TD 13 - Vendredi 27 novembre 2020

ex 4.9.

$d = 5$

$\bar n \backslash \bar m$	$\bar 0$	$\boxed{\bar 1}$	$\boxed{\bar 2}$	$\boxed{\bar 3}$	$\boxed{\bar 4}$
$\bar 0$	$\bar 0$	$\bar 0$	$\bar 0$	$\bar 0$	$\bar 0$
$\boxed{\bar 1}$	$\bar 0$	$\boxed{\bar 1}$	$\bar 2$	$\bar 3$	$\bar 4$
$\boxed{\bar 2}$	$\bar 0$	$\bar 2$	$\bar 4$	$\boxed{\bar 1}$	$\bar 3$
$\boxed{\bar 3}$	$\bar 0$	$\bar 3$	$\boxed{\bar 1}$	$\bar 4$	$\bar 2$
$\boxed{\bar 4}$	$\bar 0$	$\bar 1$	$\bar 3$	$\bar 2$	$\boxed{\bar 1}$

(colonnes $\bar 1$ à $\bar 4$: y ; lignes $\bar 1$ à $\bar 4$: x)

dans $\mathbb{Z}/6\mathbb{Z}$

$\bar n \backslash \bar m$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$
$\bar 0$	$\bar 0$	$\bar 0$	$\bar 0$	$\bar 0$	$\bar 0$	$\bar 0$
$\bar 1$	$\bar 0$	$\bar 1$	$\bar 2$	$\bar 3$	$\bar 4$	$\bar 5$
$\bar 2$	$\bar 0$	$\bar 2$	$\bar 4$	$\bar 0$	$\bar 2$	$\bar 4$
$\bar 3$	$\bar 0$	$\bar 3$	$\bar 0$	$\bar 3$	$\bar 0$	$\bar 3$
$\bar 4$	$\bar 0$	$\bar 4$	$\bar 2$	$\bar 0$	$\bar 4$	$\bar 2$
$\bar 5$	$\bar 0$	$\bar 5$	$\bar 4$	$\bar 3$	$\bar 2$	$\bar 1$

(colonnes $\bar 1$ à $\bar 5$: y ; lignes $\bar 1$ à $\bar 5$: x)

← trouver un $\bar 0$.

2- $\forall x \in \mathbb{Z}/5\mathbb{Z}$, $x \neq \bar 0$, $\exists y \in \mathbb{Z}/5\mathbb{Z}$ tq $xy = \bar 1$.

$$x \cdot y = \bar 1$$
$$\bar 1 \cdot \bar 1 = \bar 1$$
$$\bar 2 \cdot \bar 3 = \bar 1$$
$$\bar 3 \cdot \bar 2 = \bar 1$$
$$\bar 4 \cdot \bar 4 = \bar 1$$

Dans l'exercice 4.11, on verra que $\mathbb{Z}/d\mathbb{Z}$ a la même propriété si d est un nombre premier :

si d premier, $\forall x \in \mathbb{Z}/d\mathbb{Z}$, $\exists y \in \mathbb{Z}/d\mathbb{Z}$ tq $xy = \bar 1$.
$x \neq \bar 0$

" tout élément non nul de $\mathbb{Z}/d\mathbb{Z}$ est inversible si d premier ".

3- $\exists x, y \in \mathbb{Z}/6\mathbb{Z}$, $x, y \neq \bar 0$ tq $xy = \bar 0$.

D'après le tableau, $\bar 2 \cdot \bar 3 = \bar 0$ et $\bar 2 \neq \bar 0$, $\bar 3 \neq \bar 0$

autre exemple : $\bar 3 \cdot \bar 4 = \bar 0$. $\bar 4 \neq \bar 0$.

On dit que " $\mathbb{Z}/6\mathbb{Z}$ est non intègre "

aussi, " $\bar{2}$ est un diviseur de $\bar{0}$ "

$\bar{3}$ "

$\bar{4}$ "

<u>ex 4.10</u> Soit $d \geq 2$ non premier.

Mq $\exists\, x, y \in \mathbb{Z}/d\mathbb{Z} \setminus \{\bar{0}\}$ tq $xy = \bar{0}$:

d non premier : $\exists\, a, b \in \mathbb{N}$, $a, b \neq 1$ et $d = ab$.

En particulier, $2 \leq a, b < d$. donc $\bar{a}, \bar{b} \neq \bar{0}$.

car, a, b non divisible par d.

En outre, $\bar{a}\bar{b} = \overline{ab} = \bar{d} = \bar{0}$.

On prend $x = \bar{a}$ et $y = \bar{b}$.

[$d = 6$: $x = \bar{2}$, $y = \bar{3}$]

" si d n'est pas premier, $\mathbb{Z}/d\mathbb{Z}$ n'est pas intègre ".

<u>ex 4.11</u> : cas où d est premier, $d = p$ $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \underbrace{\bar{1}, \dots, \overline{p-1}}_{\neq}\}$

1- $1 \leq a \leq p-1$, alors a est premier avec p.

[soit $\delta \in \mathbb{N}$. si δ / a et δ / p alors comme p premier, $\delta = 1$ ou p

et comme δ / a, $\delta \leq p-1$ donc $\boxed{\delta = 1}$ donc

$\mathrm{pgcd}(a, p) = 1$]

donc $\exists\, u, v \in \mathbb{Z}$ tq $au + pv = 1$

2- Soit $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$. $\exists\, 1 \leq a \leq p-1$ tq $x = \bar{a}$.

Par 1-, $\exists\, u, v \in \mathbb{Z}$ tq $1 = au + pv$. On réduit modulo p:

$\bar{1} = \bar{a}\bar{u} + \underbrace{\cancel{\bar{p}}}_{\bar{0}} . \bar{v}$

donc $\bar{1} = \bar{a}\bar{u}$.

On peut prendre $y = \bar{u}$.

" tout élt non nul ($\neq \bar{0}$) de $\mathbb{Z}/p\mathbb{Z}$ est inversible "

$\Leftrightarrow$ " $\mathbb{Z}/p\mathbb{Z}$ est un corps "

[comme $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$,

$\mathbb{Q}(x)$ = fractions rationnelles en une variable à coeffs rationnels.

$$\mathbb{Q}(x) = \left\{ \frac{P(x)}{Q(x)} : \begin{array}{l} P(x) \in \mathbb{Q}[x] \\ Q(x) \in \mathbb{Q}[x] \setminus \{0\} \\ \text{polynômes} \end{array} \right\} \ni x+1 \ni \frac{x+1}{x-1} \ni \frac{1}{x}$$

$\mathbb{Q}(x)$ est à $\mathbb{Q}[x]$ ce que $\mathbb{Q}$ est à $\mathbb{Z}$.

$$\mathbb{Q} = \left\{ \frac{p}{q} , p,q \in \mathbb{Z} \; q \neq 0 \right\}.$$

On peut aussi considérer $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{R}(x)$, $\mathbb{C}(x)$, $\mathbb{Z}/p\mathbb{Z}[x]$.

3- Par l'absurde, supposons qu'il existe $x, y \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ tq $xy = \bar{0}$.
Comme $x \neq \bar{0}$, $\exists z \in \mathbb{Z}/p\mathbb{Z}$ tq $zx = \bar{1}$ (par 2.). On obtient

$$\underbrace{zx}_{=\bar{1}}y = \bar{0} \quad \text{donc } y = \bar{0} \text{, ce qui est absurde.}$$

Donc on ne peut pas trouver de tels x, y.

<u>exercice 4.12</u> : <u>ex</u> : 12345678 est divisible par $\left\{ \begin{array}{l} 9 \\ 3 \end{array} \right.$ car
$1+2+3+4+5+6+7+8 = \frac{8(8+1)}{2} = 4 \cdot 9$ est divisible par 3, même par 9.

1- $n \in \mathbb{N}$, $n = [a_k \cdots a_1 a_0]$ écriture de n en base 10.

$$n = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots$$
$$= \sum_{k \geq 0} a_k \cdot 10^k .$$ [pour k grand, $a_k = 0$ donc cette somme est en fait finie].

2- a- Que vaut $\overline{10^i}$? $i \in \mathbb{N}$.
[$10 \equiv 1 \; [3]$, $10^2 = 100 = 3 \times 33 + 1$ donc $100 \equiv 1 \; [3]$ ...]
$10 \equiv 1 \; [9]$ $\quad 10^2 \equiv 1 \; [9]$

$$10^i = \underbrace{10 \times 10 \cdots \times 10}_{i \text{ fois}} \quad \text{donc } \overline{10^i} = \underbrace{\overline{10} \times \overline{10} \times \cdots \times \overline{10}}_{i \text{ fois}}$$
$$= \underbrace{\bar{1} \times \bar{1} \times \cdots \times \bar{1}}_{i \text{ fois}}$$
$$= \bar{1}$$

ce calcul marche aussi dans $\mathbb{Z}/9\mathbb{Z}$ car $\overline{10} = \bar{1}$ dans $\mathbb{Z}/9\mathbb{Z}$.

$\forall i \in \mathbb{N}$,
donc $\overline{10^i} = \bar{1}$ dans $\mathbb{Z}/3\mathbb{Z}$.
dans $\mathbb{Z}/9\mathbb{Z}$ aussi !

b. $n = \sum_{k \geq 0} d_k \cdot 10^k$ Donc $\overline{n} = \sum_{k \geq 0} \overline{d_k} \cdot \underbrace{\overline{10^k}}_{= \overline{1}}$

$= \sum_{k \geq 0} \overline{d_k}$. dans $\mathbb{Z}/3\mathbb{Z}$ ou $\mathbb{Z}/9\mathbb{Z}$

$\Leftrightarrow \overline{n - \sum_{k \geq 0} d_k} = \overline{0}$

$\Leftrightarrow 3 \mid n - \sum_{k \geq 0} d_k$ (9)

$\Leftrightarrow n \equiv \sum_{k \geq 0} d_k$ [3]. [9]

ex . $361 \equiv \underbrace{3+6+1}_{=10}$ [3]

$\equiv 1$ [3].

c. $n \equiv 0$ [3] [9] $\Leftrightarrow \sum_{k \geq 0} d_k \equiv 0$ [3] [9]

$\Updownarrow \qquad \Updownarrow$

$3 \mid n$ $\Longleftrightarrow$ $3 \mid \sum_{k \geq 0} d_k$

$9 \mid n$ $\qquad$ $9 \mid \sum_{k \geq 0} d_k$

donc 3 divise n ssi 3 divise la somme de ses chiffres.
9 divise n ssi 9

3- . ok

4- divisibilité par 11.

$n = \sum_{k \geq 0} d_k 10^k$

Donc, dans $\mathbb{Z}/11\mathbb{Z}$, $\overline{n} = \sum_{k \geq 0} \overline{d_k} \, \overline{10^k}$.

$a = 10$
$b = -1$
$a - b = 11$

Il faut déterminer $\overline{10^k}$ dans $\mathbb{Z}/11\mathbb{Z}$ pour $k \in \mathbb{N}$.

$\left[\begin{array}{l} \overline{a} = \overline{b} \text{ dans } \mathbb{Z}/11\mathbb{Z} \\ \Leftrightarrow 11 \mid a - b. \end{array} \right.$

$\boxed{\overline{10^k}} = \underbrace{\overline{10} \times \dots \times \overline{10}}_{k \text{ fois}} = \underbrace{(\overline{-1}) \times \dots \times (\overline{-1})}_{k \text{ fois}}$

car $\overline{10} = \overline{-1}$

$= (\overline{-1})^k$

$= \boxed{\overline{(-1)^k}}$.

Donc $\overline{n} = \overline{\sum_{k\geq 0} d_k \cdot (-1)^k}$ dans $\mathbb{Z}/11\mathbb{Z}$

donc $n \equiv \sum_{k\geq 0} d_k (-1)^k \ [11]$.

donc $11 / n \iff n \equiv 0 \ [11]$

$\iff \sum_{k\geq 0} d_k (-1)^k \equiv 0 \ [11]$.

$\iff 11 \mid \sum_{k\geq 0} d_k (-1)^k$.

Ex. $5472819 \equiv 9 - 1 + 8 - 2 + 7 - 4 + 5 \ [11]$

$\equiv 22 \ [11]$

$\equiv 0 \ [11]$.

donc 5472819 est divisible par 11.

[critère de divisibilité par 7 ?

$\overline{10^k}$ dans $\mathbb{Z}/7\mathbb{Z}$?

$10^0 \equiv 1 \ [7]$

$10^1 \equiv 3 \ [7]$

$10^2 \equiv 2 \ [7]$

$10^3 \equiv 2 \times 3 \ [7] \equiv -1 \ [7]$

$10^4 \equiv -3 \ [7]$

$10^5 \equiv -2 \ [7]$

$10^6 \equiv 1 \ [7]$

$10^7 = 10^6 \times 10 \equiv 3 \ [7]$ périodique

$\vdots$

$n = [a_4 a_3 a_2 a_1 a_0] = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 10^4$

$\equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 \ [7]$

$7 / n \iff 7 \mid a_0 + 3a_1 + 2a_2 - a_3 - 3a_4$

→ critère de divisibilité pas très pratique.

ex 4.13. combien de chiffres a 2017^{2019} ?

Beaucoup.

$$2017 \geq 2 \cdot 10^3$$
$$2017^{2019} \geq 2^{2019} \cdot 10^{3 \cdot 2019}$$
$$= 2^{2019} \cdot \underbrace{10^{6057}}_{1\underbrace{0 \cdots 0}_{6057 \text{ zéro}}}$$

Dans $\mathbb{Z}/10\mathbb{Z}$,

1- $\overline{7^0} = \overline{1}$

$\overline{7^1} = \overline{7}$

$\overline{7^2} = \overline{49} = \overline{-1} = \overline{6}$

$\overline{7^3} = \overline{7^2} \cdot \overline{7}$

$= \overline{-1} \cdot \overline{7}$

$= \overline{-7} = \boxed{\overline{3}}$

$\overline{7^4} = \overline{7^2} \cdot \overline{7^2}$

$= (\overline{-1}) \cdot (\overline{-1})$

$= \overline{1}$

$\leadsto n = 4$.

2. Soit $q, r \in \mathbb{N}$. $\overline{7}^{4q+r} = \overline{7}^{4q} \cdot \overline{7}^r$ $\quad (a^b)^c = a^{bc}$

$= \cancel{(\overline{7}^4)}^q \cdot \overline{7}^r$ $\quad \overline{1} =$

$= \overline{7}^r$, dans $\mathbb{Z}/10\mathbb{Z}$.

3- Soit $n \in \mathbb{N}$. Le chiffres des unités de n est l'unique entier $0 \leq a \leq 9$ tel que $\overline{n} = \overline{a}$ dans $\mathbb{Z}/10\mathbb{Z}$.

$n = 10 \cdot q + r$ avec $0 \leq r \leq 9$

$n = 2017^{2019}$

Dans $\mathbb{Z}/10\mathbb{Z}$, $\overline{2017^{2019}} = \overline{2017}^{2019}$

$= \overline{7}^{2019}$

Or, $2019 = \underset{q}{4 \times 504} + \underset{r}{3}$ $\quad$ $4q + r$ $\quad$ division euclidienne de 2017 par 4

2.

donc $\overline{7}^{2019} = \overline{7}^3 = \overline{3}$ dans $\mathbb{Z}/10\mathbb{Z}$.

Donc le chiffre des unités de 2017^{2019} est 3. car $\overline{2017^{2019}} = \overline{3}$ dans $\mathbb{Z}/10\mathbb{Z}$.

exercice 3.14.

1- Mq $7 \mid 3^{2n+1} + 2^{n+2}$ pour tout $n \geq 0$.

$\Updownarrow$

$\overline{3^{2n+1} + 2^{n+2}} = \bar{0}$ dans $\mathbb{Z}/7\mathbb{Z}$.

Dans $\mathbb{Z}/7\mathbb{Z}$, $\overline{3^{2n+1}} = \left(\overline{3^2}\right)^n \cdot \bar{3}$ et $\overline{2^{n+2}} = \bar{2}^n \cdot \bar{2}^2$

$= (\bar{9})^n \cdot \bar{3}$ $\qquad$ $= \bar{2}^n \cdot \overline{-3}$

$= (\bar{2})^n \cdot \bar{3}$ $\qquad$ $= -\bar{2}^n \cdot \bar{3}$

Donc $\overline{3^{2n+1} + 2^{n+2}} = \bar{2}^n \cdot \bar{3} - \bar{2}^n \cdot \bar{3}$

$= \bar{0}$.

2- Dans $\mathbb{Z}/11\mathbb{Z}$, $\overline{2^{6n+3}} = \left(\overline{2^6}\right)^n \cdot \overline{2^3}$

$= \overline{64}^n \cdot \bar{8}$

$= (\overline{-2})^n \cdot \overline{-3}$

et $\overline{3^{2n+1}} = (\overline{3^2})^n \cdot \bar{3}$

$= \bar{9}^n \cdot \bar{3}$

$= (\overline{-2})^n \cdot \bar{3}$

donc $\overline{2^{6n+3} + 3^{2n+1}} = -(\overline{-2})^n \cdot \bar{3} + (\overline{-2})^n \cdot \bar{3} = \bar{0}$.

donc $11 \mid 2^{6n+3} + 3^{2n+1}$. $(\forall n \in \mathbb{N})$.

3- Dans $\mathbb{Z}/3\mathbb{Z}$, $\bar{4} = \bar{1}$ donc $\overline{4^n - 1} = \bar{4}^n - \bar{1}$

$= \bar{1}^n - \bar{1}$

$= \bar{0}$

Il vaut mieux écrire

$2^{4^n} = 2^{(4^n)}$

$(2^2)^3 = 4^3 = 64$ $= 2^6$

$2^{(2^3)} = 2^8 = 256$

$2^{(4^n)} \neq (2^4)^n$ en général

• Calculons dans $\mathbb{Z}/7\mathbb{Z}$.

$\overline{2^0} = \bar{1}$

$\overline{2^1} = \bar{2}$

$\overline{2^2} = \bar{4}$

$\overline{2^3} = \bar{1}$

$q, r \in \mathbb{Z}$.

donc $\overline{2^{3q+r}} = \overline{2^3}^{\,q} \cdot \overline{2^r}$

$= \overline{2^r}$

$\overline{2^{4^n}} = \overline{2^{3q+1}} = \overline{2}^1$ dans
$= \overline{2}$. $\mathbb{Z}/7\mathbb{Z}$.

donc $\overline{2^{4^n} - 2} = \overline{2^{4^n}} - \overline{2}$
dans $\mathbb{Z}/7\mathbb{Z}$ $= \overline{2} - \overline{2}$
$= \overline{0}$

$4^n \equiv 1\,[3]$
donc $4^n = 3 \cdot q + 1$
pour un certain $q \in \mathbb{Z}$
$\Leftrightarrow$ $3 \mid 4^n - 1$,

- Arithmétique.
- prochain TD Lundi 15h45.