• Exo 7 (Suite)

2) $x^2 - 5x + 2 \equiv 0 \pmod 7$.

$\Leftrightarrow x^2 + 2x + 2 \equiv 0 [7]$. à vérifier.

L'ensemble des solutions est $\{\varnothing\}$.

3) $2x^2 + 4x + 1 \equiv 0 \pmod 7$.

$S = \{\bar{1}, \bar{4}\}$

4) $(x^2 - 1)^2 \equiv 9 \pmod{11}$

$(x^2 - 1)^2 - 9 \equiv 0 \pmod{11}$

$(x^2 - 4)(x^2 + 2) \equiv 0 \pmod{11}$

• Exo 8 (thm chinois)

- Problème chinois :

x : nb d'objet. $x = 23$. ou $x = 128$

$x \equiv 2 \pmod 3$ ~~$x = 128$~~

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

• Thm chinois :

Soient $a, b \in \mathbb{Z}$ tq $\text{pgcd}(a,b) = 1$.

$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Soient $\bar{x} \in \mathbb{Z}/a\mathbb{Z}$ et $\bar{y} \in \mathbb{Z}/b\mathbb{Z}$

Comment trouver $z \in \mathbb{Z}$ tq $\begin{cases} z \equiv x \pmod a \\ z \equiv y \pmod b \end{cases}$ et

$\exists u, v \in \mathbb{Z}$ tq : $au + bv = 1$.

$\Rightarrow \begin{cases} au \equiv 1 \bmod b \\ bv \equiv 1 \bmod a \end{cases}$ Prenons $z = bvx + auy$

$\begin{cases} z \equiv bvx \pmod a \\ z \equiv auy \pmod b \end{cases}$

or $\begin{cases} bv \equiv 1 [a] \Rightarrow bvx \equiv x \pmod a \\ au \equiv 1 [b] \Rightarrow auy \equiv y \pmod b \end{cases} \Rightarrow \begin{cases} z \equiv x [a] \\ z \equiv y [b] \end{cases}$ et

23 est solution et $\forall x \in \mathbb{N}$ tq $x \equiv 23\ [105]$
on a x solution aussi ie.
$\forall k \in \mathbb{N}$, $23 + 105k$ est solution.

$\mathbb{Z}/105\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$
$23 \longrightarrow (2, 3, 2)$

On utilise le thm des restes chinois
si $a_1, \dots, a_r \in \mathbb{Z}$ premiers entre eux
$\mathbb{Z}/a_1 \dots a_r\mathbb{Z} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_r\mathbb{Z}$.

Theorème d'Euler - Fermat.

• Exo 1 :

a) $a = 2001^{1613}$, $b = 143$. $12^2 = 144$ $143 = 11 \times 13$.
143 n'est pas un nb premier.

Petit Thm de Fermat.
Soit p un nb premier. $n \in \mathbb{N}$.
$n^p \equiv n \pmod p$. $n^p \equiv n\ [p]$.
$\varphi(n)$: ens des entiers premiers avec n entre $[\![0, n]\!]$.
$a^{\varphi(n)} \equiv 1\ [n]$.
on suppose $n \wedge p = 1$, $n^{p-1} \equiv 1\ [p]$. $\Rightarrow n^{\varphi(p)} \equiv 1\ [p]$.
$\varphi(p) = p - 1$. si p est premier.
Thm d'Euler : Generalisation du thm de Fermat.
Soit $a \in \mathbb{Z} - \{0\}$
$\forall n \in \mathbb{Z}$, $n^{\varphi(a)+1} \equiv n\ [a]$.
$a \pmod b = R$. $|R| < b$.
$2001 = (143 \times 13) + 142$
ou encore $2001 \equiv -1\ [143]$.
$2001^{1613} \equiv (-1)^{1613}\ [143]$ $1613 = (2 \times 806) + 1$.

Donc $2001^{1613} \equiv ((-1)^2)^{806} \cdot (-1)\ [143] = -1\ [143]$.
$\Rightarrow 2001^{1613} \equiv 142\ [143]$ ie $2001^{1613} = 143k + 142$.

143
12 13 14
286 429 572
143 143 1902
1716 1859 2