CC "1S" Mat 301 Groupe MIN 2/S&D.

Ex. 1 On calcule :

$76 \equiv 1 \ (5)$.

$2^2 = 4 \equiv (-1) \ (5)$

donc $2^4 \equiv 1 \ (5)$

donc $2^{34} = 2^{4 \times 8} \times 2^2$

$\equiv 1 \times (-1) \ (5)$

$\equiv -1 \ (5)$

Au final, $2^{34} + 76 \equiv 1 - 1 \ (5)$

$\equiv 0 \ (5)$.

Le reste dans la division euclidienne par 5 est 0.

Ex. 2

$$
\begin{array}{r|l}
X^4 + X^3 + 0 + X + 1 & X^2 + X + 1 \\
\cline{2-2}
-(X^4 + X^3 + X^2) & X^2 - 1 \\
\cline{1-1}
-X^2 + X + 1 & \\
-(-X^2 - X - 1) & \\
\cline{1-1}
2X + 2 &
\end{array}
$$

On a ainsi :

$$X^4 + X^3 + X + 1 = (X^2 - 1)(X^2 + X + 1) + 2X + 2$$

En outre

$$X^2 + X + 1 = (X+1)(X) + 1.$$

donc le pgcd est 1 : ils sont premiers entre eux.

Ex. 3 On cherche à résoudre

$$\begin{cases} x \equiv \bar{5}\ [7] \\ x \equiv 3\ [13]. \end{cases}$$

$7 \wedge 13 = 1$ donc le théorème des restes chinois nous dit que l'ensemble des solutions est de la forme $x_0 + 91k$, où x_0 est une sol. particulière

identité de Bézout : $2 \times 7 - 13 = 1$ ou $14 - 13 = 1$.

on a donc $\begin{cases} 14 \equiv 0\ (7) \\ 14 \equiv 1\ (13) \end{cases}$ $\begin{cases} -13 \equiv 1\ [7] \\ -13 \equiv 0\ [7]. \end{cases}$

Une solution particulière est donc :

$$-13 \times 5 + 3 \times 14 = 42 - 65 = -23.$$

D'après le théorème des restes chinois, les autres solutions sont $-23 + k \times 7 \times 13$, $k \in \mathbb{Z}$.

$$S = \{68 + k\,91,\ k \in \mathbb{Z}\}.$$

vérification : $68 = 5 + 9 \times 7$ ← utile !

$68 = 3 + 5 \times 13$.

Ex. 4 Calculs :

1) $\bar{0}^3 = \bar{0}$, $\bar{1}^3 = \bar{1}$, $\bar{2}^3 = \bar{8} = \bar{1}$, $\bar{3}^3 = \overline{27} = -\bar{1}$, $\bar{4}^3 = (-\bar{3})^3 = \bar{1}$, $\bar{5}^3 = (-\bar{2})^3 = -\bar{1}$, $\bar{6}^3 = (-\bar{1})^3 = -\bar{1}$.

d'où la conclusion.

2) $x_1^3 + x_2^3 \in \{\bar{0}, \bar{1}, -\bar{1}, \bar{2}, -\bar{2}\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{5}, \bar{6}\} \not\ni \bar{4}$!

3) on a $\bar{x}^7 = 0\ (7)$ si $\bar{x} \equiv 0\ (7)$

si $\bar{x} \neq \bar{0}$, $\bar{x}^3 = \pm\bar{1}$ donc $\bar{x}^6 = \bar{1}$ donc $\bar{x}^7 = \bar{x} \cdot \bar{x}^6 = \bar{x}$.

On peut aussi faire appel au petit théorème de Fermat :

7 est premier donc $\mathbb{Z}/7\mathbb{Z}$ est un corps d'où $\forall x \in (\mathbb{Z}/7\mathbb{Z})^*$ $x^6 \equiv 1\ [7]$

... en regardant séparément $x = \bar{0}$, $x \neq \bar{0}$.