CONGRUENCIA EN Z

I. CONGRUENCIAS

1. Indicar Verdadero o Falso, justificando:

   a) 541 ≡ 100 (3)
   b) 327 ≡ 3 (8)
   c) 21 ≡ -4 (5)
   d) 3795 ≡ 0 (11)
   e) $\bar{2}\ (10) \subseteq \bar{2}(5)$
   f) $\bar{3}\ (6) \subseteq \bar{4}(5) = \phi$
   g) *a* ≡ 0 (2) => *a* ≡ 0 (4)
   h) *a* ≡ b (2) <=> *a* + b ≡ 0 (2)

2. Se sabe que en Z^+ cumple: n ≡ 3 (7) ^ n ≡ 2 (8), se pide:

   a) Hallar los dos números que cumplen eso y son menores que 100.
   b) Demostrar que todos los números que verifican esas condiciones son n ≡ 10 (56)

3. Hallar todos los enteros positivos n que sean congruentes a 2 tanto en módulo 3 como módulo 4 y módulo 5.

4. Demostrar las siguientes propiedades*:*

   a) *a ≡ b (n) ^ c ≡ d (n) => a . c ≡ b . d (n)*
   b) *a ≡ b (n) ^ c ≡ d (n) => a - c ≡ b - d (n)*
   c) *a ≡ b (n) ^ m | n => a ≡ b (m)*
   d) *a . c ≡ b . c (n) ^ mcd(c,n) = 1 => a ≡ b (n)*
   e) *a ≡ b (n) => $a^2 \equiv b^2$ (n)*
   f) *a ≡ b (n) => $a^m \equiv b^m$ (n)* siendo m ϵ N (usar inducción)

5. Resolver las siguientes ecuaciones o sistemas de ecuaciones en Zn indicado:

   a) En Z_7 : $\bar{3}\,\bar{x} + \bar{4} = \bar{2}$
   b) En Z_{23}: $\bar{5}\,\bar{x} + \bar{9} = \bar{8}$
   c) En Z_{17}: $\bar{4}\,\bar{x} + \bar{7} = \bar{1}$
   d) En Z_{11}: $\bar{7}\,\bar{x} + \bar{y} = \bar{0} \quad \wedge \quad \bar{x} + \bar{3}\,\bar{y} = \bar{4}$
   e) En Z_{13}: $\bar{x} + \bar{2}\,\bar{y} = \bar{6} \quad \wedge \quad \bar{3}\,\bar{x} + \bar{4}\,\bar{y} = \bar{6}$
   f) En Z_{11}: $\bar{2}\,\bar{x} + \bar{y} = \bar{1} \quad \wedge \quad \bar{3}\,\bar{x} + \bar{2}\,\bar{y} = \bar{5}$

II. FUNCIÓN φ DE EULER, TEOREMAS DE EULER, EULER-FERMAT

6. Calcular la función φ de Euler de los siguientes números, utilizando las propiedades:

   a) φ(450)
   b) φ(211)
   c) φ(840)
   d) φ(500)
   e) φ(2019)
   f) φ(2401)

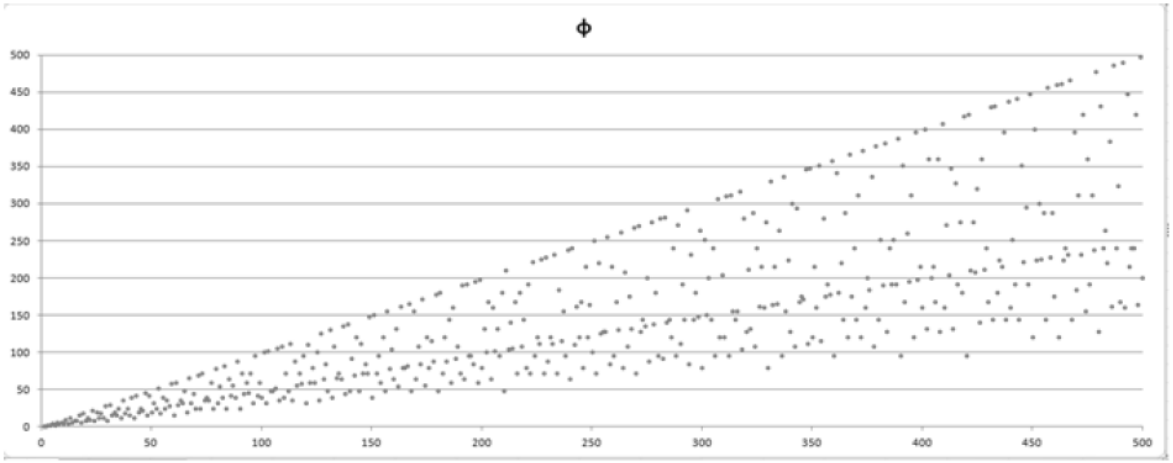
7. Para pensar:

   a) Indicar todos los valores de n ϵ N tales que φ(n)=8
   b) ¿cuánto vale φ(n) para n = 2^k (k ϵ N)? ¿Por qué?

8. Demostrar:

   a) Si n es impar, entonces φ (2n) = φ (n)
   b) Si n>2 entonces φ (n) es par

9. Observar este gráfico que representa a los primeros 500 valores de φ (n)



a) ¿Se llega a descubrir algún patrón? ¿Por qué creés que pasa?
b) ¿A qué números corresponden los valores alineados en la parte superior?
c) ¿Ves algún valor de φ (n) < 100 para algún n > 40? Intenta descubrir el valor de n

10. Hallar el resto de las divisiones de *a* por *b* utilizando el teorema de Fermat:

a) $a = 8^{44138}$; $b = 11$
b) $a = 5^{48963}$; $b = 13$
c) $a = 2^{94990}$; $b = 47$
d) $a = 3^{123159}$; $b = 61$
e) $a = 5^{28574}$; $b = 17$

11. Hallar el resto de las divisiones de *a* por *b* utilizando el Teorema de Euler-Fermat:

a) $a = 2^{340}$; $b = 341$
b) $a = 4444^{4444}$; $b = 9$
c) $a = 7^{2019}$; $b = 100$

12. Demostrar, justificando, cada una de las siguientes cuestiones:

a) La suma de los cubos de 3 enteros consecutivos es congruente con 0 módulo 9
b) Si mcd(n,7) = 1, entonces $n^{12} - 1 \equiv 0\ (7)$
c) $3.\ 5^{2n+1} + 2^{3n+1} \equiv 0\ (17)$
d) $2^{2n+1} + 1 \equiv 0\ (3)$

III. ECUACIONES EN CONGRUENCIA

13. Resolver las siguientes ecuaciones de congruencia:

a) $99\ x \equiv 25\ (140)$
b) $33\ x \equiv 24\ (15)$
c) $35\ x \equiv 14\ (182)$
d) $48\ x \equiv 50\ (98)$
e) $64\ x \equiv 18\ (96)$
f) $15\ x \equiv 125\ (140)$

14. Indicar Verdadero o Falso, justificando:

a) La ecuación $102\ x \equiv 35\ (342)$ no tiene solución
b) La ecuación $112\ x \equiv 392\ (91)$ tiene 7 soluciones principales
c) x = 62 es una de las únicas 6 soluciones principales de: $72\ x \equiv 54\ (126)$
d) x = 56 es una de las 6 soluciones principales de: $78\ x \equiv 84\ (102)$
e) La ecuación $102\ x \equiv 24\ (42)$ tiene 6 soluciones principales

Guía 7 — Congruencia en $\mathbb{Z}$ — 2020

I) Congruencias

1) Indicar V o F, justificando:

a) $541 \equiv 100\ (3) \equiv 1\ (3)$

$541 = 180 \cdot 3 + 1 \Rightarrow 541 \equiv 1\ (3)$ ✓ **V**

b) $327 \equiv 3\ (8)$

$327 = 40 \cdot 8 + 7 \Rightarrow 327 \equiv 7\ (8)$ **F**

c) $21 \equiv -4\ (5) \equiv 1\ (5)$

$21 = 4 \cdot 5 + 1$ ✓ **V**

d) $3795 \equiv 0\ (11)$ ✓

$3795 = 345 \times 11 \Rightarrow 3795 \equiv 0\ (11)$ **V**

e) $\bar{2}\ (10) \subseteq \bar{2}\ (5) \rightarrow x \in \bar{2}(5) \Rightarrow x = k_1 \cdot 5 + 2$

$x \in \bar{2}(10) \Rightarrow x = k_2 10 + 2 = k_2 \cdot 2 \cdot 5 + 2 = k_3 \cdot 5 + 2$ ✓ **V**

($k_3 = k_2 \cdot 2$)

f) $\bar{3}(6) \cap \bar{4}(5) = \emptyset$

$9 \equiv 3(6) \Rightarrow 9 \in \bar{3}(6) \wedge 9 \equiv 4(5) \Rightarrow 9 \in \bar{4}(5)$ **F**

$\therefore \bar{3}(6) \cap \bar{4}(5) = 9$ (o más elementos)

g) $a \equiv 0(2) \Rightarrow a \equiv 2(4)$

si $a = 4 \Rightarrow 4 \equiv 0(2)$ pero también es $4 \equiv 0(4)$ **F**

h) $a \equiv b\ (2) \Leftrightarrow a + b \equiv 0\ (2)$

$a = k_1 2 + b \qquad a + b = k_2 2$ **V**

$\Rightarrow$ hip $\Rightarrow a = k k_1 + b$: $a + b \overset{\text{hip}}{=} (2k_1 + b) + b = 2k_1 + 2b = 2(\underbrace{k_1 + b}_{k_2}) \Rightarrow a + b = 2k_2$ ✓

$\Leftarrow$ hip: $a + b = 2k_2$ ($a = 2k_2 - b$) : $a \overset{\text{hip.}}{=} k_2 2 - b + 2b - 2b = 2k_2 - 2b + b = 2(\underbrace{k_2 - b}_{k_1}) + b$

$\Rightarrow a = 2k_1 + b$ ✓

② Se sabe que $n \in \mathbb{Z}^+$ cumple: $n \equiv 3(7) \wedge n \equiv 2(8)$, se pide:

a) Hallar los dos números que cumplen eso y son menores que 100:

$X = \{ n \in \mathbb{Z}^+, n < 100, n \equiv 3(7) \} = \overline{3}\ (7)$

$Y = \{ n \in \mathbb{Z}^+, n < 100, n \equiv 2(8) \} = \overline{2}\ (8)$

$X = \{ 3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73, 80, 87, 94 \}$

$Y = \{ 2, 10, 18, 26, 34, 42, 50, 58, 66, 74, 82, 90, 98 \}$

$\boxed{n = 10 \quad y \quad n = 66}$

$10 = 1 \times 7 + 3 \Rightarrow 10 \equiv 3(7)$
$10 = 1 \times 8 + 2 \Rightarrow 10 \equiv 2(8)$ ✓ 10

$66 = 9 \times 7 + 3 \Rightarrow 66 \equiv 3(7)$
$66 = 8 \times 8 + 2 \Rightarrow 66 \equiv 2(8)$ ✓ 66

b) Demostrar que todos los números que verifican esas condiciones son $n \equiv 10(56)$ $\quad n = k_3 56 + 10$

$n \equiv 3(7) \Rightarrow n = k_1 7 + 3 \xrightarrow{\times 8} 8n = 56k_1 + 24$

$n \equiv 2(8) \Rightarrow n = k_2 8 + 2 \xrightarrow{\times 7} 7n = 56k_2 + 14$

$n = 56(k_1 - k_2) + 10$

$n \equiv 10\ (56)$

③ Hallar todos los enteros positivos n que sean congruentes a 2 tanto en módulo 3, módulo 4 y módulo 5.

$n \equiv 2(3) \wedge n \equiv 2(4) \wedge n \equiv 2(5)$

$n = k_1 3 + 2 \wedge n = k_2 4 + 2 \wedge n = k_3 5 + 2$ $\quad k_i \in \mathbb{Z}$, $i \in [1, 4]$

$n - 2 = 3k_1 \quad n - 2 = 4k_2 \quad n - 2 = 5k_3$

$n - 2$ debe ser múltiplo de 3, 4 y 5

$mcm(3, 4, 5) = 60 \Rightarrow n - 2 = 60k_4$

$n - 2 \equiv 0\ (60)$

$\boxed{n \equiv 2(60)}$

$\boxed{n = 60k_4 + 2}$

Unidad 7

④ Demostrar las sig. propiedades: $k_i \in \mathbb{Z}$

a) $a \equiv b\,(n) \wedge c \equiv d\,(n) \Rightarrow a.c \equiv b.d\,(n)$

$a = k_1 n + b \qquad c = k_2 n + d$

$a.c = c.(k_1 n + b) = (k_2 n + d)(k_1 n + b) =$

$= k_1 k_2 n^2 + k_2 n b + d k_1 n + d.b =$

$= n(k_1 k_2 n + k_2 b + k_1 d) + d.b$

$\Rightarrow \quad a.c - d.b = n(\underbrace{k_1 k_2 n + k_2 b + k_1 d}_{\in \mathbb{Z}})$

(lo llamo k_3)

$a.c - d.b = n k_3 \Rightarrow \boxed{a.c \equiv d.b\,(n)}$ ✓

× def. de congruencia

b) $a \equiv b\,(n) \wedge c \equiv d\,(n) \Rightarrow a - c \equiv b - d\,(n)$

$a = n k_1 + b \qquad c = k_2 n + d$

$k_3 \in \mathbb{Z}$

$a - c \overset{hip}{=} (n k_1 + b) - (n k_2 + d) = n(k_1 - k_2) + b - d$

$(a-c) - (b-c) = n k_3 \Rightarrow \boxed{a - c \equiv b - c\,(n)}$

c) $a \equiv b\,(n) \wedge m \mid n \Rightarrow a \equiv b\,(m)$

$a = k_1 m + b \qquad n = k_2 m \qquad a = k_3 m + b$

$a \overset{hip}{=} k_1 m + b \overset{hip}{=} k_1 (k_2 m) + b = \underbrace{k_1 k_2}_{k_3} m + b \Rightarrow a = k_3 m + b$

$\boxed{a \equiv b\,(m)}$

d) $a.c \equiv b.c\,(n) \wedge mcd(c, n) = 1 \Rightarrow a \equiv b\,(n)$

$ac = k_1 n + bc \qquad 1 = sc + tn,\ s, t \in \mathbb{Z}$ (× Bezout) $\qquad \hookrightarrow a = k_2 n + b$

Dem: $a = a.1 \overset{hip}{=} a(sc + tn) = acs + atn \overset{hip}{=} (k_1 n + bc)s + atn =$

$= n k_1 s + bcs + n\,at \overset{\text{factor común}}{=} n(k_1 s + at) + bsc =$

$\overset{hip}{=} n(k_1 s + at) + b(1 - tn) = n(k_1 s + at) + b - btn =$

$= n(\underbrace{k_1 s + at - bt}_{\in \mathbb{Z}}) + b = n k_2 + b \Rightarrow a = n k_2 + b$

$\boxed{a \equiv b\,(n)}$

e) $a \equiv b\ (n) \Rightarrow a^2 \equiv b^2\ (n)$

$a - b = k n \Rightarrow a = k n + b$

$(a+b)(a-b) = (a+b)\, k n$

$a^2 - b^2 = \underbrace{(a+b)}_{\in \mathbb{Z}}\, k \cdot n = k_2 n \Rightarrow a^2 - b^2 = k_2 n \Rightarrow \boxed{a^2 \equiv b^2\ (n)}$

k_2

f) $a \equiv b\ (n) \Rightarrow a^m \equiv b^m\ (n)$ siendo $m \in \mathbb{N}$ (usar inducción)

hip: $a = k_1 n + b$ $\quad a - b = k_1 n$ $\quad$ tesis: $a^m = k_2 n + b^m$

$a^m \equiv b^m\ (n)$

Paso base: $m = 1$: $a \equiv b\ (n) \Rightarrow a^1 \equiv b^1\ (n)$ ✓ $\quad a^n - b^n = k n$

Paso inductivo: H.I) $a^n \equiv b^n\ (n) \Rightarrow a^n = k n + b^n$

T.I) $a^{n+1} \equiv b^{n+1}\ (n) \rightsquigarrow a^{n+1} - b^{n+1} = k_2 n$

Dem: (hip.) $a^n - b^n = k n$

$(a+b)(a^n - b^n) = (a+b)\, k n$

$a^{n+1} - a b^n + b a^n - b^{n+1} = (a+b)\, k n$

$a^{n+1} - b^{n+1} = (a+b)\, k n + a b^n - b a^n =$

$= (a+b)\, k n + a b^n - b a^n + b^n b - b^n b =$

$= (a+b)\, k n + b(-a^n + b^n) + b^n (a - b) =$

$= (a+b)\, k n - b(a^n - b^n) + b^n (a - b) \equiv$

$\times$ H.I) $= (a+b)\, k n - b\,(k_1 n) + b^n\,(k_1 n) =$

$= k n (a + b - b) + b^n k_1 n =$

$= n(k a + b^n k_1) = n\, k_3$

$a^{n+1} - b^{n+1} = n\, k_3$

$\boxed{a^{n+1} \equiv b^{n+1}\ (n)}$

U.7

⑤ Resolver las sig. ecuaciones o sist. de ecuaciones en el $\mathbb{Z}_n$ indicado:

a) En Z_7: $\bar{3}\bar{x} + \bar{4} = \bar{2}$

$3x + 4 \equiv 2 (7)$

$3x \equiv (2-4)(7) \Rightarrow 3x \equiv -2 (7)$

$3x \equiv 5 (7)$ $\quad \{(3,7) = 1$ ✓ $\quad 1 \mid 5$ ✓ tiene sol ún

$3x \equiv 12 (7)$

$3x \equiv 3 \cdot 4 (7) \Rightarrow \boxed{x \equiv 4 (7)}$

b) En Z_{23}: $\bar{5}\bar{x} + \bar{9} = \bar{8}$

$5x + 9 \equiv 8 (23)$

$5x \equiv 8 \cdot 9 (23) \Rightarrow 5x \equiv 22 (23)$ $\quad \{(23,5) = 1$ ✓ $\quad 1 \mid 22$ ✓

$5x \equiv 45 (23)$

$5x \equiv 5 \cdot 9 (23)$

$\boxed{x \equiv 9 (23)}$

c) En Z_{17}: $\bar{4}\bar{x} + \bar{7} = \bar{1}$

$4x \equiv -6 (17) \Rightarrow 4x \equiv 11 (17)$ $\quad \{(4,17) = 1$ ✓ $\quad 1 \mid 11$ ✓

$4x \equiv 28 (17)$

$4x \equiv 4 \cdot 7 (17)$

$\boxed{x \equiv 7 (17)}$

d) En $\mathbb{Z}_{11}$: $\bar{7}\bar{x} + \bar{y} = \bar{0} \wedge \bar{x} + \bar{3}\bar{y} = \bar{4}$

$$\begin{cases} 7x + y \equiv 0 \ (11) \\ x + 3y \equiv 4 \ (11) \end{cases} \longrightarrow y \equiv -7x \ (11) \equiv 4x \ (11)$$

$$x + 3(4x) \equiv 4 \ (11)$$

$$13x \equiv 4 \ (11), \quad \varphi(11) = 10$$

$$x = 13^9 \cdot 4 = (13^3)^3 \cdot 4$$

$13^3 \equiv 8 \ (11)$

$$x \equiv 24 \ (11) \equiv 2 \ (11) \qquad \equiv 6 \ (11)$$

$7x + y \equiv 0 \ (11)$, $7x \equiv 2 \ (11)$

$\equiv 3 \ (11) \Rightarrow y \equiv 8 \ (11)$

$\boxed{x \equiv 2 \ (11)}$

$\boxed{x \equiv 2 \ (11) \wedge y \equiv 8 \ (11)}$ ✓

e) En $\mathbb{Z}_{13}$: $\bar{x} + \bar{2}\bar{y} \equiv \bar{6} \wedge \bar{3}\bar{x} + \bar{4}\bar{y} = \bar{6}$

$$\begin{cases} x + 2y \equiv 6 \ (13) \\ 3x + 4y \equiv 6 \ (13) \end{cases} \longrightarrow \boxed{x \equiv 6 - 2y \ (13) \equiv 6 + 11y \ (13)}$$

$$3(6 + 11y) + 4y \equiv 6 \ (13)$$

$$18 + 37y \equiv 6 \ (13) \qquad \equiv 12 \ (13)$$

$$37y \equiv 1 \ (13) \Rightarrow y = 37^{11} \cdot 1 = 37^6 \cdot 37^5 \qquad \equiv 7 \ (13)$$

$y \equiv 84 \ (13)$

$\boxed{y \equiv 6 \ (13)}$

$x + 2y \equiv 6 \ (13)$, $2y \equiv 6 \ (13)$

$12 \ (13)$

$\boxed{x \equiv 7 \ (13)}$ ✓

f) $\bar{2}\bar{x} + \bar{y} = \bar{1} \wedge \bar{3}\bar{x} + \bar{2}\bar{y} = \bar{5}$

En $\mathbb{Z}_{11}$

$$\begin{cases} 2x + y \equiv 1 \ (11) \\ 3x + 2y \equiv 5 \ (11) \end{cases} \longrightarrow \boxed{y \equiv -2x + 1 \ (11) \equiv 9x + 1 \ (11)}$$

$$3x + 2(9x + 1) \equiv 5 \ (11)$$

$$21x \equiv 3 \ (11)$$

$$x = 21^9 \cdot 3 = (21^3)^3 \cdot 3$$

$21^3 \equiv 10 \ (11)$

$\equiv 10 \ (11) \qquad 30 \ (11)$

$\boxed{x \equiv 8 \ (11)}$ ✓

$2x + y \equiv 1 \ (11)$, $2x \equiv 8 \ (11)$

$5 \ (11)$

$y \equiv -4 \ (11)$

$\boxed{y \equiv 7 \ (11)}$

$\varphi(m)$ → si m es primo $\Rightarrow \varphi(m) = m-1$

↳ si NO es primo $\Rightarrow \varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots$

U7

(11) Función φ de EULER, teoremas de Euler, Euler-Fermat

⑥ Calcular la función φ de Euler de los seg. números, utilizando las propiedades:

a) $\varphi(450) = 450\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 120$

450	2
225	3
75	3
25	5
5	5
1	

$450 = 2 \cdot 3^2 \cdot 5^2$

$\boxed{\varphi(450) = 120}$ ✓

b) $\varphi(211) = 210$ (pues 211 es primo) $\boxed{\varphi(211) = 210}$ ✓

c) $\varphi(840) = 840\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 192$

840	2
420	2
210	2
105	3
35	5
7	7
1	

$840 = 2^3 \cdot 3 \cdot 5 \cdot 7$

$\boxed{\varphi(840) = 192}$ ✓

d) $\varphi(500) = 500\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 200$

500	2
250	2
125	5
25	5
5	5
1	

$500 = 2^2 \cdot 5^3$

$\boxed{\varphi(500) = 200}$ ✓

e) $\varphi(2019) = 2019\left(1-\frac{1}{3}\right)\left(1-\frac{1}{673}\right) = 1344$

2019	3
673	673
1	

$\boxed{\varphi(2019) = 1344}$ ✓

f) $\varphi(2401) = 2401\left(1-\frac{1}{7}\right) = 2058$

2401	7
343	7
49	7
7	7
1	

$2401 = 7^4$

$\boxed{\varphi(2401) = 2058}$ ✓

⑦ Para pensar:

a) Indicar todos los valores de $n \in \mathbb{N}$ tales que $\varphi(n) = 8$

Si n es primo $\Rightarrow \varphi(n) = n-1$, si $n-1 = 8 \Rightarrow n = 9 \Rightarrow n$ NO es primo

- n NO es primo: $\varphi(n) = n\underbrace{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)}_{k} = 8$

$n > 8$

$n = 9 = 3^2 \Rightarrow \varphi(9) = 6$
$n = 10 = 2.5 \Rightarrow \varphi(10) = 4$
$n = 12 = 2^2.3 \Rightarrow \varphi(12) = 4$
$n = 14 = 2.7 \Rightarrow \varphi(14) = 6$
$n = 15 = 3.5 \Rightarrow \boxed{\varphi(15) = 8}$
$n = 16 = 2^4 \Rightarrow \boxed{\varphi(16) = 8}$
$n = 18 = 2.3^2 \Rightarrow \varphi(18) = 6$
$n = 20 = 2^2.5 \Rightarrow \boxed{\varphi(20) = 8}$
$n = 21 = 3.7 \Rightarrow \varphi(21) = 12$
$n = 22 = 2.11 \Rightarrow \varphi(22) = 10$
$n = 24 = 2^3.3 \Rightarrow \boxed{\varphi(24) = 8}$
$n = 25 = 5^2 \Rightarrow \varphi(25) = 20$
$n = 26 = 2.13 \Rightarrow \varphi(26) = 12$
$n = 27 = 3^3 \Rightarrow \varphi(27) = 18$
$n = 28 = 2^2.7 \Rightarrow \varphi(28) = 12$
$n = 29$ es primo (no va)
$n = 30 = 2.3.5 \Rightarrow \boxed{\varphi(30) = 8}$
$n = 32 = 2^5 \Rightarrow \varphi(32) = 16$
$n = 33 = 3.11 \Rightarrow \varphi(33) = 20$
$n = 34 = 2.17 \Rightarrow \varphi(34) = 16$

Los $n \in \mathbb{N}$ tales que $\varphi(n) = 8$ son 15, 16, 20, 24 y 30

b) ¿Cuánto vale $\varphi(n)$ para $n = 2^k$ ($k \in \mathbb{N}$)? ¿Por qué?

$\varphi(n) = \frac{n}{2}$ pues $\varphi(n) = n \cdot \left(1 - \frac{1}{2}\right) = n \cdot \frac{1}{2} = \frac{n}{2}$

U.7

⑧ Demostrar q:

a) Si n es impar entonces: $\varphi(2 \cdot n) = \varphi(n)$

$\varphi(2 \cdot n) = \varphi(2) \cdot \varphi(n) = 1 \cdot \varphi(n) = \varphi(n)$

b) Si $n > 2$ entonces: $\varphi(n)$ es par los primos > 2 son todos impares

- Si $n > 2$ y n es primo $\Rightarrow \varphi(n) = n - 1 = (2k+1) - 1 = 2k \Rightarrow$ es par

$n > 2$ y n NO es primo $\Rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) = n\left(\frac{p_1 - 1}{p_1}\right) \cdots \left(\frac{p_k - 1}{p_k}\right)$

Si n es par $\Rightarrow \varphi(n) = 2k(\ldots\ldots) \Rightarrow$ par

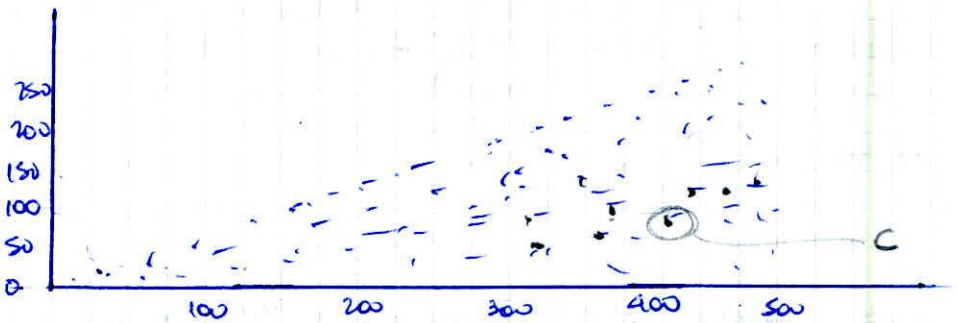
Si n impar $\Rightarrow \varphi(n) = (2k+1)\left(\frac{p_1 - 1}{p_1}\right) \cdots \left(\frac{p_k - 1}{p_k}\right)$

todos los primos > 2 son impares

$\Rightarrow p_i - 1$ es par

---

⑨ Observar este gráfico que representa a los primeros 500 valores de $\varphi(n)$:



a) ¿Llegas a descubrir algún patrón? ¿por qué crees que pasa?

No se puede observar ningún patrón. La distribución de los números primos es aleatoria

b) ¿A qué números corresponden los valores alineados en la parte superior?

A los $\varphi(n)$ con n número primo

c) ¿Hay algún valor de $\varphi(n) < 100$ para algún $n > 400$? Intenta descubrir el valor de n

$n = 420 \Rightarrow \varphi(420) = 420\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 96$

420	2
210	2
105	3
35	5
7	7

(10) Hallar el resto de las divisiones de a por b utilizando el teorema de Fermat.

a) $a = 8^{44138}$; $b = 11$ — 11 es primo ✓

$44138 = 4413 \times 10 + 8$

$8^{44138} = (8^{10})^{4413} \cdot 8^8 \Rightarrow 8^{44138} \equiv 8^8 (11) \equiv \overbrace{16777216}^{5}(11)$

$8^{44138} \equiv 1(11)$ $\quad 1(11)$

$\boxed{8^{44138} \equiv 5(11)} \Rightarrow \text{resto} = 5$ ✓

b) $a = 5^{48963}$; $b = 13$ — 13 es primo ✓

$48963 = 4080 \times \underbrace{12}_{13-1} + 3$

$5^{48963} = 5^{12 \cdot 4080 + 3} = (5^{12})^{4080} \cdot 5^3 \equiv 125(13) \equiv 8(13)$

$5^{12} \equiv 1(13)$ $\quad 1(13)$

$\boxed{\text{resto} = 8}$ ✓

c) $a = 2^{94990}$; $b = 47$ — 47 es primo ✓

$94990 = 2065 \times 46$

$2^{94990} = 2^{46 \times 2065} = (2^{46})^{2065} \equiv 1(47)$

$2^{46} \equiv 1(47)$

$\boxed{\text{resto} = 1}$

d) $a = 3^{123159}$; $b = 61$ — 61 es primo ✓

$123159 = 2052 \times 60 + 39$

$3^{123159} = 3^{60 \cdot 2052 + 39} = (3^{60})^{2052} \, 3^{39} \equiv 1(61)$

$= 3^{10} \cdot 3^{10} \cdot 3^{10} \cdot 3^9 =$

$= \underbrace{59049}_{\equiv 1(61)} \times \underbrace{59049}_{\equiv 1(61)} \times \underbrace{59049}_{\equiv 1(61)} \times \underbrace{19683}_{\equiv 41(61)}$

$\boxed{\text{resto} = 41}$

e) $a = 5^{28574}$; $b = 17$ — 17 es primo ✓

$28574 = 1785 \times 16 + 14$

$5^{28574} = 5^{16 \cdot 1785 + 14} = (5^{16})^{1785} \cdot 5^{14} \equiv 5^{14}(17) \equiv 100(17) \equiv 15(17)$

$5^{16} \equiv 1(17)$

$5^{14} = \underbrace{5^7}_{78125} \cdot \underbrace{5^7}_{78125}$

$\equiv 10(17) \quad \equiv 10(17)$

$\boxed{\text{resto} = 15}$

$$\text{si } (a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 (m)$$

U7

(11) Hallar el resto de las divisiones de a por b. utilizando el teorema de Euler Fermat:

a) $a = 2^{340}$; $b = 341$

341 no es primo . $(2, 341) = 1$ ✓ $\quad a^{\varphi(m)} \equiv 1(m)$

$341 = 11 \cdot 31$

$\varphi(341) = 341\left(1-\frac{1}{11}\right)\left(1-\frac{1}{31}\right) = 300$

$2^{340} = 2^{300} \cdot 2^{40} = \underbrace{2^{300}}_{\equiv 1(341)} \cdot 2^{20}\, 2^{20} = \underbrace{2^{300}}_{\equiv 1(341)} \cdot \underbrace{1048576}_{\equiv 1(341)} \cdot \underbrace{1048576}_{\equiv 1(341)}$

$\equiv 1 (341)$

resto = 1

b) $a = 4444^{4444}$; $b = 9$

$(9, 4444) = 1$, $\varphi(9) = 9\left(1-\frac{1}{3}\right) = 6$

$4444 = 740 \cdot 6 + 4$

$4444^{4444} = \underbrace{(4444^6)^{740}}_{\equiv 1(9)} \cdot \underbrace{4444^4}_{\equiv 1(9)} \equiv (4444^2)^2 (9) \equiv \underbrace{19749136^2}_{\equiv 4(9)} (9)$

$\equiv 16(9) \equiv 7(9)$

resto = 7

c) $a = 7^{2019}$; $b = 100$

$(7, 100) = 1$ ✓ $\quad \varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$

$100 = 2^2 \cdot 5^2$

$7^{2019} = 7^{40 \cdot 50 + 19} = (7^{40})^{50} \cdot 7^{19} = \underbrace{(7^{40})^{50}}_{\equiv 1(100)} \cdot \underbrace{7^{10}}_{\equiv 49(100)} \cdot \underbrace{7^9}_{\equiv 7(100)}$

$7^{2019} \equiv \overbrace{343}^{7 \times 49} (100) \equiv 43 (100)$

resto = 43

$7^{19} = (7^4)^4 \, 7^3$

$7^4 = 2401 \equiv 1(100)$, $7^3 \equiv 43(100)$

(12) Demostrar, justificando, cada una de las sig. cuestiones:

a) La suma de los cubos de 3 enteros consecutivos es congruente con 0 módulo 9.

$$n^3 + (n+1)^3 + (n+2)^3 = \underbrace{n^3}_{n^3} + \underbrace{n^3+3n^2+3n+1}_{(n+1)^3} + \underbrace{n^3+6n^2+12n+8}_{(n+2)^3} =$$

$$= 3n^3 + \underbrace{9n^2}_{\equiv 0(9)} + 15n + \underbrace{9}_{\equiv 0(9)} \equiv 3n^3 + 15n \ (9)$$

- Si $n \equiv 0(3) \Rightarrow 3n^3 + 15n \equiv 0(9)$ ✓
- Si $n \equiv 1(3) \Rightarrow \underbrace{3n^3}_{\equiv 3(9)} + 15n \equiv 9(9) \equiv 0(9)$ ✓ $\quad \equiv 6(9)$
- Si $n \equiv 2(3) \Rightarrow \underbrace{3n^3}_{\equiv 24(9)} + 15n \equiv 9(9) \equiv 0(9)$ ✓ $\quad \underbrace{\equiv 30(9)}_{\equiv 3(9)}$
$\equiv 6(9)$

b) Si $\text{mcd}(n,7) = 1$ entonces $n^{12} - 1 \equiv 0(7) \rightarrow n^{12} \equiv 1(7)$

$(n,7) = 1$ ∧ 1|0 ✓ $\Rightarrow n^{12} = n^{6 \cdot 2} = (n^6)^2 \equiv 1(7)$ ✓

$\varphi(7)$ $\quad \equiv 1(7)$

c) $3 \cdot 5^{2n+1} + 2^{3n+1} \equiv 0(17)$ 17 es primo

$3 \cdot 5 \cdot 5^{2n} + 2 \cdot 2^{3n} = 15\,(5^2)^n + 2 \cdot (2^3)^n =$

$= 15 \cdot 25^n + 2 \cdot 8^n \equiv 15 \cdot 8^n + 2 \cdot 8^n \equiv$

$(\equiv 8(17))^n$

$\equiv \underbrace{17}_{\equiv 0(17)} \cdot 8^n \equiv 0(17)$

d) $2^{2n+1} + 1 \equiv 0(3)$

$2 \cdot (2^2)^n + 1 \equiv 2 \cdot 1^n + 1 \equiv 3(3) \equiv 0(3)$ ✓

$2^2 \equiv 1(3)$ $\quad \varphi(3)$

$ax \equiv b(n)$. Si n NO es primo
• $(a,n) = 1$ $\longrightarrow$ $x = a^{\varphi(n)-1} \cdot b \ (n)$ 7

U7

III Ecuaciones en congruencia

(13) Resolver las sig. ecuaciones de congruencia:

a) $99x \equiv 25\ (140)$

99 | 3	140 | 2
33 | 3	70 | 2
11 | 11	35 | 5
1	7 | 7
	1

$(99,140) = 1 \Rightarrow x \equiv 99^{47} \cdot 25$

(140 NO es primo)

$\varphi(140) = 140\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 48$

La reduzco un poco (son números muy grandes)

$99x \equiv 25\ (140) \overset{+140}{\equiv} 165\ (140)$

$9 \cdot 11x \equiv 15 \cdot 11\ (140) \Rightarrow 9x \equiv 15\ (140)$

$x = 9^{47} \cdot 15 = \left(\left(9^3\right)^2\right)^7 \cdot 9^5 \cdot 15$

$47 = 3 \cdot 2 \cdot 7 + 5$

$9^3 = 729 \equiv 29\ (140)$; $841 \equiv 1\ (140)$

$9^5 = 59049 \equiv 109\ (140)$; $1635 \equiv 95\ (140)$

$\equiv 95\ (140) \Rightarrow \boxed{x \equiv 95\ (140)}$ ✓

b) $\overset{a}{33}x \equiv \overset{b}{24}\ (\overset{m}{15})$

$(a,m) = (33,15) = 3 \Rightarrow$ 3 soluciones posibles

$11x \equiv 8\ (5)$, 5 es primo $\Rightarrow x = 11^4 \cdot 8 = 117128 \equiv 3\ (5)$

$x \equiv 3\ (5)$

$\boxed{x = 3,\ x = 8,\ x = 13}$ ✓ (+5, +5)

c) $35x \equiv 14\ (182)$

35 | 5	182 | 2
7 | 7	91 | 7
1	13 | 13
	1

$(35,182) = 7$ → 7 soluciones

$5x \equiv 2\ (26) \Rightarrow x = 5^{11} \cdot 2 = 97656250 \equiv 16\ (26)$ ($11 = 12-1$)

$\varphi(26) = 26\left(1-\frac{1}{2}\right)\left(1-\frac{1}{13}\right) = 12$

$\boxed{x = 16,\ x = 42,\ x = 68,\ x = 94,\ x = 120,\ x = 146,\ x = 172}$ ✓ (+26, +26)

d) $48x \equiv 50\ (98)$

48	2	98	2
24	2	49	7
12	2	7	7
6	2	1	
3	3		
1			

$(48,98) = 2$ → 2 soluciones

$\rightarrow 24x \equiv 25\ (49)$

$\varphi(49) = 49\left(1-\frac{1}{7}\right) = 42$

$x = 24^{41} \cdot 25 =$

$= (24^7)^5 \cdot 24^6 \cdot 25$

$24^7 \equiv 31\ (49)$

$31^5 \equiv 19\ (49)$

$\equiv 19(49)$ $\quad 24^6 \equiv 36(49)$ $\quad \equiv 17100\ (49)$

$x \equiv 48(49)$

$+49$

$x_1 = 48 \qquad x_2 = 97$ ✓

$24^{41} \cdot 25$

$(24^{20})^2 \cdot 24 \cdot 25$

$\equiv 12(49)$

e) $64x \equiv 18\ (96)$

$64 = 2^6$
$96 = 2^5 \cdot 3$ $\Big\}$ $(64,96) = 2^5 = 32$ pero $32 \nmid 18 \Rightarrow$ no tiene solución

f) $15x \equiv 125\ (140)$

$15 = 3 \times 5$
$140 = 2^2 5 \cdot 7$ $\Big\}$ $(15,140) = 5$

$5 \mid 125$ tiene 5 solu.

$\rightarrow 3x \equiv 25\ (28)$

$\varphi(28) = 28\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right) = 12$

$x = 3^{11} \cdot 25 = 4428675$

$\equiv 27(28)$

$x_1 = 27 \qquad x_2 = 55$

$x_3 = 83 \qquad x_4 = 111$

$x_5 = 139$ ✓

$ax \equiv b(m)$

Si $(a,m) = c \wedge t \mid b \Rightarrow$ se puede simplificar y tiene t soluciones posibles

$3^{11} \cdot 25 = 3^4 \cdot 3^4 \cdot 3^3 \cdot 25$

$25 \cdot 25 \quad 27 \cdot 25$

$625 \quad \equiv 3(28)$

$\equiv 9(28)$

$\equiv 27(28)$

(14) Indicar V o F, justificando:

a) La ecuación $102x \equiv 35 (342)$ no tiene solución. **V**

102	2	342	2
51	3	171	3
17	17	57	3
1		19	19
		1	

$(102, 342) = 2 \times 3 = 6$ pero $6 \nmid 35$

$\therefore$ No tiene solución

b) La ecuación $112x \equiv 392 (91)$ tiene 7 soluc. ppales. **V**

112	2	91	7
56	2	13	13
28	2	1	
14	2		
7	7		
1			

$(112, 91) = 7$ y $7 \mid 392$

$\Rightarrow$ tiene 7 soluciones

$16x \equiv 56 (13) \equiv 160 (13) \equiv 16 \times 10 (13)$

$x \equiv 10 (13)$

$x_1 = 10$
$x_2 = 23$
$x_3 = 36$
$x_4 = 49$
$x_5 = 62$
$x_6 = 75$
$x_7 = 86$

c) $x = 62$ es una de las únicas 6 sol. ppales de: $72x \equiv 54 (126)$

$72 = 2^3 3^2$
$126 = 2 \cdot 3^2 7$
$(74, 126) = 2 \cdot 3^2 = 18$ y $18 \mid 54$ ✓

tiene 18 soluciones ppales

≠

d) $x = 56$ es una de las 6 sol. ppales de: $78x \equiv 84 (102)$

$78 = 2 \cdot 3 \cdot 13$
$102 = 2 \cdot 3 \cdot 17$
$(78, 102) = 6$ y $6 \mid 84$ ✓ $\Rightarrow$ tiene 6 sol. ppales.

$13x \equiv 14 (17) \equiv 65 (17) \equiv 5 \times 13 (17)$

$x \equiv 5 (17) \Rightarrow x_1 = 5$

V

$x_2 = 22$ $x_3 = 39$
$x_4 = 56$ $x_5 = 73$ $x_6 = 90$
$x_7 = 107$

e) La ecuación $102x \equiv 24 (42)$ tiene 6 sol. ppales.

$102 = 2 \cdot 3 \cdot 17$
$42 = 2 \cdot 3 \cdot 7$
$(102, 42) = 6$ y $6 \mid 24$ $\therefore$ tiene 6 soluciones ppales

V