ARITMÉTICA MODULAR

1. Siete ladrones tratan de repartirse entre ellos, a partes iguales, un botín de monedas de oro. Desafortunadamente, sobran seis monedas en el reparto por lo que los ladrones acaban peleando y muere uno de ellos. Vuelven a intentar el reparto y ahora sobran dos monedas. Se desata entonces una nueva pelea y muere otro de los ladrones. En el siguiente reparto vuelve a sobrar una moneda, y sólo después de que muera otro ladrón es posible repartir las monedas a partes iguales. ¿Cuál es el mínimo número de monedas para que esto suceda? (**Julio14**)

$x \equiv 6 \pmod 7$

$x \equiv 2 \pmod 6$ Como los módulos no son primos entre sí, entonces no podemos aplicar el TCR

$x \equiv 1 \pmod 5$

$x \equiv 0 \pmod 4$

- 1º Ecuación:

  $x \equiv 6 \pmod 7$

  $x = 6 + 7i$

- 2º Ecuación:

  $x \equiv 2 \pmod 6$ → sustituyo la x por lo hallado en la ecuación anterior

  $6 + 7i \equiv 2 \pmod 6$ → paso al módulo

  $i \equiv 2 \pmod 6$

  $i = 2 + 6j$ → sustituyo la i en la ecuación anterior

  $x = 6 + 7(2 + 6j) = 20 + 42j$

- 3º Ecuación:

  $x \equiv 1 \pmod 5$ → sustituyo la x por lo hallado en la ecuación anterior

  $20 + 42j \equiv 1 \pmod 5$ → paso al módulo

  $2j \equiv 1 \pmod 5$ → hallamos el inverso de 2 en módulo 5*

  $j \equiv 3 \pmod 5$

  $j = 3 + 5k$ → sustituyo la j en la ecuación anterior

  $x = 20 + 42(3 + 5k) = 146 + 210k$

- 4º Ecuación:

  $x \equiv 0 \pmod 4$ → sustituyo la x por lo hallado en la ecuación anterior

  $146 + 210k \equiv 0 \pmod 4$ → paso al módulo

  $2 + 2k \equiv 0 \pmod 4$ → despejamos

  $2k \equiv -2 \pmod 4$ → pasamos al módulo

  $2k \equiv 2 \pmod 4$ → Aplicamos la propiedad cancelativa: $ac\,x \equiv bc \pmod m$

  $k \equiv 1 \pmod{4/2}$ $\qquad ax \equiv bc (\bmod\ m/\text{mcd}(m,c))$

  $k \equiv 1 \pmod 2$

  $k = 1 + 2t$ → sustituyo la k en la ecuación anterior

$x = 146 + 210(1+2t) = 356 + 420t, \ \forall\ t \in Z$

* Buscamos un número que multiplicado por 2 y dividirlo entre 5 me dé de resto 1 → 2*6 = 6 = paso al módulo = 1

* Otra opción es con la ecuación diofántica 2x + 5y = 1 y nos quedamos con la solución particular de x (x1). Si es negativo le sumo el módulo.

Luego, el mínimo número de monedas posible para que esto suceda es cuando t=0, es decir, 356 monedas de oro.

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

$514x \equiv 16 \pmod{40}$

$40x \equiv 12 \pmod{38}$ Como los módulos no son primos entre sí, no podemos hacerlo con el TCR

$64x \equiv 16 \pmod{45}$ (**Oct.15 - MATES**)

Pasamos las ecuaciones al módulo:

$34x \equiv 16 \pmod{40}$

$2x \equiv 12 \pmod{38}$

$19x \equiv 16 \pmod{45}$

Despejamos las ecuaciones:

$x \equiv 4 \pmod{20}$

$x \equiv 6 \pmod{19}$

$x \equiv 34 \pmod{45}$

Descomponemos en factores primos:

$x \equiv 4 \pmod{2^2} \rightarrow x \equiv 0 \pmod{4}$

$x \equiv 4 \pmod{5} \rightarrow x \equiv 4 \pmod{5}$

$x \equiv 6 \pmod{19} \rightarrow x \equiv 6 \pmod{19}$

$x \equiv 34 \pmod{3^2} \rightarrow x \equiv 7 \pmod{9}$

$x \equiv 34 \pmod{5} \rightarrow x \equiv 4 \pmod{5}$

pasamos al módulo

1º Ecuación

$34x \equiv 16 \pmod{40}$ → Prop. Cancelativa

$17x \equiv 8 \pmod{40/2}$

$17x \equiv 8 \pmod{20}$ → Hallo el inverso de 17 en módulo 20

$x \equiv 8*13 \pmod{20}$ → 8*13 = 104 = pasamos al módulo = 4

$x \equiv 4 \pmod{20}$

Ecuación Diofántica: 17x + 20y = 1

20 = 17*1 + 3

17 = 3*5 + 2

3 = 2*1 + 1 ← d = mcd(17,20)

2 = 1*2 + 0

¿1|1? → Sí

1 = 3 + 2(-1)

1 = 3 + (17 + 3(-5))(-1) → 1 = 17(-1) + 3*6

1 = 17(-1) + (20 + 17(-1))*6 → 1 = 20*6 + 17(-7)

Luego, el inverso de 17 es -7+20 = 13

2º Ecuación

$2x \equiv 12 \pmod{38}$ → Prop. Cancelativa

$x \equiv 6 \pmod{38/2}$

$x \equiv 6 \pmod{19}$

3º Ecuación

$19x \equiv 16 \pmod{45}$ → Inverso de 19 en módulo 45

$x \equiv 16*19 \pmod{45}$ → 16*19 = 304 = pasamos al módulo = 34

$x \equiv 34 \pmod{45}$

Ecuación Diofántica: $19x + 45y = 1$

$45 = 19*2 + 7$
$19 = 7*2 + 5$
$7 = 5*1 + 2$
$5 = 2*2 + 1 \leftarrow d = mcd(19,45)$
¿1|1? → Sí

$1 = 5 + 2(-2)$
$1 = 5 + (7 + 5(-1))(-2) \rightarrow 1 = 7(-2) + 5*3$
$1 = 7(-2) + (19 + 7(-2))*3 \rightarrow 1 = 19*3 + 7(-8)$
$1 = 19*3 + (45 + 19(-2))(-8) \rightarrow 1 = 45(-8) + 19*19$
Luego, el inverso de 19 es 19

Luego, me queda el sistema de congruencias siguiente:

$x \equiv 0 \pmod{4}$
$x \equiv 4 \pmod{5}$
$x \equiv 6 \pmod{19}$
$x \equiv 7 \pmod{9}$

Como los módulo son primos entre sí, ahora sí que podemos aplicar el TCR
El sistema tiene solución en el módulo Z4*5*19*9 = Z3420

Para m1 = 4 → como a1 = 0 no hallo los cálculos
Para m2 = 5:
m/m1 = 3420/5 = 684
[m/m1]^-1 = [684]^-1 = pasamos al módulo = [4]^-1 = hallamos el inverso = [4]

Para m3 = 19:
m/m3 = 3420/19 = 180
[m/m3]^-1 = [180]^-1 = pasamos al módulo = [9]^-1 = hallamos el inverso = [17]

Ecuación Diofántica: $9x + 19y = 1$

$19 = 9*2 + 1 \leftarrow d = mcd(9,19)$
$9 = 1*9 + 0$
¿1|1? → Sí

$1 = 19 + 9(-2)$
Luego, el inverso de 9 es -2 + 19 = 17

Para m4 = 9
m/m4 = 3420/9 = 380
[m/m4]^-1 = [380]^-1 = pasamos al módulo = [2]^-1 = hallamos el inverso = [5]

x1 = 0 + 4*684*4 + 6*180*17 + 7*380*5 = 31804 = pasamos al módulo = 1024
Luego, $x = 1024 + 3420t, \forall t \in Z$

Notación: $x \equiv 1024 \pmod{3420}$

3. Resuelve el siguiente sistema de congruencias:

$6x \equiv 12\ (mod\ 15)$

$6!x \equiv 2\ (mod\ 7)$ Como los módulos no son primos entre sí, no podemos aplicar el TCR

$3x \equiv 1\ (mod\ 10)$ (**Enero16**)

1º Ecuación

$6x \equiv 12 (\text{mod } 15)$ → Prop. Cancelativa: como mcd(6,15) = 3 → mod 15/3 → mod 5

$x \equiv 2 (\text{mod } 5)$

$x = 2 + 5i$

2º Ecuación

$6!x \equiv 2\ (\text{mod } 7)$ → Tma Wilson: $(p-1)! \equiv -1\ (\text{mod } p)$

$-1x \equiv 2\ (\text{mod } 7)$ → pasamos al módulo

$6x \equiv 2\ (\text{mod } 7)$ → Prop Cancelativa: como mcd(2,7) = 1 → mod 7/1 → mod 7

$3x \equiv 1\ (\text{mod } 7)$ → Inverso de 3 en módulo 7 = 5 → 3*5 = 15 = pasamos al módulo = 1

$x \equiv 5\ (\text{mod } 7)$ → sustituimos

$2 + 5i \equiv 5\ (\text{mod } 7)$ → despejamos

$5i \equiv 3\ (\text{mod } 7)$ → inverso de 5 en módulo 7 = 3

$i \equiv 9\ (\text{mod } 7)$ → pasamos al módulo

$i \equiv 2\ (\text{mod } 7)$

$i = 2 + 7j$ → sustituimos

$x = 2 + 5(2 + 7j) = 12 + 35j$

3º Ecuación

$3x \equiv 1\ (\text{mod } 10)$ → inverso de 3 en módulo 10 = 7

$x \equiv 7\ (\text{mod } 10)$ → sustituimos

$12+35j \equiv 7\ (\text{mod } 10)$ → pasamos al módulo (dividimos el número entre el módulo y nos quedamos con el resto)

$2+5j \equiv 7 (\text{mod } 10)$ → despejamos

$5j \equiv 5\ (\text{mod } 10)$ → Prop Cancelativa: mcd(5,10) = 5 → mod 10/5 → mod 2

$j \equiv 1\ (\text{mod } 2)$

$j = 1+2t$ → sustituimos

$x = 12 + 35(1 + 2t) = 47 + 70t,\ \forall\ t \in Z$

También: $x \equiv 47\ (\text{mod } 70)$

También: $\overline{x} \equiv \overline{47}$

También: $x \equiv [47]_{70}$

4. Resuelve el siguiente sistema de congruencias:

$5!x \equiv 3\ (mod\ 7)$

$14x \equiv 2\ (mod\ 20)$ Como los módulos no son primos entre sí, no podemos aplicar TCR

$x \equiv 17\ (mod\ 18)$ **(Julio16)**

1º Ecuación

5!x ≡ 3 (mod 7) → **Tma Wilson**: como no tenemos 6! (mod 7), donde 7 es primo, entonces 5! ≡ 1 (mod 7)

x ≡ 3 (mod 7)

x = 3 + 7i

2º Ecuación

14x ≡ 2(mod 20) → Prop. Cancelativa → mcd(2,20) = 2 → mod 20/2 → mod 10

7x ≡ 1(mod 10) → Inverso de 7 en módulo 10 = 3

x ≡ 3 (mod 10) → sustituimos

3 + 7i ≡ 3 (mod 10) → despejamos

7i ≡ 0 (mod 10) → no me merece la pena calcular el inverso de 7 ya que lo multiplico por 0

i ≡ 0 (mod 10)

i = 10j → sustituyo

x = 3 + 7 * 10j = 3+70j

3º Ecuación

x ≡ 17 (mod 18) → sustituyo

3 + 70j ≡ 17 (mod 18) → despejo y paso al módulo

16j ≡ 14 (mod 18) → Prop Cancelativa: mcd(2,18) = 2 → mod 18/2 → mod 9

8j ≡ 7 (mod 9) → Inverso de 8 en módulo 9 = 8 → 8*8 = 64 = pasamos al módulo = 1

j ≡ 7*8 (mod 9) → 7*8 = 56 = pasamos al módulo = 2

j ≡ 2 (mod 9)

j = 2 + 9t → sustituyo

x = 3 + 70(2+9t) = 143 + 630t, ∀ t ∈ Z

5. El sistema planetario de la estrella Beta consta de tres planetas: Lirón, Maneto y Nurbia. La nave espacial Alfa23 dispone de los siguientes datos astronómicos: Lirón se alineará con la nave dentro de 12 meses sidéreos y tiene un período de 15 meses, Maneto lo hará dentro de 3 meses y su período es de 14 meses y, finalmente, Nurbia se alineará dentro de 9 meses y su período es de 11 meses. ¿Cuándo se producirá la próxima conjunción planetaria?
(Oct14 - MATES)

$x \equiv 12 \pmod{15}$

$x \equiv 3 \pmod{14}$ Como los módulos son primos entre sí, se puede aplicar el TCR

$x \equiv 9 \pmod{11}$ El sistema tiene solución en Z15*14*11 = Z2310

Para m1 = 15
m/m1 = 2310/15 = 154
[m/m1]^-1 = [154]^-1 = pasamos al módulo = [4]^-1 = calculamos su inverso = [4]

Para m2 = 14
m/m2 = 2310/14 = 165
[m/m2]^-1 = [165]^-1 = pasamos al módulo = [11]^-1 = calculamos su inverso = [9]

Para m3 = 11
m/m3 = 2310/11 = 210
[m/m3]^-1 = [210]^-1 = pasamos al módulo = [1]^-1 = calculamos su inverso = [1]

x1 = 12*154*4 + 3*165*9 + 9*210*1 = 13737 = pasamos al módulo = 2187
$x = 2187 + 2310t, \ \forall \ t \in Z$

Luego, la próxima conjunción planetaria será dentro de 2187 meses.

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

$5x \equiv 11 \pmod{4!}$ Como 4! = 24, y mcd(24,9) = 1, entonces podemos aplicar el TCR

$7x \equiv 1 \pmod{9}$ El sistema tiene solución en Z24*9 = Z216 (**Julio19**)

Despejamos los sistemas

$5x \equiv 11 \pmod{24}$ → Inverso de 5 en Z24 = 5 → $x \equiv 55 \pmod{24}$ → pasamos al módulo → $x \equiv 7 \pmod{24}$

$7x \equiv 1 \pmod{9}$ → Inverso de 7 en Z9 = 4 → $x \equiv 4 \pmod{9}$

Descomponemos en factores primos:

$x \equiv 7 \pmod{2^3}$

$x \equiv 7 \pmod{3}$

$x \equiv 4 \pmod{3^3}$

Pasamos al módulo

$x \equiv 7 \pmod{8}$

$x \equiv 1 \pmod{3}$ ←prescindimos de ella, ya que tiene un exponente menor

$x \equiv 4 \pmod{9}$ ← con las dos restantes aplicamos el TCR

El problema tiene solución en Z9*8 = Z72

Para m1 = 8

m/m1 = 72/8 = 9

[m/m1]^-1 = [9]^-1 = pasamos al módulo = [1]^-1 = calculamos el inverso = [1]

Para m2 = 9

m/m2 = 72/9 = 8

[m/m2]^-1 = [8]^-1 = calculamos el inverso = [8]

x1 = 7*9*1 + 4*8*8 = 63 + 256 = 319 = pasamos al módulo = 31

$x = 31 + 72t, \ \forall\, t \in Z$