ARITMÉTICA MODULAR

7. Razona si el siguiente sistema de congruencias tiene solución y, en caso afirmativo, resuélvelo:

$4x - 3 \equiv 5 \pmod 6$

$6x + 1 \equiv 3 \pmod{10}$ (**Dic.15**)

Primero debemos despejar las ecuaciones.

1ª Ecuación:

$4x-3 \equiv 5 \pmod 6$ → despejamos la ecuación

$4x \equiv 5+3 \pmod 6$ → sumamos 5+3 = 8 y pasamos al módulo 8* ≡ 2 (mod 6)

$4x \equiv 2 \pmod 6$ → P Cancelativa mcd(6,2) = 2 → mod 6/2 → mod 3

$2x \equiv 1 \pmod 3$ → Inverso de 2 en módulo 3 → 2*2 = 4 ≡ 1 (mod 3) → el inverso es 2

$x \equiv 2 \pmod 3$

* PARA PASAR AL MÓDULO UN NÚMERO MÁS GRANDE: dividimos y nos quedamos con el resto de la división

2ª Ecuación:

$6x+1 \equiv 3 \pmod{10}$ → despejamos

$6x \equiv 2 \pmod{10}$ → Prop Cancelativa mcd(10,2) = 2 → mod 10/2 → mod 5

$3x \equiv 1 \pmod 5$ → Inverso de 3 en módulo 5 → 3*2 = 6 ≡ 1 (mod 5) → el inverso es 2

$x \equiv 2 \pmod 5$

Como me ha quedado el siguiente sistema, donde los módulos son primos entre sí, el sistema tiene solución.

$x \equiv 2 \pmod 3$

$x \equiv 2 \pmod 5$

Resolvemos por el TCR. El problema tiene solución en el módulo Z3*5 = Z15

- Para m1 = 3
  m/m1 = 15/3 = 5
  [m/m1]^-1 = [5]^-1 = pasamos al módulo = [2]^-1 = calculamos su inverso = [2]
- Para m2 = 5
  m/m2 = 15/5 = 3
  [m/m2]^-1 = [3]^-1 = calculamos su inverso = [2]

x1 = 2*5*2 + 2*3*2 = 20 + 12 = 32 = pasamos a módulo 15 = 2

$x = 2 + 15t,\ \forall\ t \in \mathbb{Z}$ $x \equiv 2 \pmod{15}$

8. Estudia para qué valores de c tiene solución el siguiente sistema de congruencias, y resuélvelo en dichos casos.

$x \equiv 4 \pmod{5}$
$2x \equiv c \pmod{14}$
$x \equiv 3 \pmod{7}$ **(Enero20)**

Despejamos la segunda ecuación

$2x \equiv c \pmod{14}$ → Necesitamos poder aplicar la propiedad cancelativa, ya que el inverso de 2 en Z14 no existe (de momento nos quedan las siguientes opciones: 0,2,4,6,8,10,12)

Como 14 no es primo, entonces debemos dividir la ecuación en tantas como factores primos tenga

$2x \equiv c \pmod{2}$
$2x \equiv c \pmod{7}$ → Como tenemos que $x \equiv 3 \pmod{7}$, entonces necesitamos que c sea múltiplo de 3 para que el sistema tenga solución (en este punto nos quedan las siguientes opciones: 6,12)

Si c = 6, entonces:

$2x \equiv 6 \pmod{14}$ → Propiedad Cancelativa: mcd(2,14) = 2 → mod 14/2 → mod 7
$x \equiv 3 \pmod{7}$ → Como coincide exactamente con la tercera ecuación de mi sistema, entonces tiene solución

Si c = 12, entonces:

$2x \equiv 12 \pmod{14}$ → Propiedad Cancelativa: mcd(2,14) = 2 → mod 14/2 → mod 7
$x \equiv 6 \pmod{7}$ → Como no coincide con la tercera ecuación, entonces 12 no es una posible solución de c, ya que en este caso el sistema no tendría solución

Resolvemos el sistema en el caso de que c sea igual a 6. En este caso las ecuaciones 2 y 3 son exactamente iguales, por lo que podemos prescindir de cualquiera de ellas, quedándonos el siguiente sistema:

$x \equiv 4 \pmod{5}$
$x \equiv 3 \pmod{7}$

1º Ecuación

$x \equiv 4 \pmod{5}$
$x = 4 + 5i$

2º Ecuación

$x \equiv 3 \pmod{7}$ → sustituimos
$4+5i \equiv 3 \pmod{7}$ → despejamos: 3-4 = -1 = pasamos al módulo (le sumamos 7) = 6
$5i \equiv 6 \pmod{7}$ → inverso de 5 en módulo 7 → 5*3 = 15 = pasamos a módulo 7 = 1 → el inverso es 3
$i \equiv 6*3 \pmod{7}$ → operamos y pasamos al módulo → 6*3 = 18 = pasamos a módulo 7 = 4
$i \equiv 4 \pmod{7}$
$i = 4 + 7t$
$x = 4 + 5(4 + 7t) = 24 + 35t, \ \forall\, t \in Z$ || $x \equiv 24 \pmod{35}$

RELACIONES DE RECURRENCIA

Hay dos tipos de relaciones de recurrencia. Veamos cuáles son y cómo resolverlas:

- **Homogéneas**: son del tipo $a_n + a_{n-1} + ... = 0$

  Por ejemplo: $a_n + a_{n-1} = 0$, $a_{n+1} + a_n = a_{n-3}$

  → Calculamos la ecuación característica (pasamos de a_n a una ecuación con una incógnita x y resolvemos)

  - Si las soluciones son del tipo α y β (raíces distintas), entonces $a_n = k_1 \cdot \alpha^n + k_2 \cdot \beta^n$
  - Si las soluciones son del tipo α raíz doble, entonces $a_n = (k_1 + k_2 n) \cdot \alpha^n$

  Por ejemplo:

  1. Raíces: α=1, ß=-3 → E.C. $a_n = k1 \cdot 1^n + k2 \cdot (-3)^n$
  2. Raíces: α=4 (raíz doble) → E.C. $a_n = (k1 + k2n) \cdot 4^n$
  3. Raíces: α=-1 (raíz triple) → E.C. $a_n = (k1 + k2n + k3n^2) \cdot (-1)^n$
  4. Raíces: α=2, ß = 3 (raíz doble) → E.C. $a_n = k1 \cdot 2^n + (k2 + k3n) \cdot 3^n$

  → Aplicamos las condiciones generales (proporcionadas en el problema)

1. Ejemplo básico de resolución de recurrencias homogéneas:

   $a_{n+1} = 2a_n + a_{n-1}$ cuyas condiciones iniciales (C.I.) son $a_0 = 7$, $a_1 = 3$

   - Ecuación Característica (E.C.):

     $a_{n+1} - 2a_n - a_{n-1} = 0 \rightarrow x^2 - 2x - 1 = 0$ → Resolvemos

     x = $(2 \pm \sqrt{4+4})/2 = (2 \pm 2\sqrt{2})/2 = 1 \pm \sqrt{2}$

     $\alpha = 1+\sqrt{2}$, ß = $1-\sqrt{2}$ → E.C. an = k1* $(1+\sqrt{2})^n$ + k2* $(1-\sqrt{2})^n$

   - Aplicamos Condiciones Iniciales (ACI):

     a0 = 7 = k1 + k2 → k1 = 7 - k2 = 7-7/2+2/ $\sqrt{2}$ = 7/2+2/ $\sqrt{2}$

     a1 = 3 = (7 - k2) * $(1+\sqrt{2})$ + k2* $(1-\sqrt{2})$ → $2\sqrt{2}$ k2 = 4+7 $\sqrt{2}$ → k2 = 2/ $\sqrt{2}$ + 7/2

     Sustituimos:

     an = (7/2+2/ $\sqrt{2}$)* $(1+\sqrt{2})^n$ + (7/2+2/ $\sqrt{2}$)* $(1-\sqrt{2})^n$

$a_n = 7a_{n-1} - 10a_{n-2}$, cuyas C.I. son a0 = 2, a1 = 1

- E.C.: $a_n - 7a_{n-1} + 10a_{n-2} = 0 \rightarrow x^2 - 7x + 10 = 0$
  x = $(7 \pm \sqrt{49-40})/2 = (7 \pm 3)/2 \rightarrow$ α =5; ß=2
  $a_n = k1 * 5^n + k2 * 2^n$

- ACI:
  a0 = 2 = k1 + k2 → k1 = 2-k2 = 2-3 = -1
  a1 = 1 = 5k1 + 2k2 → 1 = 5(2-k2) + 2k2 → 9 = 3k2 → k2 = 3

  Luego, sustituyendo nos queda $a_n = -5^n + 3 * 2^n$

  ****NOTA**: NO ES LO MISMO -5^n que $(-5)^n$

$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$, cuyas C.I. son a0 = 2, a1 = 5, a2 = 15

- E.C.:
  $a_n - 6a_{n-1} + 11a_{n-2} - 6a_{n-3} = 0 \rightarrow x^3 - 6x^2 + 11x - 6 = 0 \rightarrow$ RUFINI

	|1	-6	11	-6
1|		1	-5	6
	|1	-5	6	0
2|		2	-6	
	|1	-3	0	

  Luego, α = 1, ß=2 y γ =3

  $a_n = k1 * 1^n + k2 * 2^n + k3 * 3^n$
  $a_n = k1 + k2 * 2^n + k3 * 3^n$

- A.C.I.:
  a0 = 2 = k1 + k2 + k3 → k1 = 2-k2-k3 = 2 - 3 +2k3-k3 = k3 - 1 = 2-1 = 1
  a1 = 5 = k1 + 2k2 + 3k3 → 5 = 2-k2-k3 → k2 = 3-2k3 = 3 - 2 = 1
  a2 = 15 = k1 + 4k2 + 9k3 → 15 = k3-1+4(3-2k3)+9k3 → 2k3 = 4 → k3 = 2

  Luego, $a_n = 1 + 2^n + 2 * 3^n$

- **NO Homogéneas**: son del tipo $a_n + a_{n-1} + ... =$ algo_diferente_de_0 (y de a_n)

  Por ejemplo: $a_n + a_{n-2} = 2 * (-1)^n$, $a_{n+1} + a_n = 2$, $a_{n+1} + a_n = 2n^2 - 1 * 1\hat{}n$

  → Calculamos la homogénea asociada (ecuación característica del problema sin tener en cuenta la parte que hace que la recurrencia sea NO Hom.)

  → Calculamos la solución particular ayudándonos de la tabla adjunta*

g(n) → Parte NO Homogénea	**Ecuación característica de C(x)**	**p(n) → Solución particular**
c·b^n	b no raíz de C(x)	k*b^n
c·b^n	b raíz de C(x) con multiplicidad s	k*n^s*b^n
polinomio	1 no raíz de C(x)	polinomio del mismo grado
polinomio	1 raíz de C(x) con multiplicidad s	n^s*(polinomio del mismo grado)

  * **OJO!!** A si es raíz y su multiplicidad (número de veces que es raíz, es decir, si es raíz doble (2), simple (1), triple(3), …)

  → Sumamos ambas soluciones (las halladas en los dos pasos anteriores)

  → Aplicamos las condiciones generales (proporcionadas en el problema)

2. Resolución de recurrencias no homogéneas:

a) $a_n = a_{n-1} + 6a_{n-2} + 2^n$
   $a_0 = 0,\ a_1 = 1$

b) $a_n - 3a_{n-1} = 3^n \cdot 5$
   $a_0 = 2$

c) $a_n = 6a_{n-1} - 9a_{n-2} + 2 \cdot 3^n$
   $a_0 = 0,\ a_1 = 6$

d) $a_{n+2} - 6a_{n+1} + 9a_n = 3 \cdot 2^n + 7 \cdot 3^n$
   $a_0 = 1,\ a_1 = 4$

e) $a_{n+1} - 2a_n = 5$
   $a_0 = 1$

f) $a_n = a_{n-1} + 2n - 1$
   $a_0 = 1$

g) $a_n = 4a_{n-1} - 4a_{n-2} + n$
   $a_0 = 1,\ a_1 = 3$

h) $a_n = 3a_{n-1} - 4a_{n-3} + n^2$
   $a_0 = 11,\ a_1 = 1,\ a_2 = -1$

a) $a_n = a_{n-1} + 6a_{n-2} + 2^n \rightarrow$ NO HOMOGÉNEA

$a_0 = 0,\ a_1 = 1$

- E.C.: $a_n - a_{n-1} - 6a_{n-2} = 0 \rightarrow x^2 - x - 6 = 0$
  x = $(1 \pm \sqrt{1+24})/2 = (1 \pm 5)/2 \rightarrow$ α=3; ß=-2
  $a_n = k1 * 3^n + k2 * (-2)^n$

- Solución Particular (S.P.):
  g(n)= $2^n \rightarrow$ TABLA: c* b^n donde b=2 NO es raíz $\rightarrow$ p(n) = k* 2^n
  $a_n - a_{n-1} - 6a_{n-2} = 2^n$
  k* $2^n - k * 2^{n-1} - 6k * 2^{n-2} = 2^n$
  Divido por $2^{n-2} \rightarrow$ k* $2^{n-n+2} - k * 2^{n-1-n+2} - 6k * 2^{n-2-n+2} = 2^{n-n+2}$
  4k-2k-6k = 4 $\rightarrow$ k = -1 $\rightarrow$ p(n) = - 2^n

- Sumamos Ambas Soluciones (SAS):
  $a_n = k1 * 3^n + k2 * (-2)^n - 2^n$

- ACI:
  a0 = 0 = k1 + k2 - 1 $\rightarrow$ k1 = 1-k2 = 1
  a1 = 1 = 3k1-2k2-2 $\rightarrow$ 1 = 3(1-k2) -2k2 -2 $\rightarrow$ k2 = 0

  Luego, $a_n = 3^n - 2^n$

b) $a_n - 3a_{n-1} = 3^n \cdot 5$

$a_0 = 2$

- EC: x - 3 = 0 $\rightarrow$ x = 3 $\rightarrow$ $a_n = k1 * 3^n$
- SP:
  g(n) = 5* 3^n $\rightarrow$ TABLA: c* b^n , donde b=3 es raíz simple (multiplicidad = 1) $\rightarrow$ p(n) = k*n^1* 3^n
  p(n) = kn 3^n
  kn3^n - 3k(n-1)3^(n-1) = 5*3^n
  Divido por 3^(n-1) $\rightarrow$ kn3^(n-n+1) - 3k(n-1)3^(n-1-n+1) = 5*3^(n-n+1)
  3kn-3k(n-1) = 5*3 $\rightarrow$ 3kn-3kn+3k = 15 $\rightarrow$ k = 5 $\rightarrow$ p(n) = 5n*3^n

- SAS:
  $a_n = k1 * 3^n + 5n * 3^n$ $\rightarrow$ an = (k1 + 5n) $* 3^n$

- ACI:
  a0 = 2 = (k1 + 5*0) $\rightarrow$ k1 = 2
  Luego, an = (2 + 5n) $* 3^n$

f) $a_n = a_{n-1} + 2n - 1$

$a_0 = 1$

- E.C.: $a_n - a_{n-1} = 0$ → x - 1 = 0 → x = 1 → $a_n = k1 * 1^n$ → $a_n = k1$
- S.P.:

  g(n) = 2n -1 → TABLA: polinomio, donde 1 es raíz simple (multiplicidad = 1) → p(n) = n^1(a+bn)

  p(n) = (an+bn^2)

  an+bn^2 - (a(n-1)+b(n-1)^2) = 2n-1

  an + bn^2 - an +a - bn^2 +2bn -b = 2n - 1

  2bn +a-b = 2n-1

  Para n → 2b = 2 → b = 1

  Para el término independiente → a-b = -1 → a = 1-1 = 0

  p(n) = n^2

- SAS:

  $a_n = k1 +$ n^2

- ACI:

  a0 = 1 = k1

  Luego, $a_n = 1 + n^2$

e) $a_{n+1} - 2a_n = 5$

$a_0 = 1$

- EC:

  $a_{n+1} - 2a_n = 0$ → x - 2 = 0 → x = 2 → $a_n = k1 * 2^n$

- SP:

  g(n) = 5 → TABLA: polinomio, donde 1 NO es raíz → p(n) = a

  a -2*a = 5 → a = -5 → p(n) = -5

- SAS:

  $a_n = k1 * 2^n$ -5

- ACI:

  a0 = 1 = k1 - 5 → k1 = 6

  Luego, $a_n = 6 * 2^n - 5$