 5m) → x = 13 + 15m; reemplazamos este último valor en la tercera congruencia → 13 + 15m ≡ 2(mod 7) → 15m ≡ – 11 (mod 7) → 15m ≡ –11 + 2.7 (mod 7) → 15m ≡ 3(mod 7) → 15m – 2.7m ≡ 3(mod 7) → m ≡ 3(mod 7) → m = 3 + 7n, pero x = 13 + 15m → x = 13 + 15(3 + 7n) → x = 58 + 105n → x = {58, 163, 268,…} para n entero ≥ 0, averígüelo para n entero < 0

ECUACIONES DIOFANTICAS DE UNA ECUACIÓN CON DOS INCÓGNITAS

Sea la ecuación diofántica ax + by = c, para resolverla, resolveremos la congruencia ax ≡ c (mod b), como observará la condición para que tenga solución es que c sea múltiplo de (a, b)

Ejemplo resolver 3x + 7y = 8, 8 es múltiplo de (3, 7) = 1

→ 3x ≡ 8(mod 7) → 3x ≡ 1(mod 7) → 3x ≡ 1 + 7.2 (mod 7) → 3x ≡ 15(mod 7) → x ≡ 5(mod 7) → los valores de x para que y sea entero son x = {5, 12, 19,…} los valores respectivos de y son y = {– 1, – 4, – 7,…}

PROBLEMA

Se compran 12 trajes entre negros y grises por un valor 1200 Euros, los trajes negros valen 30 Euros más que los trajes grises. ¿Cuántos trajes negros y grises se compran?

Sea x el número de trajes negros, entonces 12 – x es el número de trajes grises

Sea y el valor de cada traje gris, entonces y + 30 es el precio de cada traje negro

Entonces x (y + 30) + y (12 – x) = 1200 → 5x + 2y = 200 → 5x ≡200 (mod 2) → 5x ≡ 0(mod 2) → x ≡ 0(mod 2), de donde x = 0 + 2k = {0, 2, 4, 6, 8, 10} → 12 – x = {12, 10, 8, 6, 4, 2}

Si tomamos como solución **10 trajes negros** y **2 trajes grises**

10(y + 30) + 2y = 1200 → y = 75 Euros ^ y + 30 = 75 + 30 = 105 Euros

R/ el valor de un traje gris es 75 Euros y el valor de un traje negro es 105 Euros

(10 × 105) + 2(75) = 1200 Euros

Si tomamos como solución **8 trajes negros** y **4 trajes grises**

8(y + 30) + 4y = 1200 → y = 80 ^ y + 30 = 80 + 30 = 110

R/ el valor de un traje gris es 80 Euros y el valor de un traje negro es 110 Euros

(8 × 110) + (4 × 80) = 1200 Euros

Si tomamos como solución **6 trajes negros** y **6 trajes grises**

$6(y + 30) + 6y = 1200 \rightarrow y = 85 \wedge y + 30 = 85 + 30 = 115$

R/ el valor de un traje gris es 85 Euros y el valor de un traje negro es 115 Euros

$(6 \times 115) + (6 \times 85) = 1200$, de esta misma forma podemos verificar las demás soluciones.

Carlos al comprar un artículo debe pagar 397 soles con monedas de 1 sol, 2 soles y 5 soles. Si se debe utilizar los tres tipos de monedas. ¿Cuántas monedas como mínimo se debe utilizar?

Sea x el número de monedas de 1 sol; y el número de monedas de 2 soles y z el número de monedas de 5 soles.

$X + 2y + 5z = 397$, para hallar el mínimo de monedas dividimos 397 entre 5 y nos da 79 como cociente y residuo 2 entonces serían 79 monedas de 5 soles, entonces $x + 2y = 2$ entonces $x = 0 \wedge y = 1$, pero no se emplearían monedas de 1 sol, entonces debemos utilizar 78 monedas de 5 soles, o sea $78 \times 5 = 390$, $x + 2y = 7 \rightarrow x \equiv 7 \pmod 2 \rightarrow x \equiv 1 \pmod 2$, o sea una moneda de 1 sol $y = 3$ o sea 3 monedas de 2 soles

$(1 \times 1) + (3 \times 2) + (78 \times 5) = 1 + 6 + 390 = 397$ Euros, total de monedas $1 + 3 + 78 = 82$ monedas.

El número 5X8Y3 es múltiplo de 67 ¿Cuáles deben ser los valores de X ^ Y?

$50803 + 1000X + 10Y \equiv 0(\text{mod } 67$

$50803(\text{mod } 67) + 1000X\ (\text{mod } 67) + 10Y\ (\text{mod } 67) \equiv 0\ (\text{mod } 67)$

$17 + 62X + 10Y \equiv 0 \pmod{67} \rightarrow 17 + 62X + 10Y = 67k$, como $X \wedge Y$ son dígitos, su mayor valor será $17 + 62(9) + 10(9) = 665 \rightarrow 67k = 665 \rightarrow 67k \leq 65$ de donde $k \leq 9,9$ luego k puede tomar los valores $\{1, 2, \ldots, 9\}$

Veamos para $k = 1 \rightarrow 17 + 62X + 10Y = 67 \rightarrow 62X + 10Y = 50 \rightarrow 31X + 5Y = 25 \rightarrow 31X \equiv 25 \pmod 5 \rightarrow 31X \equiv 0 \pmod 5 \rightarrow X \equiv 0 \pmod 5$ entonces $X = \{0, 5, 10, \ldots\} \rightarrow$ si $X = 0 \rightarrow y = 5$, entonces el número será $5X8Y3 = 50853$

Para $k = 2$ el problema no tiene solución

Para $k = 3$ y $k = 9$ el problema tiene más soluciones, verifíquelo el estudiante.