ARITMÉTICA MODULAR

PROPIEDAD CANCELATIVA

ab x ≡ ac (mod m) → Podemos quitarnos lo común en ambos lados de la igualdad (**<u>TODO</u>** lo común, es decir, elevado al <u>máximo</u> exponente posible)
b x ≡ c (mod m/ mcd(m,a))

b) Resuelve la ecuación $2018^{2018}x \equiv 18 \pmod{50}$ (**Oct.18 - MATES**)

Resolvemos 2018^2018 en módulo 50: primero pasamos 2018 a módulo 50 (resto de la división)
18^2018x ≡ 18(mod 50)
18*18^2017 x ≡ 18 (mod 50) → Propiedad cancelativa
18^2017 x ≡ 1 (mod 50/mcd(18,50)) → 50/mcd(18,50) → 50/2 → 25
18^2017 x ≡ 1 (mod 25) → como mcd(18, 25) = 1, entonces podemos aplicar el **Tma Euler**

Tma Euler: 18^ φ (25) ≡ 1(mod 25)
Calculamos φ (25) = φ (5^2) = 5^2 - 5^1 = 25 - 5 = 20. Luego 18^20 ≡ 1 (mod 25)

18^2017 = 18^(20*100+17) = (18^20)^100 * 18^17 = 1^100 * 18^17 = 18^17 = 18^(20-3) = 18^20 * 18^-3 =
= 18^(-1*3) = (18^(-1))^3 = 7^3 = 49*7 = pasamos al módulo = 24*7 = 168 = pasamos al módulo = 18

Otra forma posible y un poco simplificada sería 49*7 = pasamos al módulo = (-1)*7 = -7 = pasamos al módulo = 18

49 en Z25 es lo mismo que 24, pero también que -1

Calculamos el inverso de 18 en módulo 25
18x + 25y = 1

25 = 18*1 + 7	1 = 4 + 3(-1)	
18 = 7*2 + 4	1 = 4 + (7 + 4(-1))(-1)	→ 1 = 7(-1) + 4*2
7 = 4*1 + 3	1 = 7(-1) + (18 + 7(-2))*2	→ 1 = 18*2 + 7*(-5)
4 = 3*1 + 1 ← d = mcd(18,25)	1 = 18*2 + (25 + 18(-1))(-5)	→ 1 = 25(-5) + 18*7
3 = 1*3 + 0		
¿1|1? → Sí, hay una única solución posible	Luego, el inverso de 18 en módulo 25 es 7	

18^2017 x ≡ 1 (mod 25)
18 x ≡ 1 (mod 25) → Despejamos la x (calculamos el inverso de 18 en Z25) → es 7 (lo hemos calculado antes)
x ≡ 7 (mod 25)
x = 7 + 25 t, con t = 0 **= {0, 1, …, d-1}. Como d = 1, entonces t = 0 nada más**→ Luego x = 7

c) Resuelve la ecuación $2018^{2017}x \equiv 40 \pmod{46}$ (**Oct.17 - MATES**)

Lo primero que hacemos es pasar 2018 a módulo 46:

40^2017 x ≡ 40 (mod 46)

40*40^2016 x ≡ 40 (mod 46) → Propiedad cancelativa

40^2016 x ≡ 1 (mod 46/mcd(46,40)) → 46/mcd(40,46) = 46/2 = 23

40^2016 x ≡ 1 (mod 23) → Pasamos 40 a módulo 23

17^2016 x ≡ 1 (mod 23) → Como mcd(17,23) = 1, entonces podemos aplicar el **Tma Euler**

Tma Euler: 17^ φ(23) ≡ 1(mod 23)

Calculamos φ(23) = 23^1 - 23^0 = 22

Luego, 17^22 ≡ 1(mod 23)

17^2016 = 17^(22*91+14) = (17^22)^91 * 17^14 = 1^91 * 17^14 = 17^14 = 17^(22-8) = 17^22 * 17^-8 =
= 17^(-1*8) = (17^(-1))^8 = (-4)^8 = (-4)^2 *(-4)^2 *(-4)^2 = 16*16*16 = 4096 = pasamos al módulo = 2

Calculamos el inverso de 17 en módulo 23

17x + 23y = 1

23 = 17*1 + 6

17 = 6*2 + 5

6 = 5*1 + 1 ← d = mcd(17, 23)

5 = 1*5 + 0

¿1|1? → Sí

1 = 6 + 5(-1)

1 = 6 + (17+6*(-2))(-1) → 1 = 17*(-1) + 6*3

1 = 17*(-1) + (23 + 17(-1))*3 → 1 = 23*3 + 17*(-4)

Luego, el inverso de 17 en Z23 es -4 + 23 = 19

17^2016 x ≡ 1 (mod 23)

2 x ≡ 1 (mod 23) → Calculamos el inverso de 2 en Z23 (como 12*2 = 24 ≡ 1 en módulo 23,
entonces 12 es el inverso de 2 en Z23)

x ≡ 12 (mod 23)

Como el mcd(2,23) = 1, entonces hay una única solución posible

x = 12 + 23*t, con t = 0 → Luego, x = 12

d) Halla, si existen, los inversos de $\overline{11}$ y $\overline{22}$ en Z72

Un número a tiene inverso en un módulo m ↔ mcd(m,a) = 1, es decir, son primos entre sí

Como mcd(22,72) = 2, entonces no existe el inverso de 22 en Z72

Como mcd(11,72) = 1, entonces existe el inverso de 11 en Z72. Lo calculamos:

11x + 72y = 1

72 = 11*6 + 6

11 = 6*1 + 5

6 = 5*1 + 1 ← d = mcd(72,11)

5 = 1*5 + 0

¿1|1? → Sí

1 = 6 + 5(-1)

1 = 6 + (11 + 6(-1))(-1) → 1 = 11(-1) + 6*2

1 = 11(-1) + (72 + 11(-6))*2 → 1 = 72 * 2 + 11 (-13)

Luego, el inverso de 11 en Z72 es -13+72 = 59

e) Resuelve la ecuación $\overline{1809^{2016}}\,\overline{x} \equiv \overline{27}$ en Z75 (**Oct.16 - MATES**)

1809^2016 x ≡ 27 (mod 75) → pasamos 1809 a módulo 75

9^2016 x ≡27 (mod 75)

9*9^2015 x ≡9*3 (mod 75) → Propiedad cancelativa

9^2015 x ≡ 3 (mod 75/mcd(75,9))

9^2015 x ≡ 3 (mod 75/3)

9^2015 x ≡ 3 (mod 25) → Me intento quitar la potencia con el Teorema de Euler

Como mcd(9,25) = 1, entonces podemos aplicar el Tma Euler y nos queda 9^ φ(25) ≡ 1 (mod 25)

Calculamos φ (25) = φ (5^2) = 5^2 - 5^1 = 25 - 5 = 20. Luego 9^20 ≡ 1 (mod 25)

9^2015 = 9^(20*100 + 15) = (9^20)^100 * 9^15 = 1^100 * 9^15 = 9^15

9^15 x ≡ 3 (mod 25) → Aplicamos la propiedad cancelativa

3^30 x ≡3 (mod 25)

3*3^29 x ≡3 (mod 25)

3^29 x ≡1 (mod 25/mcd(25,3)) → mcd(25,3) = 1 → 25/1 = 25

3^29 x ≡1 (mod 25) → como mcd(3,25) = 1, podemos aplicar el Tma Euler: 3^ φ(25) ≡ 1 (mod 25)

3^20 ≡ 1 (mod 25)

3^29 = 3^(20 + 9) = 3^20 * 3^9 = 3^9 = 3^3 * 3^3 * 3^3 = 27 * 27 * 27 = (pasamos al módulo) = 2 * 2 * 2 = 8

8x ≡ 1 (mod 25) → despejamos x (calculamos el inverso de 8 en Z25)

8x + 25y = 1   1 = 25 + 8(-3)

25 = 8*3 + 1 ← d = mcd(25,8)

8 = 1*8 + 0   Luego, el inverso de 8 en módulo 25 es -3 + 25 = 22

¿1|1? → Sí, tenemos una única solución posible a la ecuación

x ≡1*22 (mod 25)

x ≡ 22 (mod 25)

x = 22 + 25 t, con t = 0 → x = 22

f) Resuelve la siguiente ecuación $8!x \equiv 21^{18}$ (mod 11) (**Julio12**)

Factorial de un número: 5! = 1*2*3*4*5 = 120

TEOREMA DE WILSON (generalizado):

$\prod_{1 \le a < n} a \equiv -1 \ (mod\ n)$ si n = 4, p^k, $2p^k$, donde p = número primo y k = número natural

$\prod_{1 \le a < n} a \equiv 1 (\text{mod n})$ en otro caso

$8!x \equiv 21^{18}$ (mod 11)	→ Aplicamos el Tma Wilson: 8! ≡(-1) (mod 11)
(-1)x ≡21^18 (mod 11)	→ Pasamos -1 a módulo 11 y me queda 10
10x ≡21^18 (mod 11)	→ Pasamos 21 a módulo 11 y me queda 10
10x ≡10^18 (mod 11)	→ Simplificamos aplicando la Propiedad Cancelativa
10x ≡10*10^17 (mod 11)	
x ≡10^17 (mod 11/mcd(10,11))	→ 11/mcd(10,11) = 11/1 = 11
x ≡10^17 (mod 11)	→ Como mcd(10,11) = 1 y 11 es primo, podemos aplicar el **Tma Fermat**

Tma Fermat: 10^(11-1) ≡1 (mod 11) → 10^10 ≡1 (mod 11)
10^17 = 10^(10+7) = 10^10 * 10^7 = 10^7 = 10^(10-3) = 10^10 * 10^(-3) = 10^(-1*3) = (10^-1)^3 = 10^3 =
= 1000 = pasamos al módulo = 10

Calculamos el inverso de 10 en módulo 11
10x + 11y = 1

11 = 10*1 + 1 ← d = mcd(11,10)	1 = 11 + 10(-1)
10 = 1*10 + 0	
¿1|1? → Sí	Luego, el inverso de 10 en módulo 11 es -1 + 11 = 10

x ≡10^17 (mod 11)
x ≡10 (mod 11)
x = 10 + 11 t, con t = 0 → Luego, x = 10

SISTEMAS DE CONGRUENCIA

TEOREMA CHINO DEL RESTO

Si tenemos un sistema de congruencias:

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$ donde mcd(mi,mj) = 1, $\forall$ i $\neq$ j $\rightarrow$ los módulos son primos entre sí

… el sistema tiene solución en Zm, donde m = m1*m2*...*mn

$x \equiv a_n \pmod{m_n}$

Entonces, $x1 = \sum_{i=1}^{n} a_i \cdot \frac{m}{m_i} \cdot \left[\frac{m}{m_i}\right]_{m_i}^{-1}$ y x = x1 + mt, $\forall$ t $\in$ Z

1. Aplicando el Teorema Chino del Resto, hallar tres números enteros consecutivos que sean divisibles, respectivamente, por los cuadrados de 2, 3 y 5. (**Enero12**)

$x - 2 \equiv 0 \pmod{4}$ Como los módulos son primos entre sí, podemos aplicar el **TCR**

$x - 1 \equiv 0 \pmod{9}$ El sistema solución en Z4*9*25 = Z900

$x \equiv 0 \pmod{25}$

Despejamos las ecuaciones:

$x \equiv 2 \pmod{4}$

$x \equiv 1 \pmod{9}$

$x \equiv 0 \pmod{25}$

- Para m1 = 4

m/m1 = 900/ 4 =225

[m/m1]^-1 = [225]^-1 = pasamos al módulo = [1]^-1 = calculamos el inverso = 1

- Para m2 = 9

m/m2 = 900/9 = 100

[m/m2]^-1 = [100]^-1 = pasamos al módulo = [1]^-1 = calculamos el inverso = 1

- Para m3 = 25 → como a3 = 0, no necesito hacer los cálculos de este módulo

Luego, x1 = 2*225*1 + 1*100*1 + 0*?? = 550

Por lo que, x = 550 + 900 t, $\forall$ t $\in$ Z

Una posible solución serían los números 548, 549, 550.

2. Un padre dispone de cierto número de monedas de oro, comprendidas entre 1500 y 2000. Las pretende repartir entre sus 10 hijos, entre los que hay 7 chicas y 3 chicos. Si en el reparto sólo intervienen los chicos, sobran 2 monedas de oro, si sólo intervienen las chicas sobran otras 2 monedas, mientras que si intervienen todos sobran 4 monedas. ¿Cuántas monedas de oro tiene? (**Enero15**)

$x \equiv 2 \pmod 3$	Como los módulos son primos entre sí, entonces podemos aplicar el **TCR**
$x \equiv 2 \pmod 7$	El sistema tiene solución en Z3*7*10 = Z210
$x \equiv 4 \pmod{10}$	

- Para m1 = 3
  m/m1 = 210/3 = 70
  [m/m1]^-1 = [70]^-1 = pasamos al módulo = [1]^-1 = calculamos el inverso = 1

- Para m2 = 7
  m/m2 = 210 /7 = 30
  [m/m2]^-1 = [30]^-1 = pasamos al módulo = [2]^-1 = calculamos el inverso = 4

  Buscamos el inverso de 2 en Z7 → tengo que encontrar un número que multiplicado por 2 me dé 7k+1
  Busco un número que me dé 8,15,22, …
  Como 2*4 = 8 = pasamos al módulo = 1

  Si no, ecuación diofántica: 2x + 7y = 1 y nos quedamos con x1 (si es negativo, le sumo el módulo 7)

- Para m3 = 10
  m/m3 = 210/10 = 21
  [m/m3]^-1 = [21]^-1 = pasamos al módulo = [1]^-1 = calculamos el inverso = 1

Luego x1 = 2*70*1 + 2*30*4 + 4*21*1 = 464 = pasamos al módulo = 44
Por lo que x = 44 + 210 t, $\forall t \in Z$

Para t = 7 → x = 1514
Para t = 8 → x = 1724
Para t = 9 → x = 1934
Para cualquier otra t no llego o me paso del número de monedas posible.

Por lo que puede tener 1514, 1724 ó 1934 monedas de oro.