QUÈ HEM FET FINS ARA?

El darrer dia vam acabar el temari i només cal fer més exercicis i donar una segona versio del petit teorema de Fermat. Darrera classe del curs.

CLASSE D'AVUI 21/12/2020

Una altra versió equivalent al petit teorema de Fermat és la següent:

PROP.:(segona versió del petit teorema de Fermat). Sigui p un primer, $n,m \geq 1$ i $n \equiv m(\mathrm{mod}(p-1)) \Rightarrow a^n \equiv a^m(\mathrm{mod}\, p)$.

DEM.: Si el $mcd(a,p) = 1$ llavors de la hipòtesi tenim que $n - m = k(p-1) \Rightarrow n = k(p-1) + m$ per tant

$a^n \equiv a^{k(p-1)+m} \equiv (a^{p-1})^k a^m \equiv 1^k a^m \equiv a^m(\mathrm{mod}\, p)$

I en el cas que $mcd(a,p) \neq 1$ en ser p un primer $p|a, p|b \Rightarrow a \equiv 0,\ a^n \equiv 0,$ $a^m \equiv 0 \Rightarrow a^n \equiv a^m(\mathrm{mod}\, p)$.

Dit de manera basta és que l'exponent funciona mòdul $p-1$ quan es calcula una potència mòdul p.

EX.: (46) Calculeu $44^{444}(\mathrm{mod}\, 13)$.

En primer lloc tenim que $444\, \mathrm{mod}(p-1) = 444\, \mathrm{mod}\, 12 = 0$ per tant $44^{444}(\mathrm{mod}\, 13) \equiv 44^0(\mathrm{mod}\, 13) \equiv 1$.

EX.: (47) Demostreu que per tot a, $\bar{a}^5 = \bar{a}$ a $\mathbb{Z}_{15}$. (Pista: useu Fermat i la última propietat de les congruències).

No podem utilitzar el petit teorema de Fermat perquè $15 = 3 \cdot 5$ no és primer. Si mirem la mateixa expressió a $\mathbb{Z}_3$ i a $\mathbb{Z}_5$ obtenim:

- A $\mathbb{Z}_3$ tenim que $5\, \mathrm{mod}(p-1) = 5\, \mathrm{mod}\, 2 = 1$ per tant $\bar{a}^5 = \bar{a}$ a $\mathbb{Z}_3$.
- A $\mathbb{Z}_5$ tenim que $5\, \mathrm{mod}(p-1) = 5\, \mathrm{mod}\, 4 = 1$ per tant $\bar{a}^5 = \bar{a}$ a $\mathbb{Z}_5$.

Ara apliquem la darrera propietat de congruències a $a^5 \equiv a\, \mathrm{mod}\, 3,\ a^5 \equiv a\, \mathrm{mod}\, 5$ llavors $a^5 \equiv a\, \mathrm{mod}(mcm(3,5)) \Leftrightarrow a^5 \equiv a\, \mathrm{mod}(15)$.

EX.: (48) Calculeu, usant Fermat i la última propietat de les congruències:

a) $11^{1234}(\mathrm{mod}\, 14)$.
b) $7^{1234}(\mathrm{mod}\, 165)$.

a) $11^{1234}(\mathrm{mod}\, 14)$: $14 = 2 \cdot 7,\ 1234\, \mathrm{mod}\, 6 = 4$

$$\left.\begin{array}{l} 11^{1234}\, \mathrm{mod}\, 2 \equiv 1^{1234}\, \mathrm{mod}\, 2 \equiv 1 \equiv -3 \\ 11^{1234}\, \mathrm{mod}\, 7 \equiv 7^{1234}\, \mathrm{mod}\, 7 \equiv 7^4\, \mathrm{mod}\, 7 \equiv 4 \equiv -3 \end{array}\right\} \Rightarrow 11^{1234}\, \mathrm{mod}(mcm(2,7)) \equiv -3 \Leftrightarrow$$

$\Leftrightarrow 11^{1234}\, \mathrm{mod}\, 14 \equiv -3 \equiv 11$

b) $7^{1234}\, \mathrm{mod}\, 165$: $165 = 3 \cdot 5 \cdot 11,\ 1234\, \mathrm{mod}\, 4 = 2,\ 1234\, \mathrm{mod}\, 10 = 4$

$$\left.\begin{array}{l} 7^{1234} \bmod 3 \equiv 1^{1234} \bmod 3 \equiv 1 \\ 7^{1234} \bmod 5 \equiv 2^{1234} \bmod 5 \equiv 2^2 \bmod 5 \equiv 4 \\ 7^{1234} \bmod 11 \equiv 7^4 \bmod 11 \equiv 3 \end{array}\right\} \Rightarrow ???$$

No és tan directe com els anteriors. Busquem un x tal que:

$$\left.\begin{array}{l} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 5 \\ x \equiv 3 \bmod 11 \end{array}\right\}$$

Fem el sistema de les dues primeres equacions:

$$\left.\begin{array}{l} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 5 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x = 1 + 3a \\ x \equiv 4 + 5b \end{array}\right\} \Rightarrow 1 + 3a = 4 + 5b \Leftrightarrow 3a - 5b = 3$$

Aquesta equació diofàntica té solució perquè $mcd(3,5) = 1|3$. És molt fàcil trobar que:
$3 \cdot (2) - 5 \cdot (1) = 1 \Rightarrow 3 \cdot (6) - 5 \cdot (3) = 3$

per tant les solucions de la diofantica són $a = 6 + 5t, b = 3 + 3t$ i d'aquí $x = 1 + 3a = 1 + 3(6 + 5t) = 19 + 15t$ o sigui $x \equiv 19 \bmod 15$, per tant reduint queda $x \equiv 4 \bmod 15$ i ara al resoldre el sistema amb la darrera equació:

$$\left.\begin{array}{l} x \equiv 4 \bmod 15 \\ x \equiv 3 \bmod 11 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x = 4 + 15a \\ x \equiv 3 + 11b \end{array}\right\} \Rightarrow 4 + 15a = 3 + 11b \Leftrightarrow 15a - 11b = -1$$

Aquesta equació diofàntica té solució perquè $mcd(15,11) = 1|-1$. Una solució particular la podem calcular fàcilment:

1	0	1	–2	3
0	1	–1	3	4
	1	2	1	3
15	11	4	3	1
4	3	1	0	

$15 \cdot (3) - 11 \cdot (4) = 1 \Rightarrow 15 \cdot (-3) - 11 \cdot (-4) = -1$

Per tant les solucions de la diofantica són $a = -3 + 11t, b = -4 + 15t$ i d'aquí $x = 4 + 15a = 4 + 15(-3 + 11t) = -41 + 165t$ o sigui $x \equiv -41 \bmod 165$, per tant reduint queda $x \equiv 124 \bmod 165$.

EX.: (49c) Calculeu: $25^{1025} (\bmod 251)$.

Tenim que 251 és primer i com que $1025 \bmod 250 = 25$ llavors:
$25^{1025} \bmod 251 = 25^{25} \bmod 251 = \ldots = 1$

EX.: (50a) Calculeu, usant Fermat i la última propietat de les congruències: a) $8^{1235}(\bmod 15)$.

Com que $15 = 3 \cdot 5$ em miro el mateix càlcul a $\mathbb{Z}_3$ i a $\mathbb{Z}_5$:

- A $\mathbb{Z}_3$ tenim que $8^{1235} \equiv 2^{1235} \equiv 2^1 \equiv 2 \bmod 3$ perquè $1235 \bmod 2 = 1$
- A $\mathbb{Z}_5$ tenim que $8^{1235} \equiv 3^{1235} \equiv 3^3 \equiv 2 \bmod 5$ perquè $1235 \bmod 4 = 3$

I de $mcm(3,5) = 15$ deduïm $8^{1235} \bmod(15) = 2$.

EXERCICIS DIVISIBILITAT

EX.: (80) Sigui a enter posiu. Demostreu que si $\sqrt{a}$ és racional llavors a és un quadrat (és igual al quadrat d'un altre nombre enter).

1ª MANERA

Suposem que $\sqrt{a} = \frac{b}{c}$ amb $\frac{b}{c}$ és fracció irreduïble (amb $b \geq 0, c > 0$ o sigui $mcd(b,c) = 1$) i volem demostrar que $c = 1$. Tenim que:

$\sqrt{a} = \frac{b}{c} \Rightarrow a = \frac{b^2}{c^2} \Rightarrow ac^2 = b^2$

Com que $c|ac^2 = b^2 \Rightarrow c|b^2$, o sigui que $c|b \cdot b$ amb $mcd(b,c) = 1$ i pel lema de Gauss obtenim que $c|b$; a partir de $c|b$ i $mcd(b,c) = 1$ llavors $c = 1$ i per tant $a = \frac{b^2}{1^2} = b^2$ com es volia demostrar.

2ª MANERA

Supposem que $b = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $c = p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}$, $a = p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k}$, amb $e_i, f_i, g_i \geq 0$ per tant:

$$\sqrt{a} = \frac{b}{c} \Rightarrow a = \frac{b^2}{c^2} \Rightarrow p_1^{g_1} p_2^{g_2} \ldots p_k^{g_k} = \frac{p_1^{2e_1} p_2^{2e_2} \ldots p_k^{2e_k}}{p_1^{2f_1} p_2^{2f_2} \ldots p_k^{2f_k}} \Rightarrow p_1^{g_1+2f_1} p_2^{g_2+2f_2} \ldots p_k^{g_k+2f_k} = p_1^{2e_1} p_2^{2e_2} \ldots p_k^{2e_k}$$

Així per a tota i tenim que $g_i + 2f_i = 2e_i \Rightarrow 2f_i \leq 2e_i \Rightarrow f_i \leq e_i \Rightarrow c|b$.

EX.: (86) S'ha de començar a jugar un partit de futbol i només disposem de dos rellotges de sorra que mesuren 6 i 11 minuts. És possible mesurar exactament els 45 minuts que ha de durar cada part? Trobeu totes les possibles maneres de fer-ho.

Diem x ="número de vegades que s'ha de posar el rellotge de 6 minuts", y ="número de vegades que s'ha de posar el rellotge d'11 minuts", llavors cal resoldre l'equació diofàntica $6x + 11y = 45$. Com que el $mcd(6,11) = 1|45$ llavors té solució. Per determinar una solució particular només cal trobar una identitat de Bezout que es veu fàcilment:

$6 \cdot (2) + 11 \cdot (-1) = 1 \Rightarrow 6 \cdot (90) + 11 \cdot (-45) = 45$

per tant les solucions de la diofantica són $x = 90 + 11t$, $y = -45 - 6t$ i de totes aquestes solucions només tenen sentit en el nostre problema les que verifiquen:

$$\left.\begin{array}{l} x \geq 0 \\ y \geq 0 \end{array}\right\} \Rightarrow \left.\begin{array}{l} 90+11t \geq 0 \\ -45-6t \geq 0 \end{array}\right\} \Rightarrow \left.\begin{array}{l} t \geq -\frac{90}{11} \\ t \leq -\frac{45}{6} \end{array}\right\} \Rightarrow -8,18\ldots \leq t \leq -7,5\ldots \Rightarrow t=-8$$

per tant només hi ha una manera possible: $x = 90 + 11(-8) = 2$, $y = -45 - 6(-8) = 3$.

EX.: (93) Calculeu els enters positius tals que $a + b = 57$ i $mcm(a,b) = 680$.

Tenim que $57 = 3 \cdot 19$ i que $680 = 2^3 \cdot 5 \cdot 17$. Si sabem que $a = p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$, $b = p_1^{f_1}p_2^{f_2}\ldots p_k^{f_k}$ llavors $mcm(a,b) = p_1^{\max(e_1,f_1)}p_2^{\max(e_2,f_2)}\ldots p_k^{\max(e_k,f_k)} = 2^3 \cdot 5 \cdot 17$ per tant sabem que $k = 3$ i podem suposar que tenim els primers ordenats, és a dir, que: $p_1 = 2$, $p_2 = 5$, $p_3 = 17$ i $\max(e_1,f_1) = 3$, $\max(e_2,f_2) = 1$, $\max(e_3,f_3) = 1$. En el segon i tercer factor els exponents només poden ser $0,1$ però no poden coincidir ni en a ni en b els dos uns a la vegada (perquè $5^1 17^1 = 85 > 57$). És a dir que els dos nombres poden ser

$a = 2^{e_1}5^1 17^0$, $b = 2^{f_1}5^0 17^1$ (o a l'inrevés)

També sabem que un dels exponents e_1,f_1 ha de ser 3, però no pot ser $f_1 = 3$ ($2^3 5^0 17^1 = 136 > 57$). Llavors $e_1 = 3$ i per tant un dels nombres serà $2^3 5^1 17^0 = 40$ i l'altre nombre $40 + 2^{f_1}5^0 17^1 = 57 \Leftrightarrow 2^{f_1}5^0 17^1 = 17$ per tant l'altre exponent haurà de ser $f_1 = 0$. Finalment només hi ha dues solucions: $2^3 5^1 17^0 + 2^0 5^0 17^1 = 57$ o bé $2^0 5^0 17^1 + 2^3 5^1 17^0 = 57$ o sigui $40 + 17 = 57$ o bé $17 + 40 = 57$.

EX.: (95) Suposem que p és primer. Demostreu que són equivalents:

a) $p^2|a$.

b) $p^4|a^2$.

c) $p^3|a^2$.

d) $mcm(p^2,a) = |a|$.

e) $p^2|mcm(p,a)$.

Demostrem cadascuna de les implicacions (en alguna utilitzarem descomposició factorial i a d'altres sense):

a)⇒**b**) Si $p^2|a$ llavors per cert enter k tenim $a = kp^2$ per tant $a^2 = k^2p^4$ i llavors $p^4|a^2$.

b)⇒**c**) Si $p^4|a^2$ llavors per cert enter k tenim $a^2 = kp^4 = (kp)p^3$ per tant $p^3|a^2$.

c)⇒**d**) Utilitzem ara la descomposició factorial del nombre $a = \varepsilon p^{e_1}p_2^{e_2}\ldots p_k^{e_k}$ a on hem considerat que el primer factor és el primer p amb tots els $e_i \geq 0$. Sabem que $p^3|a^2$, és a dir, que $p^3|\varepsilon^2 p^{2e_1}p_2^{2e_2}\ldots p_k^{2e_k} \Rightarrow 3 \leq 2e_1 \Rightarrow e_1 \geq 1,5 \Rightarrow e_1 \geq 2$ i per tant el $max(e_1,2) = e_1$ i el mínim comú múltiple serà: $mcm(p^2,\varepsilon p^{e_1}p_2^{e_2}\ldots p_k^{e_k}) = p^{e_1}p_2^{e_2}\ldots p_k^{e_k} = |a|$.

d)⇒**e**) Com a l'anterior utilitzem la descomposició factorial: $a = \varepsilon p^{e_1}p_2^{e_2}\ldots p_k^{e_k}$. A partir de $mcm(p^2,\varepsilon p^{e_1}p_2^{e_2}\ldots p_k^{e_k}) = p^{e_1}p_2^{e_2}\ldots p_k^{e_k}$ obtenim que $e_1 \geq 2$ i per tant $mcm(p,\varepsilon p^{e_1}p_2^{e_2}\ldots p_k^{e_k}) = p^{e_1}p_2^{e_2}\ldots p_k^{e_k}$ per la qual cosa podem dir que $p^2|mcm(p,a)$.

e)⇒**a**) En aquesta darrera implicació utilitzem també descomposició factorial:

$a = \varepsilon p^{e_1} p_2^{e_2} \dots p_k^{e_k}$ d'on treiem que $mcm(p, \varepsilon p^{e_1} p_2^{e_2} \dots p_k^{e_k}) = p^{\max(1,e_1)} p_2^{e_2} \dots p_k^{e_k}$. Però sabem que $p^2 | p^{\max(1,e_1)} p_2^{e_2} \dots p_k^{e_k}$ per tant $2 \leq \max(1, e_1) \Rightarrow e_1 \geq 2$ i d'aquí tenim que $p^2 | a$.

EXERCICIS CONGRUÈNCIES

EX.: (2') Sigui $p > 3$ un nombre primer. Demostreu que:

a) Si $a^2 \equiv 4b^2 (\mathrm{mod}\, p)$ llavors $a \equiv 2b (\mathrm{mod}\, p)$ o $a \equiv -2b (\mathrm{mod}\, p)$.

b) Deduïu que les solucions de la congruència $x^2 \equiv 4 (\mathrm{mod}\, p)$ són els enters tals que $x \equiv 2 (\mathrm{mod}\, p)$ o $x \equiv -2 (\mathrm{mod}\, p)$.

c) És cert b) si p no és primer?

a)Si $a^2 \equiv 4b^2 (\mathrm{mod}\, p)$ llavors $a^2 - 4b^2 = kp$ per cert enter k, o sigui $(a - 2b)(a + 2b) = kp$ i com $p | kp \Rightarrow p | a - 2b$ o bé $p | a + 2b$ (pel lema d'Euclides), aleshores $a \equiv 2b$ o bé $a \equiv -2b$ mòdul p.

b)Aplicant l'apartat anterior: $x^2 \equiv 4 (\mathrm{mod}\, p) \Leftrightarrow x^2 \equiv 4 \cdot 1^1 (\mathrm{mod}\, p) \Rightarrow x \equiv 2 (\mathrm{mod}\, p)$ o $x \equiv -2 (\mathrm{mod}\, p)$.

c)Per $p = 5 \cdot 7 = 35$ tenim que els quadrats de $2, 12, 23, 33$ són $2^2 \,\mathrm{mod}\, p = 4$, $33^2 \,\mathrm{mod}\, p = 4$ (aquests dos són òbvis perquè $2^2 = 4$ i perquè $33 \equiv -2 \,\mathrm{mod}\, p$), $12^2 \,\mathrm{mod}\, p = 4$, $23^2 \,\mathrm{mod}\, p = 4$.

EX.: (13') Determineu els criteris de divisibilitat següents:

a) Per 6 si el nombre està escrit en base 10.

b) Per 7 si el nombre està escrit en octal.

a)Sigui $n = a_k a_{k-1} \dots a_1 a_{0(10}$ la seva expressió en base 10. Llavors:

n és múltiple de $6 \Leftrightarrow a_0 + a_1 10 + a_2 10^2 + \dots + a_{k-1} 10^{k-1} + a_k 10^k \equiv 0 \bmod 6 \Leftrightarrow$

$\Leftrightarrow a_0 + a_1 4 + a_2 4 + \dots + a_{k-1} 4 + a_k 4 \equiv 0 \bmod 6 \Leftrightarrow a_0 + 4(a_1 + a_2 + \dots + a_{k-1} + a_k)$ és múltiple de 6.

b)Procedim de la mateixa manera: n és múltiple de $7 \Leftrightarrow a_0 + a_1 8 + a_2 8^2 + \dots + a_{k-1} 8^{k-1} + a_k 8^k \equiv 0 \bmod 7 \Leftrightarrow$

$\Leftrightarrow a_0 + a_1 1 + a_2 1 + \dots + a_{k-1} 1 + a_k 1 \equiv 0 \bmod 7 \Leftrightarrow a_0 + a_1 + a_2 + \dots + a_{k-1} + a_k$ és múltiple de 7.

EX.: (15) Idem que els fets a classe. Us els passo detallats.

Demostreu que no hi ha cap enter n tal que $6n + 5$ sigui un quadrat.

Volem veure que no té solució l'equació $x^2 = 6n + 5 \equiv 5 \bmod 6$. Si existís un enter x llavors $\bar{x}^2 = \bar{5}$ a $\mathbb{Z}_6$. Però si observem els quadrats a $\mathbb{Z}_6$ veurem que és impossible:

x	$x^2 \bmod 6$
0	0
1	1
2	4
3	3
4	4
5	1

EX.: (17) Demostreu que per a tot $n \geq 0$ el nombre $3^{2n+2} - 8n - 9$ és múltiple de 64 usant classes modulars i inducció.

Primer formalitzem: per a tot $n \geq 0$ en el conjunt $\mathbb{Z}_{64}$ el nombre $\overline{3}^{2n+2} - \overline{8}\overline{n} - \overline{9} = \overline{0}$.

CAS $n = 0$: cal demostrar que $\overline{3}^{2\cdot0+2} - \overline{8} \cdot \overline{0} - \overline{9} =^{???} \overline{0}$; en efecte:
$\overline{3}^{2\cdot0+2} - \overline{8} \cdot \overline{0} - \overline{9} = \overline{3}^2 - \overline{0} - \overline{9} = \overline{9} - \overline{9} = \overline{0}$.

CAS $n-1 \Rightarrow$CAS n: supossem que $\overline{3}^{2(n-1)+2} - \overline{8} \cdot \overline{n-1} - \overline{9} = \overline{0}$ (HI) i demostrem que $\overline{3}^{2n+2} - \overline{8}\overline{n} - \overline{9} =^{???} \overline{0}$. Calcularem $\overline{3}^{2n+2} - \overline{8}\overline{n} - \overline{9}$ utilitzant el fet que
$\overline{3}^{2n} - \overline{8} \cdot \overline{n} + \overline{8} - \overline{9} = \overline{0} \Leftrightarrow \overline{3}^{2n} = \overline{8}\overline{n} + \overline{1}$ és a dir:

$\overline{3}^{2n+2} - \overline{8}\overline{n} - \overline{9} = \overline{3}^{2n}\overline{3}^2 - \overline{8}\overline{n} - \overline{9} = (\overline{8}\overline{n} + \overline{1})\overline{9} - \overline{8}\overline{n} - \overline{9} = \overline{64}\overline{n} + \overline{0} = \overline{0}$

EX.: (32') Resoleu les congruències següents:

a) $17x \equiv 3 (\bmod 15)$.

b) $8x \equiv 4 (\bmod 14)$.

c) $12x \equiv 9 (\bmod 10)$.

a)Per resoldre aquesta congruència hem de trobar l'invers de $17 \equiv 2 \bmod 15$ (coprimer amb el mòdul) que es calcula provant (si no amb l'algorisme d'Euclides) i és 8:

$17x \equiv 3 (\bmod 15) \Leftrightarrow 8 \cdot 2x \equiv 8 \cdot 3 (\bmod 15) \Leftrightarrow x \equiv 9 (\bmod 15)$

b)En aquesta congruència el 8 no té invers i llavors utilitzem una de les propietats per resoldre-les:

$8x \equiv 4 (\bmod 14) \Leftrightarrow 2 \cdot 4x \equiv 2 \cdot 2 (\bmod 2 \cdot 7) \Leftrightarrow 4x \equiv 2 (\bmod 7)$

ara el 4 sí que té invers mòdul 7 (és 2):

$\ldots \Leftrightarrow 2 \cdot 4x \equiv 2 \cdot 2 (\bmod 7) \Leftrightarrow x \equiv 4 (\bmod 7)$

c)De la mateixa manera:

$12x \equiv 9 (\bmod 10) \Leftrightarrow 2x \equiv 9 (\bmod 10)$

però el 2 no té invers i no hi ha un factor a tot arreu per simplificar, per tant sabem que hi ha un nombre (el 5) tal que $2 \cdot 5 \equiv 0 (\bmod 10)$ per la qual cosa si hi hagués una solució x llavors:

$2x \equiv 9 (\bmod 10) \Rightarrow 5 \cdot 2x \equiv 5 \cdot 9 (\bmod 10) \Rightarrow 0 \equiv 5 (\bmod 10)$

cosa contradictòria, per tant la congruència no té solució.

EX.: (42') Resoleu el sistema següent: $x \equiv 3 (\bmod 4), x \equiv 5 (\bmod 6), x \equiv 9 (\bmod 10)$.

Fem el sistema de les dues primeres equacions:

$$\left.\begin{array}{l} x \equiv 3 \pmod 4 \\ x \equiv 5 \pmod 6 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x = 3 + 4a \\ x \equiv 5 + 6b \end{array}\right\} \Rightarrow 3 + 4a = 5 + 6b \Leftrightarrow 4a - 6b = 2 \Leftrightarrow 2a - 3b = 1$$

Aquesta equació diofàntica té solució perquè $mcd(2,3) = 1|1$. És molt fàcil trobar que:
$2 \cdot (-1) - 3 \cdot (-1) = 1$

per tant les solucions de la diofantica són $a = -1 + 3t, b = -1 + 2t$ i d'aquí $x = 3 + 4a = 3 + 4(-1 + 3t) = -1 + 12t$ o sigui $x \equiv -1 \bmod 12$ per tant reduint queda $x \equiv 11 \bmod 12$. A continuació resolem el sistema amb la darrera equació:

$$\left.\begin{array}{l} x \equiv 11 \bmod 12 \\ x \equiv 9 \bmod 10 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x = 11 + 12a \\ x = 9 + 10b \end{array}\right\} \Rightarrow 11 + 12a = 9 + 10b \Leftrightarrow 12a - 10b = -2 \Leftrightarrow 6a -$$

Aquesta equació diofàntica té solució perquè $mcd(6,5) = 1|-1$. Per aquesta també és molt fàcil trobar una identitat de Bezout:
$6 \cdot (1) - 5 \cdot (1) = 1 \Rightarrow 6 \cdot (-1) - 5 \cdot (-1) = -1$

per tant les solucions de la diofantica són $a = -1 + 5t, b = -1 + 6t$ i d'aquí $x = 11 + 12a = 11 + 12(-1 + 5t) = -1 + 60t$ o sigui $x \equiv -1 \bmod 60$ per tant reduint queda $x \equiv 59 \bmod 60$ que és la solució final del sistema d'equacions.