Corrigé de l'examen du 1 avril 2019

Ex 1 : On note $42 = 2 \cdot 3 \cdot 7$.

D'après le lemme de Gauss, il suffit de vérifier que $n^7 - n$ est divisible par 2, 3 et 7

- $n^7 - n$ divisible par 7 (thm. de Fermat)
- $n^7 - n$ divisible par 3 :

  thm. de Fermat : $n^3 \equiv n \ [3]$.

  $\Rightarrow n^7 \equiv n^5 \equiv n^3 \equiv n \ [3]$.

- $n^7 - n$ divisible par 2 :

  thm de Fermat : $n^2 \equiv n \ [2]$.

  $\Rightarrow n^7 \equiv n^6 \equiv \dots \equiv n^2 = n \ [2]$.

Ex 2 : 1.) $5x \equiv 2 \ [6] \iff x \equiv 4 \ [6]$.

$3x \equiv 1 \ [5] \iff x \equiv 2 \ [5]$.

$\text{pgcd}(5,6) = 1 \Rightarrow x \equiv 22 \ [30]$.

2.) $\left.\begin{array}{l} 2x \equiv 1 \ [3] \iff x \equiv 2 \ [3] \\ x \equiv 4 \ [6] \Rightarrow x \equiv 1 \ [3] \end{array}\right\} \Rightarrow$ pas de solution.

Ex 3 : 1.) non, car $\text{pgcd}(11,99) = 11 \neq 1$

2.) non, car $\text{pgcd}(12,99) = 3 \neq 1$

3.) oui, car $\text{pgcd}(13,99) = 1$.

L'algorithme d'Euclide étendu donne.

$$1 = (-38) \cdot 13 + 5 \cdot 99.$$

donc l'inverse de $\overline{13} = \overline{-38} = \overline{61}$ dans $\mathbb{Z}/99\mathbb{Z}$.

Ex 4 1) L'algorithme d'Euclide étendu donne (2

$$1 = 4 \cdot 19 - 3 \cdot 25$$

donc inverse de $\overline{19} = \overline{4}$ dans $\mathbb{Z}/25\mathbb{Z}$

2) Thm. d'Euler dans $\mathbb{Z}/25\mathbb{Z}$ appliqué à $\overline{19}$

(pgcd(19,25) = 1).

$$\overline{19}^{\varphi(25)} = \overline{1} \quad \text{dans } \mathbb{Z}/25\mathbb{Z}$$

or $\varphi(25) = 5^2 - 5 = 20$

donc $\overline{19}^{20} = \overline{1}$

et $\overline{19}^{20} = \overline{19}^{19} \cdot \overline{19} = \overline{1}$

en multipliant par l'inverse de $\overline{19}$ $(= \overline{4})$ on obtient $\overline{19}^{19} = \overline{4}$.

3) Théorème des restes chinois ; pgcd(4,25) = 1

$$\Phi : \mathbb{Z}/100\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}.$$

Il faut calculer

2019^{2019} mod 4 et mod 25.

$$2019^{2019} \equiv (-1)^{2019} \equiv -1 \quad [4]$$

$$2019^{2019} \equiv 19^{19} \equiv 4 \quad [25].$$

et 79 mod 100 est tel que $\Phi(79) = (-1, 4)$

Conclusion : Les deux derniers chiffres de 2019^{2019} sont 79.

Ex5 On a : $\overline{3}^2 = \overline{9}$, $\overline{3}^3 = \overline{27} = \overline{7}$ (3

$\overline{3}^4 = \overline{7} \cdot \overline{3} = \overline{21} = \overline{1}$

donc l'ordre de $\overline{3}$ est 4.