

CORRIGÉ DU CONTRÔLE CONTINU 2 DU 28 NOVEMBRE 2022, 15H15-16H15

Exercice 1.

- Comme 13 est un nombre premier, $\mathbb{Z}/13\mathbb{Z}$ est un corps, c'est-à-dire que tous ses éléments sont inversibles sauf $\bar{0}$. Par conséquent $(\mathbb{Z}/13\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}\}$.
- $\bar{1}^{-1} = \bar{1}$, $2 * 7 = 14 = 13 + 1$ donc $\bar{2}^{-1} = \bar{7}$ (d'où $\bar{7}^{-1} = \bar{2}$), $3 * 9 = 27 = 2 * 13 + 1$ donc $\bar{3}^{-1} = \bar{9}$ (d'où $\bar{9}^{-1} = \bar{3}$), $4 * 10 = 40 = 3 * 13 + 1$ donc $\bar{4}^{-1} = \bar{10}$ (d'où $\bar{10}^{-1} = \bar{4}$), $5 * 8 = 40$ donc $\bar{5}^{-1} = \bar{8}$ (d'où $\bar{8}^{-1} = \bar{5}$), $6 * 11 = 66 = 5 * 13 + 1$ donc $\bar{6}^{-1} = \bar{11}$ (d'où $\bar{11}^{-1} = \bar{6}$). Enfin, $\bar{12}^{-1} = \bar{-1}^{-1} = \bar{-1} = \bar{12}$, comme toujours pour $\overline{n-1}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$.
- $12! + 1 = 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * 10 * 11 * 12 + 1 = (2 * 7) * (3 * 9) * (4 * 10) * (5 * 8) * (6 * 11) * 12 + 1 \equiv 12 + 1 \equiv 0 [13]$. On a utilisé les inverses calculés à la question précédente pour simplifier les produits.
- Comme 13 est premier et $\text{pgcd}(2, 13) = 1$, on a $2^{12} \equiv 1 [13]$ par le petit théorème de Fermat. Par conséquent $2^{37} \equiv (2^{12})^3 * 2 \equiv 2 [13]$.

$$5. \sum_{i=1}^{52} i = \frac{52 * 53}{2} = 26 * 53 \equiv 0 [53].$$

(Solution alternative si on ne connaît pas la formule $\sum_{i=1}^n i = \frac{n(n+1)}{2}$:

$$\sum_{i=1}^{52} i = 1 + 2 + \dots + 52 = (1 + 52) + (2 + 51) + \dots + (26 + 27) \equiv 0 [53].)$$

$$6. \sum_{i=0}^{51} 1^i = \sum_{i=0}^{51} 1 = 52 \equiv 52 [53].$$

$$\sum_{i=0}^{51} 52^i \equiv \sum_{i=0}^{51} (-1)^i \equiv 1 - 1 + \dots + 1 - 1 \equiv 0 [53].$$

$$7. \sum_{i=0}^{51} 2^i = \frac{2^{52} - 1}{2 - 1} \equiv 1 - 1 \equiv 0 [53].$$

On a utilisé le fait que, comme 53 est premier et $\text{pgcd}(2, 53) = 1$, alors $2^{52} \equiv 1 [53]$ par le petit théorème de Fermat.

(Solution alternative si on ne connaît pas la formule $\sum_{i=0}^n a^i = \frac{a^{n+1} - 1}{a - 1}$:

Avant de calculer, on détermine l'ordre de $\bar{2}$ dans $(\mathbb{Z}/53\mathbb{Z})^*$. On sait que l'ordre de tout élément de $(\mathbb{Z}/53\mathbb{Z})^*$ doit diviser $|(\mathbb{Z}/53\mathbb{Z})^*| = 52$, et est donc égal à 1, 2, 4, 13, 26 ou 52.

$2^1 \not\equiv 1 [53]$, $2^2 = 4 \not\equiv 1 [53]$, $2^4 = 16 \not\equiv 1 [53]$, $2^{13} = 2^8 * 2^4 * 2 \equiv (-9) * 16 * 2 \equiv (-144) * 2 \equiv 15 * 2 \equiv 30 \not\equiv 1 [53]$, $2^{26} \equiv 30^2 \equiv 900 \equiv -1 \not\equiv 1 [53]$. Ainsi $\bar{2}$ est nécessairement d'ordre 52.

Comme $52 = |(\mathbb{Z}/53\mathbb{Z})^*|$, cela signifie que $\bar{2}$ est générateur du groupe $(\mathbb{Z}/53\mathbb{Z})^*$, c'est-à-dire que tout

$\bar{a} \in (\mathbb{Z}/53\mathbb{Z})^*$ s'écrit sous la forme $\bar{a} = \bar{2}^i$. Dans la somme $\sum_{i=1}^{51} \bar{2}^i$, chaque élément de $(\mathbb{Z}/53\mathbb{Z})^*$ apparaît donc une et une seule fois. Ainsi $\sum_{i=0}^{51} 2^i \equiv 1 + 2 + \dots + 52 \equiv \sum_{i=1}^{52} i \equiv 0 [53]$ d'après la question 5.)

Exercice 2.

- $\mathbb{Z}/N\mathbb{Z}$ est un corps si et seulement si N est premier. Par conséquent, c'est un corps pour $N = 2$ et $N = 13$, mais ce n'en est pas un pour $N = 9$ et $N = 42$. Dans $\mathbb{Z}/9\mathbb{Z}$, $\bar{3} * \bar{3} = \bar{0}$ donc $\bar{3}$ est un diviseur de 0. Dans $\mathbb{Z}/42\mathbb{Z}$, $\bar{2} * \bar{21} = \bar{0}$ donc $\bar{2}$ est un diviseur de 0.

- Un élément $\bar{a} \in \mathbb{Z}/12\mathbb{Z}$ est inversible si et seulement si $\text{pgcd}(a, 12) = 1$, donc $(\mathbb{Z}/12\mathbb{Z})^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$.

*	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$
$\bar{5}$	$\bar{5}$	$\bar{1}$	$\bar{11}$	$\bar{7}$
$\bar{7}$	$\bar{7}$	$\bar{11}$	$\bar{1}$	$\bar{5}$
$\bar{11}$	$\bar{11}$	$\bar{7}$	$\bar{5}$	$\bar{1}$

- L'ordre de chaque élément se déduit immédiatement de la table ci-dessus :

Ordre($\bar{1}$) = 1, Ordre($\bar{5}$) = 2 (car $\bar{5}^2 = \bar{1}$), Ordre($\bar{7}$) = 2 (car $\bar{7}^2 = \bar{1}$), Ordre($\bar{11}$) = 2 (car $\bar{11}^2 = \bar{1}$).

4. D'après la question 3, aucun élément n'est d'ordre $|(\mathbb{Z}/12\mathbb{Z})^*| = 4$, donc aucun élément n'est générateur. Par définition, cela signifie que le groupe $(\mathbb{Z}/12\mathbb{Z})^*$ n'est pas cyclique.

Exercice 3.

1. D'après le petit théorème de Fermat, comme $\text{pgcd}(2, 1381) = 1$, on a $2^{1380} \equiv 1[1381]$.
2. Si 1363 était un nombre premier, alors on pourrait appliquer le petit théorème de Fermat qui donnerait $2^{1362} \equiv 1[1363]$. Or ici $2^{1362} \equiv 361 \not\equiv 1[1363]$, donc 1363 n'est pas premier.
3. On ne peut rien dire avec certitude ! On peut avoir un entier n **non premier** tel qu'il existe tout de même un (ou des) entier(s) a satisfaisant $a^{n-1} \equiv 1[n]$: un tel a est alors appelé un "menteur de Fermat" de n .
4. Soit $n \geq 3$ un entier. On tire au hasard un entier $1 < a < n$, et on calcule a^{n-1} modulo n .
 - Si $a^{n-1} \equiv 1[n]$ alors n est **probablement** premier;
 - sinon, on sait **avec certitude** que n n'est pas premier.
