CONGRUÈNCIES

Donat $m \geq 1$

$a \equiv b \mod(m) \Leftrightarrow m \mid a-b$

$\Leftrightarrow b = mk + a$ per cert $k \in \mathbb{Z}$

$\Leftrightarrow$ a i b tenen mateix residu al dividir entre m

Quan $a \equiv b \mod(m)$ es diu: "a és congruent amb b mòdul m."

Propietat 1

La congruència de m és una relació d'equivalència.

$\mathbb{Z}_m$ "Conjunt dels enters modulars mòdul m."

- Reflexiva aRa
- Simètrica $aRb \to bRa$
- Trans. $aRb, bRc \to aRc$

Demo: Fem servir la 3ª caracterització (mateix residu) de la congruència.

Classes Modulars

La classe de a per la relació de congruència mod. m es denota per $\bar{a}$ i el conjunt quocient es denota amb $\mathbb{Z}_m$.

(Agrupació de les classes d'equiv.)

Exemple: $m = 5$.

$\bar{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 5\} = \{5k \mid k \in \mathbb{Z}\}$

$\bar{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 5\} = \{5k+1 \mid k \in \mathbb{Z}\}$

$\bar{2} = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 5\} = \{5k+2 \mid k \in \mathbb{Z}\}$ $\quad \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\bar{3} = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 5\} = \{5k+3 \mid k \in \mathbb{Z}\}$

$\bar{4} = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod 4\} = \{5k+4 \mid k \in \mathbb{Z}\}$

Fets:

I. $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod m\} = \{mk + a \mid k \in \mathbb{Z}\}$

II. $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod m$

III. $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$

Propietat 2

$$\left.\begin{array}{l} a = a' \pmod m \\ b = b' \pmod m \end{array}\right\} \Rightarrow \begin{array}{l} a+b \equiv a'+b' \pmod m \\ a \cdot b = a' \cdot b' \pmod m \end{array}$$

Demo: $m \mid a'-a$, $m \mid b'-b$ $\Rightarrow m \mid [(a'-a)+(b'-b)] \Rightarrow m \mid [(a'+b')-(a+b)] \Rightarrow a+b \equiv a'+b' \pmod m$ ✓

$m \mid [b'(a'-a) + a(b'-b)] \Rightarrow m \mid [a'b' - ab] \Rightarrow ab \equiv a'b' \pmod m$ ✓

FM-6-7-1

Em particular: $a \equiv a' \pmod m \Rightarrow a^n \equiv a'^n \pmod m$
$\Rightarrow ka \equiv ka' \pmod m$

Exemple: Residu de div. $58 * 79 \bmod 11$

$58 \equiv 3 \pmod{11}$, $79 \equiv 2 \pmod{11}$ $\Rightarrow 58*79 \equiv 3*2 \pmod{11} \Rightarrow 58*79 \equiv 6 \pmod{11}$

Exemple: Calculem $2^{1000000}$ a mà amb (mod 100)

$2 \equiv 2 \pmod{100}$ $2^{10} = 2\cdot 2^9 \equiv 2\cdot 12 \pmod{100} \equiv 24 \pmod{100}$

$2^2 \equiv 4 \pmod{100}$ $2^{20} = 2^{10}\cdot 2^{10} \equiv 24\cdot 24 \pmod{100} \equiv 76 \pmod{100}$

$2^7 \equiv 28 \pmod{100}$ $2^{22} = 2^2\cdot 2^{20} \equiv 4\cdot 76 \pmod{100} \equiv 4 \pmod{100}$

$2^8 \equiv 56 \pmod{100}$ $2^{42} = 2^2\cdot 2^{20}\cdot 2^{20} \equiv 4\cdot 76\cdot 76 \pmod{100} \equiv 4 \pmod{100}$

$2^9 \equiv 12 \pmod{100}$ $2^2 \equiv 2^2\cdot 2^{20} \equiv 2^2\cdot 2^{20}\cdot 2^{20}$ És un patró t.q. $2^2\cdot 2^{20k} \equiv 4 \pmod{100}$

Ara volem saber aquest 'k' i hauríem de fer $999998 \div 20$. Donat que és $2^{(2+20k)}$ → restar-ho

$999998 = 49999\cdot 20 + 18$. Això sig. que $1000000 = 2 + 18 + 49999\cdot 20$,

$2^{1000000} \equiv 2^2\cdot 2^{20\cdot 49999}\cdot 2^{18} \equiv 2^2\cdot 2^{18} \equiv 2^{20} \equiv 76 \pmod{100} \equiv 2^{1000000}$

Altres Propietats de les congruències

I. Si $a \equiv b \pmod m \wedge d \mid m \Rightarrow a \equiv b \pmod d$

II. Si $k > 0 \Rightarrow a \equiv b \pmod m \Leftrightarrow ka \equiv kb \pmod{km}$

III. Si $mcd(k, m) = 1 \Rightarrow ka \equiv kb \pmod m \Leftrightarrow a \equiv b \pmod m$

IV. $a \equiv b \pmod{m_1}, \dots, a \equiv b \pmod{m_n} \Leftrightarrow a \equiv b \pmod{mcm(m_1, \dots, m_n)}$

Demo: $a \equiv b \pmod m \wedge d \mid m \Rightarrow a \equiv b \pmod d$

$a \equiv b \pmod m \overset{def}{\Leftrightarrow} m \mid (a-b)$, $d \mid m$ $\overset{Trans}{\Rightarrow} d \mid (a-b) \overset{def}{\Leftrightarrow} a \equiv b \pmod d$ ☑

Demo: Si $k > 0 \Rightarrow a \equiv b \pmod m \Leftrightarrow ka \equiv kb \pmod{km}$

$a \equiv b \pmod m \Leftrightarrow m \mid (a-b) \Leftrightarrow km \mid (a-b)k \Leftrightarrow km \mid ak - bk \Leftrightarrow ak \equiv bk \pmod{km}$ ☑

Demo: Si $\text{mcd}(k,m)=1 \Rightarrow ka \equiv kb \pmod m \Leftrightarrow a \equiv b \pmod m$

$\Rightarrow$|

$ka \equiv kb \pmod m \Leftrightarrow m \mid (ka-kb) \Rightarrow m \mid (a-b)\cdot k$

Donat que per hipòtesi tenim que $\text{mcd}(k,m)=1$ podem aplicar Lema Gauss

$m \mid (a-b)\cdot k \wedge \text{mcd}(m,k)=1 \Rightarrow m \mid (a-b) \Leftrightarrow a \equiv b \pmod m$ ☑

$\Leftarrow$|

Si $m \mid (a-b)$ clarament $m \mid (a-b)\cdot k$ (Propietat de la trans) ☑

Demo: $a \equiv b \pmod{m_1}, \dots, a \equiv b \pmod{m_n} \Leftrightarrow a \equiv b \pmod{\text{mcm}(m_1,\dots,m_n)}$

Si $m_1 \mid (a-b), \dots, m_n \mid (a-b) \overset{\text{def mcm}}{\Leftrightarrow} \text{mcm}(m_1,\dots,m_n) \mid (a-b)$ ☑

Exemple: $8x \equiv 28 \pmod 6$

$8x \equiv 28 \pmod 6 \overset{\text{Prop II}}{\Rightarrow} 4x \equiv 14 \pmod 3 \overset{\text{Prop III}}{\Rightarrow} 2x \equiv 7 \pmod 3$ Però aquí ja no podem aplicar altre prop.

$2x \equiv 7 \pmod 3 \overset{\text{def}}{\Leftrightarrow} 3 \mid (2x-7) \overset{\text{def}}{\Leftrightarrow} \exists x \in \mathbb{Z} : 2x-7 = 3x \Rightarrow 2x-3x = 7$ ← Diph. eq.

Aritmètica Modular

Podem def. una aritmètica (op. de suma i producte) al conjunt $\mathbb{Z}_m$ de la següent manera:

$\bar a + \bar b = \overline{a+b}$ ← Classe d'Equiv.

$\bar a \cdot \bar b = \overline{ab}$

Això és valid per la prop. II.

$\left.\begin{matrix}\bar a = \bar{a'} \\ \bar b = \bar{b'}\end{matrix}\right\} \Rightarrow \begin{matrix}\overline{a+b} = \overline{a'+b'} \\ \overline{ab} = \overline{a'b'}\end{matrix}$

Per exemple en $\mathbb{Z}_{3000}$: $\overline{2990} * \overline{2995} = \overline{10} * \overline{5} \leftarrow \overline{50}$ # Millor primer simplifiquem

Propietats

I. De la suma:

A. $\bar a + \bar b = \bar b + \bar a$

B. $(\bar a + \bar b) + \bar c = \bar a + (\bar b + \bar c)$

C. $\bar a + \bar 0 = \bar a$

D. $\bar a + \overline{-a} = \bar 0$

E. $n\bar a = \overline{na}$ per $n \geq 1$

II. Del producte:

A. $\bar a \cdot \bar b = \bar b \cdot \bar a$

B. $(\bar a \cdot \bar b)\cdot \bar c = \bar a \cdot (\bar b \cdot \bar c)$

C. $\bar a \cdot \bar 1 = \bar a$

D. $\bar a^n = \overline{a^n}$ per $n \geq 1$

III. $\bar a \cdot (\bar b + \bar c) = \bar a \cdot \bar b + \bar a \cdot \bar c$ ← Distributiva

$\bar{2}\cdot\bar{2} = \bar{2}\cdot\bar{5}$ (≠9) (10 = 4) però $\bar{2} \neq \bar{5}$

⚠ NO és pot simplificar. Per exemple $\mathbb{Z}_6$, $\bar{2}\cdot\bar{2} = \bar{2}\cdot\bar{5}$ però $\bar{2} \neq \bar{5}$

Això és degut a que $\bar{a}\cdot\bar{5} = \bar{0}$ tot i que $\bar{a} \neq \bar{0}$ i $\bar{b} \neq \bar{0}$. Per exple en $\mathbb{Z}_6$, $\bar{2}\cdot\bar{3} = \bar{0}$.

Obs: Quan tenim dues operacions que satisfem totes propietats de "+" i "*", i diu que tenim un anell.

Obs: Quan tots els elements no nuls d'un conjunt tenen invers és diu que tenim un anell.

$\bar{a} + \overline{-a} = \bar{0}$
$\bar{a} * \overline{-a} = \bar{1}$

$\mathbb{Z}_6$:

*	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Podem veure que els únics que tenen invers són $\bar{1}$ i $\bar{5}$.

Pq.. $\bar{2} * \overline{-2} = \overline{-4} \neq \bar{1}$

$\bar{5} * \overline{-5} = \overline{-25} = \bar{1}$ (25 L 6, 1, 4)

Com que no són tots, no tenim cos.

Complement a 2

Mateixa teoria que en I.C. En aquest cas es pot fer servir per simplificar càlculs.

Representant	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
Binari	000	001	010	011	100	101	110	111
Ca 2	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\overline{-4}$	$\overline{-3}$	$\overline{-2}$	$\overline{-1}$

$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

Són el mateix

$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \overline{-4}, \overline{-3}, \overline{-2}, \overline{-1}\}$

Inversos Modulars

Buscar un invers (respecte multi) de $\bar{a}$ en $\mathbb{Z}_m$ és trobar x t.q $\bar{a}\cdot\bar{x} = \bar{1}$

Tmb. és pot veure t.q. $ax \equiv 1 \pmod m \Rightarrow mk = ax - 1 \Rightarrow 1 = ax - mk \Rightarrow$

$[k = -y] \Rightarrow \boxed{ax + my = 1}$ ← Eq diofàntica

Llavors podem dir que: $\boxed{\bar{a} \text{ té invers en } \mathbb{Z}_m \Leftrightarrow mcd(a,m) = 1.}$ # Pq. si no fos 1 mcd(a,m) ≠ 1

Exemple: Tenen invers modular $\bar{5}$ i $\bar{6}$ en $\mathbb{Z}_9$?

$\bar{5}$: $mcd(5,9) = 1$ ✓ Sí que té | $\bar{6}$: $mcd(6,9) = 3 \neq 1$ ✗ No té.

Exemple: Té invers modular $\overline{227}$ en $\mathbb{Z}_{2\cdot 292}$? Calcula. $227x + 2292y = 1$

y	1	0	1	-10	31
x	0	1	-10	101	(-313)
Q	-	10	10	3	-
R	2292	227	22	7	(1) ← mcd

En aquest cas només ens interessa, així que l'invers modular de $\overline{227}$

$\overline{227}\cdot(-313) + \overline{2292}\,y = \bar{1}$

$\overline{227}\cdot(\overline{-313}) + \bar{0}\,y = \bar{1}$

$\overline{227}\,(\overline{-313}) = \bar{1}$ # 2292 - 313 = 1979

Veiem que $mcd(2292, 227) = 1 \Rightarrow \overline{227}$ té invers en $\mathbb{Z}_{2292}$

$\boxed{\text{Invers: } \overline{227}^{-1} = \overline{1979}}$

Exemple: $\overline{6x} \equiv \overline{6} \pmod 9$

Primerament veiem que $\text{mcd}(6,9) = 3 \neq 1$, llavors $\overline{6}$ no té invers.

El que sí que podem fer és simplificar-ho per treballar millor: $\overline{2x} \equiv \overline{2} \pmod 3$

Ara $\text{mcd}(2,3) = 1$ així que sí que hi ha invers, i també podem aplicar prop III ⊛

$\overline{x} \equiv \overline{1} \pmod 3$ i així fa que $\overline{x} = \overline{1}, \overline{4}, \overline{7}, \overline{10}, \ldots$

Hem de recordar que estàvem en $\mathbb{Z}_9$ així que només ens interessa $\overline{1}, \overline{4}, \overline{7}$.

Així que podem dir que $\overline{6x} \equiv \overline{6} \pmod 9 \Rightarrow \overline{x} = \overline{1}, \overline{4}, \overline{7}$.

⊛ $\text{mcd}(k,m) = 1$
$ka \equiv kb \pmod m$
$a \equiv b \pmod m$

$\mathbb{Z}_m$ cos

Un cos és un anell on tot element llevat del $\overline{0}$ té invers. **$\mathbb{Z}_m$ cos $\Leftrightarrow$ m primer**

Demo: $\mathbb{Z}_m$ cos $\Leftrightarrow$ m primer

$\mathbb{Z}_m$ cos $\Leftrightarrow \forall \overline{k} \neq \overline{0}$ té invers en $\mathbb{Z}_m \Leftrightarrow \forall\ 1 \leq k \leq m-1$ coprimers $\Leftrightarrow$ m primer □.

Recordo que $\text{mcd}(m,k) = 1$ pq tingui invers i si m és primer i k més pot ser = m, significa que aquest mcd sempre serà 1.

Sistemes de Congruències

Siguin $m_1, m_2, \ldots, m_k$ # positius i coprimers, $\forall i$ $a_1, a_2, \ldots, a_i$ existeix solució x del sistema.

$x \equiv a_1 \pmod{m_1}$ Si tenim sol. particular t.q. $x = x_0 \bmod M$, $\#M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$

$x \equiv a_2 \pmod{m_2}$ totes les altres es poden escriure t.q. $x = x_0 + Mk$ on $k \in \mathbb{Z}$

$\vdots$

$x \equiv a_k \pmod{m_k}$ # $x = x_0 + M$, $x = x_0 + 2M$, $x = x_0 + 3M$, ...

⚠ Es redueix tot a veure si té sol, i després trobar-la (en la pràctica).

Mètode: $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$.

Tenim que $x = a_1 + m_1 y = a_2 + m_2 z$ on $y, z \in \mathbb{Z} \Rightarrow$ **$a_2 - a_1 = m_1 y - m_2 z$**

Donat que $m_1, m_2, \ldots, m_k$ eren coprimers aquesta eq. diof. té solució.

Això fa que y, z tinguem x que és solució del sistema xinès.

Obs: Sistema tindrà solució si $\text{mcd}(m_1, m_2) \mid a_2 - a_1$ # No significa que $a_2 - a_1$ sigui 1, sinó que així sempre es compleix t.q. al ser m_1, m_2 coprimers el mcd = 1 i 1 | qualsevol enter.

$ax \equiv b \pmod n$ té sol $\Leftrightarrow \text{mcd}(a,n) \mid b$

IMPORTANT

Exemple: $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$. # Veiem que mcd(3,4,5) = 1.

$\overbrace{M = 3\cdot4\cdot5 = 60}^{mcm}$, $M_1 = 4\cdot5 = 20$, $M_2 = 3\cdot5 = 15$, $M_3 = 3\cdot4 = 12$

Ara volem començar a resoldre: $2\cdot2=4$ i $4 \div 3 = 3\cdot1 + 1$ Llavors $x_1 \equiv 2 \pmod{3}$

$M_1 x_1 \equiv 1 \pmod{m_1} \Rightarrow 20x_1 \equiv 1 \pmod{3} \Rightarrow 2x_1 \equiv 1 \pmod{3} \Rightarrow x_1 \equiv 2 \pmod{3}$

$M_2 x_2 \equiv 2 \pmod{m_2} \Rightarrow 15x_2 \equiv 2 \pmod{4} \Rightarrow 3x_2 \equiv 2 \pmod{4} \Rightarrow x_2 \equiv 3 \pmod{4}$

$M_3 x_3 \equiv 3 \pmod{m_3} \Rightarrow 12x_3 \equiv 3 \pmod{5} \Rightarrow 2x_3 \equiv 3 \pmod{5} \Rightarrow x_3 \equiv 4 \pmod{5}$ ($2\cdot4=8$, $8 \div 5$: residu 3)

Ara ja podem donar la solució específica:

$x = M_1x_1b_1 + M_2x_2b_2 + M_3x_3b_3 = 20\cdot2\cdot1 + 15\cdot3\cdot2 + 12\cdot4\cdot3 = 40 + 90 + 144 = 274$

$270 - 60*4 = 34 \Rightarrow$ $\boxed{x \equiv 34 \pmod{60}}$ $\boxed{x = 34 + 60t,\ t \in \mathbb{Z}}$

Teorema petit de Fermat

Si p primer i $mcd(p,a) = 1$ on $a \in \mathbb{Z} \Rightarrow \boxed{a^{p-1} \equiv 1 \pmod{p}}$

Demo: $a^{p-1} \equiv 1 \pmod{p}$ on p primer i $p \nmid a$.

Considerem els múltiples de a t.q.: $m_1 = a$, $m_2 = 2a$, ..., $m_{p-1} = (p-1)\cdot a$

Podem veure que $p \nmid m_i$ (Pq $p \nmid a$ (per que suposem) i estem considerant fins $p-1$) $\Rightarrow p \nmid p-1$ això és impossible.

Per la divisió euclidiana tenim que $m_i = a*i = p\cdot q_i + r_i$ amb $0 < r_i \leq p-1$.

Però donat que $p \nmid m_i \Rightarrow r_i \neq 0$ (Pq si fos '0' sig que el divideix).

- Ara hem de veure que el residu de cada m_i dividit per p és únic: # Donat que $p \nmid m_i \Rightarrow$ deixa residu la div.

Tenim dos $\mathbb{Z}$ diferents i, j on $1 \leq i, j \leq p-1$ i tenim $r_i = r_j$.

Si això és així, sig: $\left.\begin{array}{l} m_i = p\cdot q_i + r_i \\ m_j = p\cdot g_j + r_i \end{array}\right\} \Rightarrow m_i - m_j = p\cdot q_i - p\cdot q_j + (r_i - r_i)$ ($r_i = r_j$)

$m_i = a*i \rightarrow a*i - a*j = p(q_i - g_j) + 0$

$a*(i-j) = p(q_i - g_j)$

Però donat que $p \nmid a \Rightarrow p \mid (i - j)$ (Lema Euclides) i això és IMPOSSIBLE $1 \leq i, j \leq p-1$.

Això sig que cada residu de m_i és únic i com que són més petits que p

segueixen la forma $\{1, 2, ..., p-1\} = \{r_1, r_2, ..., r_{p-1}\}$.

- Suposem sense perdre generalitat $r_i = i \Rightarrow m_i = p\cdot q_i + r_i = p\cdot q_i + i$.

Això significa que $m_i \equiv i \pmod{p} \Rightarrow a*2a*...*(p-1)a \equiv 1*2*...*(p-1) \pmod{p}$

$\Rightarrow a^{p-1}(1)*(2)*...*(p-1) \equiv 1*2*...*(p-1) \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$. :)

#No tenia més espai així que es queda així ;)

Petit Teorema de Fermat (V.2.)

$$n \equiv m \pmod{p-1} \Rightarrow a^n \equiv a^m \pmod{p}$$

Demo: $n \equiv m \pmod{p-1} \Rightarrow a^n \equiv a^m \pmod{p}$

Suposem: $n \equiv m \pmod{p-1}$ Volem Demo: $a^n \equiv a^m \pmod{p}$.

Si partim de $n \equiv m \pmod{p-1} \Rightarrow n = (p-1)\cdot k + m$ per un k enter.

Això ei pot expresar t.q: $a^n = a^{m+(p-1)k} = a^m \cdot a^{(p-1)k}$

Pel 6è primer vers del PTF sabem que $a^{p-1} \equiv 1 \pmod{p}$ llavors simplica que

$a^{(p-1)k} \equiv 1^k \pmod{p} \Rightarrow a^{(p-1)k} \equiv 1 \pmod{p}$.

Per tant podem dir que $a^n = a^m \cdot a^{(p-1)k} \equiv a^m \cdot 1 \pmod{p}$

$a^n \equiv a^m \pmod{p}$ → El que buscàvem ☑.

Exemple PTF(V.1): 43^{3221} mòdul 13. Calc Residu:

Primer hem de veure que $\text{mcd}(43,13) = 1$ i que $43 \mid 13$ → $4 \mid 3$ $\Rightarrow 43 \equiv 4 \pmod{13}$

El PTF ens diu que $4^{13-1} \equiv 1 \pmod{13} \Rightarrow 4^{12} \equiv 1 \pmod{13}$

El que busquem ara és agrupar 3221 en "grups" de 12 pq. Sabem que $\equiv 1 \pmod{13}$.

$3221 \mid 12$ → 268

24

82

72

101

96

005

Llavors tenim $4^{3221} = (4^{12})^{268} \cdot 4^5 \equiv 1^{268} \cdot 4^5 \equiv 4^5 \equiv 1024 \equiv 10 \pmod{13}$

$\#4^5 = 4^2 \cdot 4^2 \cdot 4 = 16 \cdot 16 \cdot 4 = 1024$

$1024 \mid 13$ → 78

91

014

10

Llavors podem dir que:

$$43^{3221} \equiv 10 \pmod{13}$$

Exemple PTF(V.2): 4^{3141} mòdul 137. Calc residu. # Sabem que 137 és primer.

Primer calculem $3141 \bmod 136$ $(137-1=136) \Rightarrow \overset{m}{3141} \equiv \overset{m}{13} \pmod{\overset{p-1}{136}}$

Llavors podem dir que $\overset{a^m}{4^{3141}} \equiv \overset{a^m}{4^{13}} \pmod{p}$

Calculem (amb calculadora) $4^{13} = 67108864$ i ara dividim entre 137.

$67108864 = 137 * 489845 - 99$ $\Rightarrow$

$$4^{3141} \equiv 4^{13} \equiv 99 \pmod{137}$$

RSA

Fabricació de Claus

1. Triem 2 primers p i q molt grans de magnitud semblant, però longitud diferent. Si tenim una magnitud similar, la "Factorització de Fermat" podria ser eficaç. Aquesta factorització és eficaç si la diferència $(|p-q|)$ és petita. Aquesta factorització busca a, b t.q. $: a^2 - n = b^2$. Si p, q pròxims és fàcil trobar.

2. Calculem $n = p \cdot q$. Aquest serà el nostre mòdul (serà públic).

3. Es fa servir funció $\lambda(n)$ "Lambda de Carmichael". $\lambda(n) = mcm(p-1, q-1)$ Aquest punt és important. $\lambda(n)$ és el nombre més petit t.q. $a^{\lambda(n)} \equiv 1 \pmod p$ i $a^{\lambda(n)} \equiv 1 \pmod q$ on a és coprimer amb p, q. Quant. de nombres coprimers amb a, $< n$ = exponent de xifrat

4. Escollim un e coprimer amb $\lambda(n)$, $1 < e < \lambda(n)$. Aquest és exponent públic. No ha de ser gaire gran per temes de velocitat, també en recomana pocs '1's en binari. #Normalment es fa servir $2^{16}+1 = 65537_{10} = 0001\ 0000\ 0000\ 0000\ 0001$

El motiu que tingui pocs 1's és pq així es calcula tot més ràpid donat que '0' només fa que desplaçar el nombre i no fa falta sumar (quan es multiplica).

5. Calculem un d que serà l'invers multiplicatiu de e mod $\lambda(n)$. Serà el valor t.q. $ed \equiv 1 \pmod{\lambda(n)}$. Aquest d permet que $(m^e)^d \equiv m \pmod n$. Aquest d és privat i permetrà desxifrar els missatges encriptats amb (e, n).

p, q primers diferents i $ed \equiv 1 \pmod{\lambda(n)} \Rightarrow (m^e)^d \equiv m \pmod n$

Clau Pública: (n, e). Tothom la pot conèixer i serveix per encriptar.

Clau Privada: (n, d). Només emissor de les claus la pot conèixer, serveix desencriptar. $d, p, q, \lambda(n)$ han de ser secret.

Lambda de Charmichael $\lambda(n)$

Propietats: associativa, $\exists$ neutre, $\exists$ invers.

Grup: Estructura algebraica. Conjunt elents + Operació que formen tercer elent.

Conjunt de coprimes amb n formen grup multiplicatiu mod n.

$\lambda(n)$ retorna el nombre positiu més petit t.q. $\forall$ elent del grup complet elent$^{\lambda(n)} \equiv 1 \pmod n$.

e ha de ser coprimer amb $\lambda(n)$ pq. existeixi l'invers d.

Xifrat

El missatge es codifica numèricament (amb UTF-8 per exemple). Si el tamany resultant és més petit que la longitud de n, s'afegeix "padding" per a fer-ho més segur. Si és més gran, es treballa amb blocs de $\text{len}(n)$.

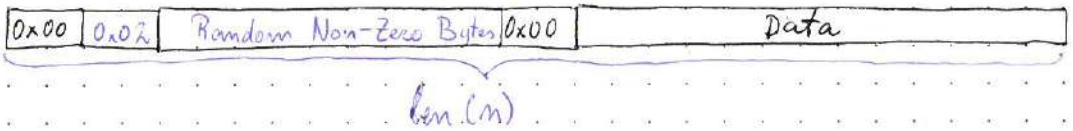
Quan ja tenim $m \Rightarrow c \equiv m^e \pmod n$ on e era expont públic i $n = p \cdot q$.

Els tamanys de n poden variar: 1024 bits, 2048 bits o fins 4096 bits. # $2048\text{ b} \approx 617$ xifres.

El padding no modifica el missatge i està ben delimitat per a treure-lo.

PKCS#1 v1.5

Estandard comú fet servir per afegir padding en RSA.



m abans de xifrar

⚠ A data 2023 NO es fa servir PKCS #1 v1.5 sinó OAEP. # Però era més difícil d'explicar

Desxifrat

Ara tenim el missatge c que ha estat encriptat amb e. $m^e \equiv c \pmod n$ # és equiv. simplement escrit al revés

Recordem que $e \cdot d \equiv 1 \pmod{\lambda(n)}$. # d és l'invers i exponent privat.

Per definició significa que $e \cdot d = 1 + \lambda(n)\,k$ on $k \in \mathbb{Z}$

Llavors tenim: $c^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+\lambda(n)k} \equiv M \cdot M^{\lambda(n)k} \pmod n$

Recordem també que $a^{\lambda(n)} \equiv 1 \pmod n$. Llavors podem reescriure com:

$c^d \equiv M \cdot M^{\lambda(n)k} \equiv M \cdot (1)^k \equiv M \pmod n$.

Com podem veure ja tenim el que buscàvem, a partir d'un c (missg. xifrat) hem pogut recuperar el M original gràcies a que e, d han sigut generats per la mateixa persona. # En el sentit que no podrien ser e, d qualsevol.

Firma

En aquest cas s'eleva a d el hash de M t.q: $H(M)^d \equiv S \pmod n$.

Llavors s'envia $M, H(M), S$ i el receptor fa $S^e \equiv H(M) \pmod n$ i després $H(M)'$. Si $H(M)' = H(M)$ sig. que no ha estat alterat.

M que ha rebut → Hash generat pel receptor ← Original enviat pel emissor.

Si M modificat, el hash no coincidex.

#) $3 \mid x \Leftrightarrow 3 \mid$ suma_dig_x

Abans de començar hem de def que serà "x": $x := C_0 \cdot 10^0 + C_1 \cdot 10^1 + \ldots + C_n \cdot 10^n$.

$\Rightarrow$ Suposem: $3 \mid x$ Volem Demo: $3 \mid$ sum_dig_x.

Per simplificar direm que $S =$ suma_dig_x i $S = C_0 + C_1 + \ldots + C_n$.

Partim de que $3 \mid x \overset{\text{def.}}{\Leftrightarrow} x \equiv 0 \pmod 3 \overset{\text{def.}}{\Leftrightarrow} (C_0 \cdot 10^0 + C_1 \cdot 10^1 + \ldots + C_n \cdot 10^n) \equiv 0 \pmod 3$

Abans de continuar hem de recordar que $10^k \equiv 1 \pmod 3$ i donat que

$\text{mcd}(10^k, 3) = 1 \overset{\text{Prop. III}}{\Rightarrow} C_i \cdot 10^k \equiv C_i \pmod 3$.

Donat que la congruència té la prop. II, podem reescriure t.q.:

$(C_0 \cdot 10^0) \equiv C_0 \pmod 3$, $(C_1 \cdot 10^1) \equiv C_1 \pmod 3$, ..., $(C_n \cdot 10^n) \equiv C_n \pmod 3$ i la suma d'aixà queda t.q. $(C_0 \cdot 10^0 + C_1 \cdot 10^1 + \ldots + C_n \cdot 10^n) \equiv (C_0 + C_1 + \ldots + C_n) \pmod 3$.

Com que suposàvem que $x \equiv 0 \pmod 3 \Rightarrow (C_0 + C_1 + \ldots + C_n) \equiv 0 \pmod 3$ ✓.

$\Leftarrow$ Suposem: $3 \mid S$ Volem Demo: $3 \mid x$.

Partim que $(C_0 + C_1 + \ldots + C_n) \equiv 0 \pmod 3$.

Tornem a recordar que $C_i \cdot 10^i \equiv C_i \pmod 3 \Rightarrow$

$$\begin{cases} C_0 \pmod 3 \equiv C_0 \cdot 1 \equiv C_0 \cdot 10^0 \\ C_1 \pmod 3 \equiv C_1 \cdot 1 \equiv C_1 \cdot 10^1 \\ \vdots \\ C_n \pmod 3 \equiv C_n \cdot 1 \equiv C_n \cdot 10^n \end{cases}$$

$C_0 + \ldots + C_n \equiv 0 \pmod 3$

Això sig que la suma t.q. $(C_0 \cdot 10^0 + C_1 \cdot 10^1 + \ldots + C_n \cdot 10^n) \equiv (C_0 + C_1 + \ldots + C_n) \pmod 3$

Llavors pel que suposem podem dir que $(C_0 \cdot 10^0 + C_1 \cdot 10^1 + \ldots + C_n \cdot 10^n) \equiv 0 \pmod 3$

i per la def de $x \Rightarrow x \equiv 0 \pmod 3$ ✓.

Queda demo que $3 \mid x \Leftrightarrow 3 \mid$ suma_digits_x ☺.

③. Sigui p primer. Demo:

a) Si $a^2 \equiv b^2 \pmod p \Rightarrow a \equiv b \pmod p$

$a^2 \equiv b^2 \pmod p \overset{\text{def.}}{\Leftrightarrow} p \mid (a^2 - b^2) \overset{\text{Id. Not.}}{\Rightarrow} p \mid (a-b)(a+b) \overset{\text{Lema Euclides}}{\Rightarrow} p \mid (a-b) \overset{\text{def}}{\Leftrightarrow} a \equiv b \pmod p$ ✓

$\Rightarrow p \mid a+b) \Leftrightarrow a \equiv -b \pmod p$ ✓.

b) Dedueix que la sol. de $x^2 \equiv 1 \pmod p$ són $x \equiv \pm 1 \pmod p$

$x^2 \equiv 1 \pmod p \Leftrightarrow x^2 \equiv 1^2 \pmod p \overset{\text{(vist en a).}}{\Rightarrow} x \equiv \pm 1 \pmod p$ ✓.

c) Es cert b) si p no és primer?

$3^2 \equiv 1^2 \pmod 8$

$3 \not\equiv 1 \pmod 8$.

No pq $x = 3$ i $m = 8$ no complex

FM-6-E-1

(15). b) Demo que n és múltiple de 9 $\Leftrightarrow$ suma dígits de n múltiple de 9.

$n = \underline{a_0}\,\underline{a_1}\ldots\underline{a_{k-1}}$ # on a_i és refereix al dígit. $n := a_0\cdot 10^0 + a_1\cdot 10^1 + \ldots + a_{k-1}\cdot 10^{k-1}$

Hem de demo que: $a_0\cdot 10^0 + a_1\cdot 10^1 + \ldots + a_{k-1}\cdot 10^{k-1} \equiv 0 \pmod 9 \Leftrightarrow a_0 + a_1 + \ldots + a_{k-1} \equiv 0 \pmod 9$

Per a fer-ho, estudiem com són les potències de 10 mod 9.

$10^1 \equiv 1 \pmod 9$; $10^2 = 10\cdot 10 \equiv 1\cdot 1 = 1 \pmod 9$, $10^3 = 10^2\cdot 10 \equiv 1^2\cdot 1 = 1 \pmod 9$, $\ldots$ $10^{k-1} \equiv 1 \pmod 9$

Llavors $10^{k-1} \equiv 1 \pmod 9 \Rightarrow a_i\cdot 10^{k-1} \equiv a_i \pmod 9$.

Es per això que $a_1 + a_2 + \ldots + a_{k-1} \equiv 0 \pmod 9 \Leftrightarrow a_0\cdot 10^0 + a_1\cdot 10^1 + \ldots + a_{k-1}\cdot 10^{k-1} \equiv 0 \pmod 9$.

(17). Demo que no hi ha cap enter n t.q. $6n+5$ sigui un quadrat.

Farem demo per R.A: Suposem que $\exists\, n_0$ t.q. $6n_0 + 5 = k^2$ $(k \in \mathbb{Z}) \rightarrow \lightning$

Si $6n_0 + 5 = k^2$ (*) $\Rightarrow 6n_0 + 5 \equiv k^2 \pmod 6$ (**) $\Rightarrow k^2 \equiv 5 \pmod 6$.

Llavors podem veure que $0^2 \not\equiv 5$, $1^2 \not\equiv 5$, $2^2 \not\equiv 5$, $3^2 \not\equiv 5$, $4^2 \not\equiv 5$, $5^2 \not\equiv 5$ llavors és contradictori.

Donat que féiem R.A. Demostrat això que no hi ha cap n. Ü.

(*) $\square \equiv \square \pmod m \Leftrightarrow m \mid 0$ donat que diem que ens el mateix.

(**) Escollim (mod 6) per $6n_0 \pmod 6$ és 0 i llavors ens simplifica molt.

(19). Demo que $\forall n \geq 0$ $2\cdot(6^{n+1})^2 + 12\cdot(2^{n+1})^3$ és múltiple de 168.

Hem de veure que: $2(6^{n+1})^2 + 12\cdot(2^{n+1})^3 \equiv 0 \pmod{168}$

Hem de veure que: $(6^{n+1})^2 + 6\cdot(2^{n+1})^3 \equiv 0 \pmod{84}$ $\}\cdot 2$ # $84 = 2^2\cdot 3\cdot 7$

Veurem: I. $(6^{n+1})^2 + 6\cdot(2^{n+1})^3 \equiv 0 \pmod 4$

II. $(6^{n+1})^2 + 6\cdot(2^{n+1})^3 \equiv 0 \pmod 3 \Rightarrow 6 \pmod 3 = 0$

III. $(6^{n+1})^2 + 6\cdot(2^{n+1})^3 \equiv 0 \pmod 7$

2) Veiem que ja és cert donat que $6 \equiv 0 \pmod 3$ llavors això. $\forall n$).

1) $(6^{n+1})^2 + 6\cdot(2^{n+1})^3 \equiv (2^{n+1})^2 + 2\cdot(2^{n+1})^3 \equiv 2^{2n+2} + 2\cdot(2^{3n+3}) \equiv 2^{2n+2} + 2^{3n+4} \equiv$

$\equiv 2^2\cdot 2^{2n} + 2^4\cdot 2^{3n} \equiv 2^2\cdot 2^{2n} + 2^2\cdot 2^2\cdot 2^{3n} \equiv 0\cdot 2^{2n} + 0\cdot 0\cdot 2^{3n} \equiv 0 \pmod 4$

3) $(6^{n+1})^2 + 6\cdot(2^{n+1})^3 \overset{6=-1}{\equiv} ((-1)^{n+1})^2 + (-1)(2^{n+1})^3 \equiv (-1)^{2n+2} - (1)(2^{3n+3}) \equiv$

$[2n+2$ és parell i $(-1)^{\text{parell}} = 1] \equiv (1) - 2^{3n}\cdot 2^3 \equiv 1 - (2^3)^n \cdot 2^3 \equiv 1 - (8)^n \cdot 8 \overset{\bar{8}=\bar{1}}{\equiv} 1 - 1^n \cdot 1 \overset{1^n=1}{\equiv} 0 \pmod 7$

② Demo. $ax \equiv b \pmod m$ té sol. $\Leftrightarrow \text{mcd}(a,m) \mid b$.

$ax \equiv b \pmod m \Leftrightarrow m \mid ax - b \Leftrightarrow ax - b = mk$ per $k \in \mathbb{Z} \Leftrightarrow ax - mk = b$ i això és el mateix que una eq. diofàntica i aquestes només es poden resoldre si $\text{mcm}(a,m) \mid b$.

① Demo: $\forall n \geq 0$ $2^4 \cdot 7^{n+1} + (6\cdot 9^n)^2$ múltiple de 148 fent ús de inducció i congruències.

Cas Base; $n=0$: $2^4 \cdot 7^{0+1} + (6\cdot 9^0)^2 = 2^4 \cdot 7 + (6)^2 = 16\cdot 7 + 36 = 148$.

Pas Inductiu: Suposem que complex per $n-1 \geq 0$ t.q: $2^4 \cdot 7^{n-1+1} + (6\cdot 9^{n-1})^2 \equiv 0 \pmod{148}$

Volem veure que complex per $n > 0$ t.q: $2^4 \cdot 7^{n+1} + (6\cdot 9^n)^2 \equiv 0 \pmod{148}$

Partim veient que $\overbrace{2^4 \cdot 7^n + (6\cdot 9^{n-1})^2 \equiv 0 \pmod{148}}^{\text{H.I.}} \Leftrightarrow 2^4 \cdot 7^n \equiv -(6\cdot 9^{n-1})^2 \pmod{148}$

Considerem: $2^4 \cdot 7^{n+1} + (6\cdot 9^n)^2 = 7(2^4 + 7^n) + (6\cdot 9^n)^2 \overset{\text{H.I.}}{\equiv} 7\left((-6\cdot 9^{n-1})^2\right) + (6\cdot 9^n)^2 \equiv$

$\equiv 7(-6\cdot 9^{2n-2}) + (6^2 \cdot 9^{2n}) \equiv$

$\equiv 9^2(-7\cdot 6\cdot 9^{n-1}) + (6^2 \cdot 9^{2n}) \equiv$

⑪ No hi ha cap $n \in \mathbb{Z}$: $7n+2$ sigui cub. # $7n+2$ diff de n^3.

$m^2 \not\equiv 2 \pmod 7$. Donat que busquem $7n+2 \neq m^3$ $\forall n, m \in \mathbb{Z}$.

$7n \equiv 0 \pmod 7$

$2 \equiv 2 \pmod 7$

$7n+2 \equiv 2 \pmod 7$

$\Downarrow$

$m^3 \equiv 2 \pmod 7$

$0^3 = 0 \equiv 0 \pmod 7$ i $\bar{0} \neq \bar{2}$

$1^3 = 1 \equiv 1 \pmod 7$ i $\bar{1} \neq \bar{2}$

$2^3 = 8 \equiv 1 \pmod 7$ i $\bar{1} \neq \bar{2}$

$3^3 = (3\cdot 3)\cdot 3 = 9\cdot 3$ $[\bar{9} = \bar{2}$ i $\bar{3} = \bar{3}] \to 3^3 \equiv \bar{2}\cdot\bar{3} \equiv \bar{6} \pmod 7$ i $\bar{6} \neq \bar{2}$

$4^3 = (4\cdot 4)\cdot 4 = 16\cdot 4$ $[\bar{16} = \bar{2}$ i $\bar{4} = \bar{4}] \to 4^3 \equiv \bar{2}\cdot\bar{4} \equiv \bar{8} \equiv \bar{1} \pmod 7$ i $\bar{1} \neq \bar{2}$

$5^3 = (5\cdot 5)5 = 25\cdot 5$ $[\bar{25} = \bar{4}$ i $\bar{5} = \bar{5}] \to 5^3 \equiv \bar{4}\cdot\bar{5} \equiv \bar{20} \equiv \bar{6} \pmod 7$ i $\bar{6} \neq \bar{2}$

$6^3 = (6\cdot 6)\cdot 6 = 36\cdot 6 = [\bar{1}\cdot 6] \to 6^3 \equiv 6 \pmod 7$ i $\bar{6} \neq 2$

~~$7^3 = 0 \equiv 0 \pmod 7$ i $\bar{0}$~~

(13). Valor de z pq. $9z86$ en dividir-lo entre 11 tingui resta 5.

$9z86 = 9\cdot1000 + z\cdot100 + 8\cdot10 + 6$; $10 \equiv -1 \pmod{11}$ (1000 | 11, 1000 = 11·90)

$100 \equiv 1 \pmod{11}$ #Regla de divisibilitat.

$1000 \equiv 10 \equiv -1 \pmod{11}$ del núm. 11.

$9\cdot(-1) + z(1) + 8(-1) + 6 \equiv 5 \pmod{11}$

$-9 + z - 8 + 6 \equiv 5 \pmod{11}$

$z + (-11) \equiv 5 \pmod{11}$ (-11 ↦ 0)

(*) $\begin{cases} z \equiv 5 \pmod{11} \\ -11 \equiv 0 \pmod{11} \end{cases} \Rightarrow [-11 \equiv 0 \pmod{11} \text{ no importa}] \Rightarrow z \equiv 5 \pmod{11}$ pq. $x+0=x$

(*) $\Rightarrow z \equiv 5 \pmod{11} \Rightarrow \boxed{z=5}$ # Pq. el més petit z pq sigui $z \equiv 5 \pmod{11}$ és el mateix 5

$5 \equiv 5 \pmod{11}$

(28). Resol: $\overline{5x} - \bar{3} = \overline{29}$ a $\mathbb{Z}_{13}$

$\overline{5x} - \bar{3} = \overline{29} \pmod{13} \Rightarrow \overline{5x} = \overline{29} + \bar{3} \pmod{13} \Rightarrow \overline{5x} = \overline{32} \pmod{13} \Rightarrow$ (32 | 13, 32 = 2·13 + 6)

$\Rightarrow 5x \equiv 6 \pmod{13}$ ▽IMPO: $\overline{5x} = \bar{6} \pmod{13} \Leftrightarrow \overline{5x} \equiv 6 \pmod{13}$

PERÒ NO FER LES DUES.

#Aquí fem eq. dio f.

$5x \equiv 6 \pmod{13} \Leftrightarrow 13 \mid 5x-6 \Leftrightarrow \exists k \in \mathbb{Z} : 5x-6 = 13k \Leftrightarrow \exists k \in \mathbb{Z} : 5x - 13k = 6$

Aquí podem veure que $\text{mcd}(5,-13) = \text{mcd}(5,13) = 1 \mid 6$ llavors té sol.

Y	1	0	1	-1	2
X	0	1	-2	3	-5
Q	-	2	1	1	-
R	13	5	3	2	1

mcd

$x' = -5$, $y' = -2$ ⇒ $5(-5) - 13(-2) = 1$

$5(-5\cdot6) - 13(-2\cdot6) = 1(6)$

$5(\underbrace{-30}_{x_0}) - 13(\underbrace{-12}_{y_0}) = 6$

(32). $\begin{cases} \bar{3}\bar{x} + \bar{5}\bar{y} = \bar{4} \\ \bar{4}\bar{x} - \bar{2}\bar{y} = \bar{2} \end{cases}$ $\mathbb{Z}_{11}$ (11 primer) . #Resolem amb Cramer

$\bar{4}\cdot\bar{3} = \overline{12} = \bar{1} \pmod{11}$

$x = \dfrac{\begin{vmatrix} \bar{4} & \bar{5} \\ \bar{2} & -\bar{2} \end{vmatrix}}{\begin{vmatrix} \bar{3} & \bar{5} \\ \bar{4} & -\bar{2} \end{vmatrix}} = \dfrac{(-\bar{2}\cdot\bar{4}) - (\bar{2}\cdot\bar{5})}{(\bar{3}\cdot(-\bar{2})) - (\bar{4}\cdot\bar{5})} = \dfrac{-\overline{18}}{-\overline{26}} = \dfrac{\overline{7}}{\bar{4}}$ (estem en $\mathbb{Z}_{11}$) $= \bar{4}^{-1}\cdot\bar{7} = \bar{3}\cdot\bar{7} = \overline{21} = \overline{10} = x$

$y = \dfrac{\begin{vmatrix} \bar{3} & \bar{4} \\ \bar{4} & \bar{2} \end{vmatrix}}{\bar{4}} = \dfrac{\bar{6} - \overline{16}}{-4} = \dfrac{-\overline{10}}{-4} = \bar{4}^{-1}\cdot\overline{10} = \bar{3}\cdot\overline{10} = \overline{30} = \overline{8} = y$

▽ Això en pot resultar així pq estem en $\mathbb{Z}_p$ on $p = 11$ i sí que hi he inves per a taba. les classes $\bar{0}, \bar{1}, \ldots, \overline{10}$?.

(34). Resol aquestes congruències.

a) $22x \equiv 9 \pmod{15} \iff \overline{22}\,\overline{x} = \overline{9} \pmod{15}$

Primer simplifiquem el 22 pq actuen en $\mathbb{Z}_{15}$.

$\overline{7}\,\overline{x} = \overline{9} \pmod{15}$ # Aquí volem multiplicar per l'invers de $\overline{7}$ per tindre $\overline{x}$.

Sabem que $\overline{7}$ té invers pq $\text{mcd}(7,15) = 1$. però a simple vista no veiem $\overline{1}$.

Però $\overline{2}\cdot\overline{7} = \overline{14} = \overline{-1} \Rightarrow -\overline{2}\cdot\overline{7} = \overline{1} \Rightarrow \underline{-\overline{2} = \overline{7}^{-1}}$, # Però $-\overline{2}$ "en fea" ràpid que $-\overline{2} = \overline{13}$ fent que $\overline{7}^{-1} = \overline{13}$. Llavors comencem:

$\overline{13}\cdot\overline{7}\overline{x} = \overline{13}\cdot\overline{9} \pmod{15} \Rightarrow \overline{91x} = \overline{117} \pmod{15} \Rightarrow \overline{1}\cdot\overline{x} = \overline{12} \pmod{15} \Rightarrow \overline{x} = \overline{12} \pmod{15}$

b) $21x \equiv 9 \pmod{15}$

Començem simplificant: $21x \equiv 9 \pmod{15} \Rightarrow 6x \equiv 9 \pmod{15}$ i $\overbrace{\text{mcd}(6,15)}^{3} \mid 9$

Llavors sí que hi ha solució. Així que simplifiquem ja que podem fer-ho.

$6x \equiv 9 \pmod{15}$ és igual a $3\cdot 2x \equiv 3\cdot 3 \pmod{3\cdot 5} \Rightarrow 2x \equiv 3 \pmod 5$

Ara $\text{mcd}(2,5) = 1$ llavors 2 sí que té invers en $\mathbb{Z}_5$. Allà podem veure que $\overline{2}^{-1} = \overline{3}$ en $\mathbb{Z}_5$, però ensmet parla de $\mathbb{Z}_{15}$ no $\mathbb{Z}_5$

$3\cdot 2x \equiv 3\cdot 3 \pmod 5 \Rightarrow 6x \equiv 9 \pmod 5 \Rightarrow \underline{x \equiv 4 \pmod 5}$

$x \equiv 9 \pmod 5$

$x \equiv 14 \pmod 5$

Llavors diem que $6x \equiv 9 \pmod{15} \Rightarrow \boxed{x \equiv 4, 9, 14 \pmod{15}}$

c) $21x \equiv 10 \pmod 9$

$21x \equiv 10 \pmod 9 \Rightarrow 3x \equiv 1 \pmod 9$ aquesta congruència no té una única sol. donat que $\text{mcd}(3,9) = 3 \neq 1$. Però en aquest cas $\underbrace{\text{mcd}(3,9)}_{3} \nmid 1$.

L'eq no té sol.

(45). $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 5 \pmod 6 \\ x \equiv 7 \pmod{10} \end{cases}$. Resol.

Primer agafem les dues primeres i després ja fem amb la tercera.

$x \equiv 1 \pmod 4$, $x \equiv 5 \pmod 6$ $\Rightarrow$ $x = 1 + 4k$, $x = 5 + 6l$ $\Rightarrow$ $1+4k = 5+6l$

$4k - 6l = 4$ [eq. dióf]

$2k - 3l = 2$ [simplifiquem]

$2k - 3l = 1 \Rightarrow 2(-1) - 3(-1) = 1$) ·2 Llavors tenim la sol. particular

$2\cdot(\underset{k_0}{-2}) - 3(\underset{l_0}{-2}) = 2$ t.q. $k_0 = -2$, $l_0 = -2$.

* Aquí pots ficar $+b, -a$ o $-b, +a$.

Ara busquem la sol. general $\begin{cases} k = -2 + 3t \\ l = -2 + 2t \end{cases}$ on $t \in \mathbb{Z}$ | així no et queda -12 després

Llavors ara resolem el sistema d'eq. $x = 1 + 4k = 1 + 4(-2-3t) = 1 + (-8) - 12t$

$x = -7 + 12t \Rightarrow$ $\boxed{x \equiv -7 \pmod{12}}$

Aquest $x \equiv -7 \pmod{12}$ és equivalent a $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 5 \pmod 6 \end{cases}$

Ara fem el sistema amb l'eq. que ens queda t.q. $\begin{cases} x \equiv -7 \pmod{12} \\ x \equiv 7 \pmod{10} \end{cases}$

Llavors fem el mateix procediment que l'anterior.

$x \equiv 77 \pmod{60} \Rightarrow$ $\boxed{x \equiv 17 \pmod{60}}$ # $60 = \text{mcm}(4,6,10)$

(53). b) Calculem $34773^{4969} \bmod 151$.

Primer que ens hem de fixar si 151 és primer. Mirem si $x \mid 151$ on $x \leq \sqrt{151} \simeq 12$'..

$x = \{2, 3, 5, 7, 11\}$; 2 no, 3 no, 5 no, 151 | 7 → 21 no, 11 no ($1-5+1=-3$; $11 \nmid -3$) llavors 151 és primer.

Primer reduïm $34773 \Rightarrow$ 34773 : 151 = 23, residu 43 $\Rightarrow 34773^{4969} \equiv 43^{4969} \pmod{151}$.

El teorema petit de Fermat diu que $43^{151-1} \equiv 1 \pmod{151} \Rightarrow 43^{150} \equiv 1 \pmod{151}$.

4969 : 150 = 33, residu 19. $4969 = 150\cdot 33 + 19$. Llavors $43^{4969} = (43^{150})^{33}\cdot 43^{19} \equiv 1^{33}\cdot 43^{19} \equiv 43^{19} \pmod{151}$

$43^{19} \equiv 43\cdot(43\cdot 43)^9 \equiv 43\cdot(1849)^9 \equiv 43\cdot 37^9 \equiv 43\cdot 37(37\cdot 37)^4 \equiv 43\cdot 37(1369)^4 \equiv$

$\equiv 43\cdot 37\cdot 10^4 \equiv 43\cdot 37\cdot 10000 \equiv 1591\cdot 10000 \equiv 80\cdot 10000 \equiv 80\cdot 34 \equiv 2720 \equiv 2 \pmod{151}$

$$\boxed{34773^{4969} \equiv 2 \pmod{151}}$$

(50). Calculem: $44^{444} \pmod{13}$

$44 \mid 13$ / 39 / 5 ; $44^{444} \equiv 5^{444} \pmod{13}$; Ara volem aplicar PTF per a poder treballar millor. Ho podem fer pq 13 és primer i $5 \not\equiv 0 \pmod{13}$.

$\boxed{a^{p-1} \equiv 1 \pmod{p}}$

$444 \mid 12$ / 0 / 37

$5^{444} \equiv (5^{12})^{37} \equiv (1)^{37} \equiv 1 \pmod{13}$. $\boxed{44^{444} \equiv 1 \pmod{13}}$

$a \equiv b \pmod{\operatorname{mcm}(m_1, \dots, m_n)} \Leftrightarrow a \equiv b \pmod{m_1}, \dots, a \equiv b \pmod{m_n}$

(52). Calculem fent Fermat i prop IV de congruències.

a) $11^{1234} \pmod{14}$ ∇ 14 no és primer així que no podrien fer Fermat. $\#14 = 2 \cdot 7$

$11^{1234} \pmod 2$ } Veiem que podem simplificar així que fem:

$11^{1234} \pmod 7$ }

$11^{1234} \equiv 1^{1234} \equiv 1 \pmod 2 \Rightarrow \underline{x \equiv 1 \pmod 2}$ $\qquad \underline{x \equiv 4 \pmod 7}$

$1234 \mid 6$ / 034 / 205 ; $11^{1234} \equiv 4^{1234} \equiv (4^6)^{205} \cdot 4^4 \equiv 1^{205} \cdot 4^2 \cdot 4^2 \equiv 2 \cdot 2 \equiv 4 \pmod 7$

$k, m \in \mathbb{Z}$

$x \equiv 1 \pmod 2 \Rightarrow x = 2k+1$

$x \equiv 4 \pmod 7 \Rightarrow x = 7m+4$

$\Rightarrow 2k+1 = 7m+4$, $\underline{7m - 2k = -3}$ ← Dioph. Eq.

Aquí podem veure que $7(1) - 2(3) = 1$) $\cdot -3$ # Fem anàlisis "by inspection"

No importa com, però han de ser contraris. $7(-3) - 2(-9) = -3$ → Que això és el que buscàvem resoldre.

$m_0 = -3$; $m = -3 - (-2)t$; $t \in \mathbb{Z}$ $\Rightarrow m = -3 + 2t$ Però això no és el que busquem,

$k_0 = -9$; $k = -9 + (7)t$ $\Rightarrow k = -9 + 7t$ hem de resoldre x així que agafem nosaltres.

$x = 2k+1 = 2(-9+7t)+1 = -17 + 14t$. Per comoditat, vull que x sigui positiu.

Si $t = 2 \Rightarrow x = 11$. Llavors podem dir que $\boxed{11^{1234} \equiv 11 \pmod{14}}$

— — — Segona manera de resoldre el sistema xino.

$\boxed{M_i x_i \equiv 1 \pmod{m_i}}$

$\boxed{x = \sum_{i=1}^{\infty} a_i \cdot M_i \cdot x_i}$

$x \equiv 1 \pmod 2$

$x \equiv 4 \pmod 7$

• $\underline{a_1 = 1}$; $\underline{M_1 = (2 \cdot 7) \div 2 = 7}$; $m_1 = 2$

$7x_1 \equiv 1 \pmod 2 \Rightarrow x_1 \equiv 1 \pmod 2 \Rightarrow \underline{x_1 = 1}$

• $\underline{a_2 = 4}$; $\underline{M_2 = (2 \cdot 7) \div 7 = 2}$; $m_2 = 7$

$2x_2 \equiv 1 \pmod 7 \Rightarrow \underline{x_2 = 4}$

$39 \mid 14$ / 28 / 2 / 11

$x = a_1 \cdot M_1 \cdot x_1 + a_2 M_2 x_2 = 1 \cdot 7 \cdot 1 + 4 \cdot 2 \cdot 4 = 7 + 32 = 39$

$x \equiv 23 \equiv 11 \pmod{14}$ Llavors $\boxed{11^{1234} \equiv 11 \pmod{14}}$

b) $7^{1234} \pmod{165}$ $\quad 165 = 3 \cdot 5 \cdot 11$

$$\left.\begin{array}{l} x \equiv 7^{1234} \pmod 3 \\ x \equiv 7^{1234} \pmod 5 \\ x \equiv 7^{1234} \pmod{11} \end{array}\right\}$$

Són equiv.

$x \equiv 7^{1234} \equiv 1^{1234} \equiv 1 \pmod 3 \Rightarrow \underline{x \equiv 1 \pmod 3}$

$x \equiv 7^{1234} \equiv 2^{1234} \equiv \left[\begin{array}{c|c} 1234 & 24 \\ 034 & 50 \\ 2 & \end{array}\right] \equiv (2^4)^{308} \cdot 2^2 \equiv 1^{308} \cdot 2^2 \equiv 4 \pmod 5$

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

$x \equiv 7^{1234} \equiv \left[\begin{array}{c|c} 1234 & 10 \\ 4 & 123 \end{array}\right] \equiv (7^{10})^{123} \cdot 7^4 \equiv 1^{123} \cdot 7^2 \cdot 7^2 \equiv 7^2 \cdot 7^2 \equiv \left[\begin{array}{c|c} 49 & 11 \\ 3 & 4 \end{array}\right] \equiv 5 \cdot 5 \equiv$

$\equiv 25 \equiv \left[\begin{array}{c|c} 25 & 11 \\ 3 & 2 \end{array}\right] \equiv 3 \pmod{11} \Rightarrow \underline{x \equiv 3 \pmod{11}}$

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

- $\boxed{a_1 = 1}$; $\boxed{M_1 = 55}$; $m_1 = 3$

$55 x_1 \equiv 1 \pmod 3$ $\quad \left[\begin{array}{c|c} 55 & 3 \\ 25 & 18 \\ 1 & \end{array}\right]$

$1 x_1 \equiv 1 \pmod 3$

$\boxed{x_1 = 1}$

- $\boxed{a_2 = 4}$; $\boxed{M_2 = 33}$; $m_2 = 5$

$33 x_2 \equiv 1 \pmod 5$ $\quad \left[\begin{array}{c|c} 33 & 5 \\ 3 & 6 \end{array}\right]$

$3 x_2 \equiv 1 \pmod 5$

$\boxed{x_2 = 2}$

- $\boxed{a_3 = 3}$; $\boxed{M_3 = 15}$; $m_3 = 11$

$15 x_3 \equiv 1 \pmod{11}$

$4 x_3 \equiv 1 \pmod{11}$

$\boxed{x_3 = 3}$

$x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3$

$x = 1 \cdot 55 \cdot 1 + 4 \cdot 33 \cdot 2 + 3 \cdot 15 \cdot 3$

$x = 55 + 264 + 135$

$x = 454 \Rightarrow \left[\begin{array}{c|c} 454 & 165 \\ 330 & 2 \\ 124 & \end{array}\right] \Rightarrow \boxed{x = 124}$

$\boxed{7^{1234} \equiv 124 \pmod{165}}$

(51). Demo $\forall a$, $\bar{a}^5 = \bar{a}$ en $\mathbb{Z}_{15}$. (Ús Fermat i prop IV)

$\bar{a}^5 = \bar{a} \pmod{15}$ és el mateix que dir $a^5 \equiv 5 \pmod{15}$.

Això es pot simplificar una mica i podem dir que:

$a^5 \equiv a \pmod{15} \Leftrightarrow a^5 \equiv a \pmod 3$, $a^5 \equiv a \pmod 5$.

Cas 1; $\bar{a} = \bar{0}$; Si això és així, ja ho tenim tot. $0 \equiv 0 \pmod{15}$ ☑.

Cas 2: $\bar{a} \neq \bar{0}$;

Apliquem PTF Tq $a^5 \equiv (a^2)^2 \cdot a \equiv (1)^2 \cdot a \equiv a \pmod 3 \Rightarrow \underline{a^5 \equiv a \pmod 3}$

Apliquem PTF Tq $a^5 \equiv (a^4)^1 \cdot a \equiv (1)^1 \cdot a \equiv a \pmod 5 \Rightarrow \underline{a^5 \equiv a \pmod 5}$

Per la prop IV de congruència podem dir que:

$a^5 \equiv a \pmod 3$, $a^5 \equiv a \pmod 5 \Rightarrow a^5 \equiv a \pmod{15}$ $\quad \#15 = mcm(3,5)$

Això és el que buscàvem així que queda demostrat l'enunciat. ☺