Correction CC1 Arithmétique

Exercice 1 (/5)

1. (/2) Un sous-groupe de $(\mathbb{Z}, +)$ est un sous-ensemble $H \subset \mathbb{Z}$ tel que :
   - $0 \in H$ (contient l'élément neutre pour l'addition),
   - Pour tout $x, y \in H$, $x + y \in H$ (stable par somme),
   - Pour tout $x \in H$, $-x \in H$ (stable par passage à l'opposé).

   Remarque : On ne note pas x^{-1} pour le symétrique de x dans un groupe additif comme $(\mathbb{Z}, +)$, on note $-x$ et on l'appelle l'opposé de x. Si on étudiait le groupe $(\mathbb{Q}^*, \times)$, le symétrique de x sera noté x^{-1} et s'appellera l'inverse de x.

   Remarque : On peut rassembler les deux derniers points en : Pour tout $x, y \in H$, $x - y \in H$.

2. a. (/1) $\mathbb{N}$ n'est pas stable par passage à l'opposé, puisque $1 \in \mathbb{N}$ mais $-1 \notin \mathbb{N}$. Donc $\mathbb{N}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$.

   b. (/1) L'ensemble des multiples de 3 est le sous-ensemble de $\mathbb{Z}$ noté $3\mathbb{Z}$. Il s'agit d'un sous-groupe de $(\mathbb{Z}, +)$ par le théorème du cours. Sinon, on peut le redémontrer :
   - $3\mathbb{Z}$ contient zéro puisque $0 = 3 \times 0$.
   - $3\mathbb{Z}$ est stable par somme puisque la somme de deux multiples de 3 est un multiple de 3.
   - $3\mathbb{Z}$ est stable par passage à l'opposé puisqu'un nombre et son opposé sont multiples des mêmes nombres.

   c. (/1) Soit $H = \{n \in \mathbb{Z} \mid n \equiv 1 \mod 3\}$. Puisque $0 \equiv 0 \mod 3$, alors $0 \notin H$. Donc H n'est pas un sous-groupe de $(\mathbb{Z}, +)$.

Exercice 2 (/4)

1. (/2) Soit $n \in \mathbb{Z}$. Le terme $(n-1)n(n+1)$ est le produit des trois entiers consécutifs $n-1$, n et $n+1$. L'un des trois est alors divisible par 3 et on en déduit que le produit l'est donc également. On vient de montrer que $(n-1)n(n+1)$ est divisible par 3, c'est à dire que :

$$\begin{aligned} (n-1)n(n+1) &\equiv 0 \mod 3 \\ n^3 - n &\equiv 0 \mod 3 \\ n^3 &\equiv n \mod 3. \end{aligned}$$

   Remarque : On pouvait également procéder par disjonction de cas ($n \equiv 0, 1$ ou $2 \mod 3$) pour montrer que $(n-1)n(n+1)$ est divisible par 3.

2. (/2) Montrons par récurrence sur $n \in \mathbb{N}^*$ la propriété :

$$\mathcal{P}(n) : \sum_{k=1}^{n} k(k-1) = \frac{n^3 - n}{3}.$$

   Initialisation : $n = 1$
   D'une part, $\sum_{k=1}^{1} k(k-1) = 1 \times 0 = 0$.
   D'autre part, $\frac{1^3-1}{3} = 0$.
   D'où $\sum_{k=1}^{1} k(k-1) = \frac{1^3-1}{3}$. $\mathcal{P}(1)$ est vraie.

   Hérédité :
   Soit $n \in \mathbb{N}^*$. Supposons $\mathcal{P}(n)$ vraie et montrons que $\mathcal{P}(n+1)$ l'est également.

$$\begin{aligned}\sum_{k=1}^{n+1} k(k-1) &= \sum_{k=1}^{n} k(k-1) + (n+1)n \\ &= \frac{n^3-n}{3} + n^2 + n && \text{par hypothèse de récurrence} \\ &= \frac{n^3-n+3n^2+3n}{3} \\ &= \frac{n^3+3n^2+3n+1-n-1}{3} \\ &= \frac{(n+1)^3-(n+1)}{3}.\end{aligned}$$

Ainsi, $\mathcal{P}(n+1)$ est également vraie.

Conclusion :
Par principe de récurrence, on en conclut que, pour tout n $in\mathbb{N}^*$,

$$\sum_{k=1}^{n} k(k-1) = \frac{n^3-n}{3}.$$

Remarque : Le passage

$$\frac{n^3+3n^2+2n}{3} = \frac{(n+1)^3-(n+1)}{3}$$

était trop rapide et passait pour une arnaque. Il fallait détailler pourquoi on avait égalité.

Exercice 3 (/6)

1. (/2) Faisons l'algorithme d'Euclide avec les nombres 33 et 45.

$$\begin{aligned}45 &= 33 \times 1 + 12 \\ 33 &= 12 \times 2 + 9 \\ 12 &= 9 \times 1 + \boxed{3} \\ 9 &= 3 \times 3 + \underline{0}.\end{aligned}$$

Donc $\text{pgcd}(45, 33) = 3$.

2. (/1) On s'intéresse à l'équation suivante d'inconnu $(x, y) \in \mathbb{Z}^2$:

$$33x + 45y = 3.$$

Remontons l'algorithme d'Euclide afin de trouver une solution particulière.

$$\begin{aligned}3 &= 12 - 9 \\ &= 12 - (33 - 12 \times 2) \\ &= 12 \times 3 - 33 \\ &= (45 - 33) \times 3 - 33 \\ &= 45 \times 3 - 33 \times 4.\end{aligned}$$

Ainsi le couple $(-4, 3)$ est solution de l'équation $33x + 45y = 3$.

L'ensemble de solution est

$$\mathcal{S} = \left\{ \left(-4 + \frac{45}{3}k, 3 - \frac{33}{3}k \right) \middle| \, k \in \mathbb{Z} \right\} = \{(-4 + 15k, 3 - 11k) | k \in \mathbb{Z}\}.$$

Remarque : On attendait un ensemble de solution et pas juste une solution particulière. Attention également à bien définir k dans l'ensemble !

3. (/1) L'équation (1) admet des solutions si et seulement si $3 \mid c$. Dans ce cas là, la solution n'est pas unique, il en existe une infinité.

   Remarque : Soyez cohérent avec la question précédente. Si vous dite que l'on a unicité, on doit avoir unicité pour $c = 3$ également. Or, on en trouve une infinité à la question précédente.

4. (/2) Par la question 2, on sait que

$$f(-4, 3) = 3 = f(11, -8).$$

   Or $(4, -3) \neq (11, -8)$ donc la fonction f n'est pas injective.
   D'autre part, comme 3 ne divise pas 2, 2 n'a pas d'antécédent par la fonction f (cf q°3). Ainsi, f n'est pas non plus surjective.

   Remarque : Trop de choses à dire, je laisse pour Mathilde du futur. Bon courage Mathilde du futur ! (Jadidou)

Exercice 4 (/4)

1. (/1) On a $3^2 = 9 = -1 + 10$ d'où :

$$3^2 \equiv -1 \mod 10.$$

   Par suite, comme $3^4 = (3^2)^2$, on a

$$\begin{aligned} 3^4 &\equiv (-1)^2 \mod 10 \\ &\equiv 1 \mod 10. \end{aligned}$$

2. (/2) En remarquant que $2025 = 506 \times 4 + 1$, on obtient :

$$3^{2025} = (3^4)^{506} \times 3$$

   puis, par passage modulo 10 et la question précédente,

$$3^{2025} \equiv (1)^{506} \times 3 \mod 10$$

   et l'on a ainsi

$$3^{2025} \equiv 3 \mod 10.$$

3. (/1) Le dernier chiffre d'un entier positif $n \in \mathbb{N}$ est égal au reste de la division euclidienne de n par 10. Ainsi, le dernier chiffre de 3^{2025} en base 10 est 3.

Exercice 5 (/6)

1. (/2)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Remarque : Si on voulait se passer de remplir le tableau en entier, il fallait bien justifier pourquoi la diagonale et la moitié supérieure sufisaient. En l'occurrence, l'addition et la multiplication sont commutatives dans $\mathbb{Z}/5\mathbb{Z}$.

2. (a) (/1) En regardant dans le tableau de multiplication, on constate que $\overline{x} \cdot \overline{2} = \overline{1}$ a pour unique solution $\overline{3}$.
   (b) (/1) En regardant dans le tableau de multiplication, on constate que $\overline{x} \cdot \overline{3} = \overline{2}$ a pour unique solution $\overline{4}$.

   Remarque : Toute réponse injustifiée ne recevait pas la totalité des points. Les justifications attendues étaient "par la table de multiplication" ou bien la justification que $\overline{2}$ et $\overline{3}$ sont inversibles. De même, il ne suffit pas de dire que $\overline{4} \times \overline{3} = \overline{2}$ pour conclure. Ceci montre que $\overline{4}$ est bien une solution, mais elle pourrait ne pas être unique.

3. (/1) Supposons par l'absurde qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv 3 \mod 5$. Ceci signifie que $\overline{x}^2 = \overline{3}$. Or, en regardant la diagonale de la table de multiplication, on constate que si $\overline{x} \in \mathbb{Z}/5\mathbb{Z}$, alors $\overline{x}^2 \in \{0, 1, 4\}$. On a alors $\overline{x}^2 = 3$ et $\overline{x}^2 \in \{0, 1, 4\}$: absurde.
   On en conclut qu'il n'existe pas d'entier tel que $x^2 \equiv 3 \mod 5$.

4. (/1) Soit $(x, y) \in \mathbb{Z}^2$. Supposons que (x, y) vérifie :

$$x^2 + 4xy - y^2 = 5008. \tag{1}$$

   On a alors,

$$x^2 + 4xy + 4y^2 \equiv 3 \mod 5$$

   puis,

$$(x + 2y)^2 \equiv 3 \mod 5.$$

   On a donc montré que si $(x, y) \in \mathbb{Z}^2$ est solution de l'équation (1), alors $(x + 2y)^2 \equiv 3 \mod 5$.
   Par la question 3, on sait qu'il n'existe pas d'entier x tel que $x \equiv 3 \mod 5$. Comme pour tout $(x, y) \in \mathbb{Z}^2$, $x+2y$ est un entier, on en déduit que pour tout $(x, y) \in \mathbb{Z}^2$, $(x+2y)^2 \not\equiv 3 \mod 5$. Par contraposition du résultat démontré précédemment, on en déduit qu'il n'existe pas de solutions $(x, y) \in \mathbb{Z}^2$ à l'équation (1).

Exercice 6 (/5)

1. (/2) Calculons les carrés des éléments de $\mathbb{Z}/8\mathbb{Z}$ dans un tableau :

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{1}$

On en déduit que l'équation

$$\overline{x}^2 = \overline{a}$$

a des solutions si et seulement si $\overline{a} \in \{\overline{0}, \overline{1}, \overline{4}\}$.

2. (/2) Supposons qu'il existe $(x, y, z) \in \mathbb{Z}^3$ tel que

$$x^2 + y^2 + z^2 \equiv 7 \mod 8.$$

En regardant cette égalité dans $\mathbb{Z}/8\mathbb{Z}$, on obtient alors

$$\overline{x}^2 + \overline{y}^2 + \overline{z}^2 = \overline{7}.$$

Par la question précédente, on sait que $\overline{x}^2$, $\overline{y}^2$ et $\overline{z}^2$ appartiennent à $\{\overline{0}, \overline{1}, \overline{4}\}$
Traitons alors tous les cas possibles :

- $\overline{0}+\overline{0}+\overline{0} = \overline{0}$
- $\overline{0}+\overline{0}+\overline{1} = \overline{1}$
- $\overline{0}+\overline{0}+\overline{4} = \overline{4}$
- $\overline{0}+\overline{1}+\overline{1} = \overline{2}$
- $\overline{0}+\overline{1}+\overline{4} = \overline{5}$
- $\overline{0}+\overline{4}+\overline{4} = \overline{1}$
- $\overline{1}+\overline{1}+\overline{1} = \overline{3}$
- $\overline{1}+\overline{1}+\overline{4} = \overline{6}$
- $\overline{1}+\overline{4}+\overline{4} = \overline{2}$
- $\overline{4}+\overline{4}+\overline{4} = \overline{5}$

On a alors d'une part $\overline{x}^2 + \overline{y}^2 + \overline{z}^2 = \overline{7}$ et d'autre part $\overline{x}^2 + \overline{y}^2 + \overline{z}^2 \in \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$: ceci est absurde !
On en conclut qu'il n'existe pas d'entier $(x, y, z) \in \mathbb{Z}^3$ tels que

$$x^2 + y^2 + z^2 \equiv 7 \mod 8.$$

3. (/1) Soit $(x, y, z) \in \mathbb{Z}^3$. Supposons que $x^2 + y^2 + z^2 = 2023$. Comme $2023 = 8 \times 252 + 7$, l'égalité devient, en passant modulo 8,

$$x^2 + y^2 + z^2 \equiv 7 \mod 8.$$

Or d'après la question précédente, il n'existe pas de tel triplet. Ceci est donc absurde et on en déduit qu'il n'existe pas d'entiers x, y, z tels que $x^2 + y^2 + z^2 = 2023$.