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.

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 $p|a, p|b \Rightarrow a \equiv 0,\ a^n \equiv 0$, $a^m \equiv 0 \Rightarrow a^n \equiv a^m(\mathrm{mod}\, p)$.

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 $\mathbb{Z}_5$:

- 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) $11^{1234}(\mathrm{mod}\, 14)$: tenim que $14 = \quad \cdot \quad$, $1234\, \mathrm{mod}\, 6 = 4$ llavors:

$$\left.\begin{aligned} 11^{1234}\, \mathrm{mod}\, 2 &\equiv \square^{1234}\, \mathrm{mod}\, 2 \equiv \quad \equiv -3 \\ 11^{1234}\, \mathrm{mod}\, 7 &\equiv \square^{1234}\, \mathrm{mod}\, 7 \equiv \square^{4}\, \mathrm{mod}\, 7 \equiv 4 \equiv \end{aligned}\right\} \Rightarrow 11^{1234}\, \mathrm{mod}(mcm(2,7)) \equiv$$

$\Leftrightarrow 11^{1234}\, \mathrm{mod} \quad \equiv \quad \equiv$

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

$$\left.\begin{aligned} 7^{1234}\, \mathrm{mod}\, 3 &\equiv 1^{1234}\, \mathrm{mod}\, 3 \equiv 1 \\ 7^{1234}\, \mathrm{mod}\, 5 &\equiv 2^{1234}\, \mathrm{mod}\, 5 \equiv 2^2\, \mathrm{mod}\, 5 \equiv 4 \\ 7^{1234}\, \mathrm{mod}\, 11 &\equiv 7^4\, \mathrm{mod}\, 11 \equiv 3 \end{aligned}\right\} \Rightarrow ???$$

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

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

Faig el sistema de les dues primeres equacions:

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

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:

$$\left.\begin{array}{l} x \equiv 4 \bmod 15 \\ x \equiv 3 \bmod 11 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x = \qquad\qquad \\ x = \qquad\qquad \end{array}\right\} \Rightarrow \qquad = \qquad \Leftrightarrow$$

Aquesta equació diofàntica té solució perquè $mcd(\quad , \quad) = \quad | \quad$. Ara una solució particular:

$\qquad = \quad \Rightarrow$

per tant les solucions de la diofantica són $a = \qquad , b = \qquad$ i d'aquí $x = 4 + 15a$ $= 4 + 15\left(\qquad \right) = \qquad$ o sigui $x \equiv \quad \bmod \quad$ per tant reduint queda $x \equiv \quad \bmod \quad$.

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

Tenim que 251 és primer i com que $1025 \bmod 250 = 25$ llavors:

$25^{1025} \bmod 251 = 25^{\quad} \bmod 251 = \qquad \bmod 251$

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

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 $8^{1235} \equiv \square^{1235} \equiv \square^{\square} \equiv \quad \mathrm{mod}\, 3$ perquè $1235 \,\mathrm{mod}\, 2 = 1$
- A $\mathbb{Z}_5$ tenim que $8^{1235} \equiv \square^{1235} \equiv \square^{\square} \equiv \quad \mathrm{mod}\, 5$ perquè $1235 \,\mathrm{mod}\, 4 = 3$

Com que $mcm(3,5) = 15$ llavors $8^{1235} \,\mathrm{mod}\, 15 = \quad$.

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 existeix un x enter tal que $x^2 = a$. 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 $c|b \cdot b$ i $mcd(b,c) = 1$ i pel lema de
obtenim que $c|$

i com que $c|$ i $mcd(b,c) = 1$ llavors $c =$ i per tant $a = \frac{b^2}{2} =$ 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:

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

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 $mcd(6,11) = \ |45$ llavors té solució. Per determinar una solució particular només cal trobar una identitat de Bezout:

$6 \cdot (\quad) + 11 \cdot (\quad) = \quad \Rightarrow 6 \cdot (\quad) + 11 \cdot (\quad) =$

per tant les solucions de la diofantica són $x = \qquad , y = \qquad$ i de totes aquestes solucions només tenen sentit en el nostre problema les que verifiquen:

$$\left.\begin{array}{l} x \geq 0 \\ y \geq 0 \end{array}\right\} \Rightarrow \qquad \left.\begin{array}{l} \geq 0 \\ \geq 0 \end{array}\right\} \Rightarrow \qquad \left.\begin{array}{l} \geq 0 \\ \geq 0 \end{array}\right\} \Rightarrow \qquad \leq t \leq$$

per tant les maneres possibles són:

EX.: (93,95) Passar-los fets.

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 $(\qquad)(\qquad) = kp$ i com $p|\qquad \Rightarrow p|$

b)

c)Per $p = 5 \cdot 7$ tenim que els quadrats de $2, 12, 23, 33$ són

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

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

b)Idem: n és múltiple de $7 \Leftrightarrow a_0 + a_1 \boxed{} + a_2 \boxed{}^2 + \ldots + a_{k-1} \boxed{}^{k-1} + a_k \boxed{}^k \equiv 0 \bmod \boxed{} \Leftrightarrow$

EX.: (15,17) Idem que els fets a classe. Us els passo detallats.

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

a) $17x \equiv 3(\mathrm{mod}\,15)$.

b) $8x \equiv 4(\mathrm{mod}\,14)$.

c) $12x \equiv 9(\mathrm{mod}\,10)$.

a) $17x \equiv 3(\mathrm{mod}\,15) \Leftrightarrow$

b) $8x \equiv 4(\mathrm{mod}\,14) \Leftrightarrow$

c) $12x \equiv 9(\mathrm{mod}\,10) \Leftrightarrow$

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

Faig el sistema de les dues primeres equacions:

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

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

$2 \cdot (\quad) - 3 \cdot (\quad) = 1$

per tant les solucions de la diofantica són $a = \quad, b = \quad$ i d'aquí $x = 3+4a = 3+4\left(\quad\right) = \quad$ o sigui $x \equiv \quad \bmod \quad$ per tant reduint queda $x \equiv \quad \bmod \quad$ i ara al resoldre el sistema amb la darrera equació:

$$\left.\begin{array}{l} x \equiv \quad \bmod \\ x \equiv 9(\bmod 10) \end{array}\right\} \Rightarrow \left.\begin{array}{l} x = \\ x = 9+10b \end{array}\right\} \Rightarrow$$