4.3 Corrections des exercices

Exercice 1 :

Montrer que $3 \times 2^{11} \equiv 2^{12} \left[2^8\right]$

Il suffit de faire la différence $3 \times 2^{11} - 2^{12}$ Nous avons :

$$3 \times 2^{11} - 2^{12} = 2^{11}(3-2) = 2^{11} = 2^3 \times 2^8$$

Donc $3 \times 2^{11} - 2^{12} = k \times 2^8$, c'est à dire $3 \times 2^{11} \equiv 2^{12} \left[2^8\right]$

Exercice 2 :

Soient $b \in \mathbb{N}^*$ *et* $a \in \mathbb{Z}$. *Comparer les quotients* q_1, q_2 *et* q_3 *des divisions de* a *par* b, *de* $2a$ *par* b *et de* $(2a+b)$ *par* $2b$

Cet exercice joue beaucoup sur l'unicité du couple (Q, R) dans le théorème 4.2.6 sur la division euclidienne

1. Pour commencer :
   $\longrightarrow$ $a = bq_1 + r_1$ avec $0 \leqslant r_1 < b$
   $\longrightarrow$ Puis $2a = bq_2 + r_2$ avec $0 \leqslant r_2 < b$
   $\longrightarrow$ Et $2a + b = 2bq_3 + r_3$ avec $0 \leqslant r_3 < b$
   Nous avons $2a = 2bq_1 + 2r_1 = b(2q_1) + 2r_1$ et même $2a + b = 2b(q_1) + (2r_1 + b)$
2. Supposons $2r_1 < b$.
   $\longrightarrow$ Alors, d'après le théorème de division euclidienne 4.2.6, des égalités $2a = bq_2 + r_2$ avec $0 \leqslant r_2 < b$ et $2a = b(2q_1) + 2r_1$, nous avons $q_2 = 2q_1$ et même $r_2 = 2r_1$.
   $\longrightarrow$ De $2r_1 < b$, nous tirons $2r_1 + b < 2b$ et toujours d'après le théorème de la division euclidienne, des égalités $2a + b = 2bq_3 + r_3$ avec $0 \leqslant r_3 < b$ et $2a + b = 2b(q_1) + (2r_1 + b)$, nous avons $q_3 = q_1$ et $r_3 = 2r_1 + b$.
   En conclusion $q_2 = 2q_1 = 2q_3 \iff q_1 + q_3 = q_2$
3. Supposons, maintenant que $b \leqslant 2r_1 < 2b$
   $\longrightarrow$ Nous avons alors :

   $$2a = 2bq_1 + 2r_1 \iff 2a = b(2q_1) + b + 2r_1 - b \iff 2a = b(2q_1 + 1) + (2r_1 - b)$$

   De $b \leqslant 2r_1 < 2b$, nous tirons $0 \leqslant 2r_1 - b < b$, et alors, comme $2a = bq_2 + r_2 = b(2q_1 + 1) + (2r_1 - b)$, d'après le théorèmes de la division euclidienne, nous obtenons $2q_1 + 1 = q_2$
   $\longrightarrow$ Maintenant :

   $$2a + b = 2bq_1 + 2r_1 + b = 2bq_1 + 2b + 2r_1 - b = 2b(q_1 + 1) + (2r_1 - b) = 2bq_3 + r_3$$

   D'après le théorème 4.2.6 nous avons $q_3 = q_1 + 1$
   Nous avons donc $q_2 = 2q_1 + 1$ et $q_3 = q_1 + 1$, c'est à dire $q_2 = q_1 + q_3$

Nous avons donc, de manière générale $q_2 = q_1 + q_3$

Exercice 3 :

1. *Faites la table de multiplication de* $\mathbb{Z}/5\mathbb{Z}$

$\times$ ↱	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

On peut remarquer qu'il n'y a aucun diviseur de 0, et que tous les éléments non nuls sont inversibles : 1 et 4 sont leur propre inverse (remarquer que $4 \equiv -1\,[5]$ et que $4^2 \equiv (-1)^2 \equiv 1\,[5]$) et que l'inverse de 2 est 3

2. *Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $\dot{2}+x=\dot{1}$ d'inconnue x*

   Nous avons :
   $$\dot{2}+x=\dot{1}\iff x=\dot{1}-\dot{2}=\dot{1}+\dot{3}=\dot{4}=\dot{-1}$$

3. *Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $\dot{3}x=\dot{2}$ d'inconnue x*

   Nous avons :
   $$\dot{3}x=\dot{2}\iff\dot{2}\times\dot{3}x=\dot{2}\times\dot{2}\iff x=\dot{4}$$

4. *Trouver, dans $\mathbb{Z}/5\mathbb{Z}$, les inconnues $x\in\mathbb{Z}/5\mathbb{Z}$ et $y\in\mathbb{Z}/5\mathbb{Z}$ vérifiant le système*

   $$\begin{cases}\dot{2}x+\dot{3}y=&\dot{2}\\ \dot{1}x+\dot{2}y=&\dot{4}\end{cases}$$

   On multiplie la seconde ligne par $\dot{2}$ et nous obtenons comme nouveau système :

   $$\begin{cases}\dot{2}x+\dot{3}y=&\dot{2}\\ \dot{2}x+\dot{4}y=&\dot{3}\end{cases}$$

   Puis nous soustrayons les 2 lignes, et nous avons $y=\dot{3}-\dot{2}=\dot{1}$ et en remplaçant y par sa valeur, nous avons $x=\dot{2}$

5. *Résoudre dans $\mathbb{Z}/5\mathbb{Z}$ l'équation $x^2+\dot{2}x-\dot{3}=\dot{0}$ d'inconnue x*

   Nous avons $x^2+\dot{2}x=\left(x+\dot{1}\right)^2-\dot{1}$ de telle sorte que nous avons :

   $$x^2+\dot{2}x-\dot{3}=\dot{0}\iff\left(x+\dot{1}\right)^2-\dot{1}-\dot{3}=\dot{0}\iff\left(x+\dot{1}\right)^2=\dot{4}$$

   D'où nous tirons $\left(x+\dot{1}\right)=\dot{2}$ ou $\left(x+\dot{1}\right)=-\dot{2}=\dot{3}$
   Ainsi nous avons comme solution $x=\dot{1}$ ou $x=\dot{2}$

6. *Résoudre dans $\mathbb{Z}/5\mathbb{Z}$, l'équation $x^2-x-\dot{2}=\dot{0}$*

   Nous allons recommencer ce que nous avons fait à la question précédente. Nous avons :

   $$x^2-x=x^2+\dot{4}x=(x+2)^2-\dot{4}$$

   Et donc $x^2-x-\dot{2}=\dot{0}\iff\left(x+\dot{2}\right)^2-\dot{4}-\dot{2}=\dot{0}\iff\left(x+\dot{2}\right)^2-\dot{1}=\dot{0}\iff\left(x+\dot{2}\right)^2=\dot{1}$.
   D'où nous tirons donc $x+\dot{2}=\dot{1}$ ou $x+\dot{2}=-\dot{1}=\dot{4}$, c'est à dire $x=\dot{4}$ ou $x=\dot{2}$

Exercice 4 :

Montrer que l'implication suivante est vraie : $x\equiv 4\,[8]\implies x^2\equiv 16\,[64]$.
En effet :

$$\begin{aligned}x\equiv 4\,[8]&\iff x=4+k\times 8\\ &\implies x^2=16+k^2\times 64+2\times 4\times 8\times k\iff x^2=16+64\left(k^2+k\right)\iff x^2\equiv 16\,[64]\end{aligned}$$

Remarquons que nous avons $x\equiv 4\,[8]\implies x^2\equiv 16\equiv 0\,[8]$

Exercice 5 :

1. *Trouver les entiers relatifs $x\in\mathbb{Z}$ tels que $x^2+x+1\equiv 0\,[4]$* Nous allons écumer toutes les valeurs que peut prendre x dans $\mathbb{Z}/4\mathbb{Z}$
   - ◇ Si $x\equiv 0\,[4]$, alors $x^2+x+1\equiv 1\,[4]$; donc $x\equiv 0\,[4]$ n'est pas une solution de l'équation
   - ◇ Si $x\equiv 1\,[4]$, alors $x^2+x+1\equiv 3\,[4]$; donc $x\equiv 1\,[4]$ n'est pas une solution de l'équation
   - ◇ Si $x\equiv 2\,[4]$, alors $x^2+x+1\equiv 3\,[4]$; donc $x\equiv 2\,[4]$ n'est pas une solution de l'équation
   - ◇ Si $x\equiv 3\,[4]$, alors $x^2+x+1\equiv 1\,[4]$; donc $x\equiv 3\,[4]$ n'est pas une solution de l'équation

   En conclusion, il n'existe pas d'entiers relatifs $x\in\mathbb{Z}$ tels que $x^2+x+1\equiv 0\,[4]$

2. *Démontrer que, pour tout $x \in \mathbb{Z}$, nous avons $x^3 - x \equiv 0\,[3]$* Nous itérons l'écumage, cette fois ci dans $\mathbb{Z}/3\mathbb{Z}$ en remarquant que $x^3 - x = x\,(x+1)\,(x-1)$:
   - ◇ Si $x \equiv 0\,[3]$, alors $x^3 - x \equiv 0\,[3]$
   - ◇ Si $x \equiv 1\,[4]$, alors $x^3 - x \equiv 0\,[3]$
   - ◇ Si $x \equiv 2\,[4]$, alors $x^3 - x \equiv 0\,[3]$

   Ce qui signifie que pour tout entier relatif $x \in \mathbb{Z}$, le produit de 3 entiers consécutifs $x\,(x+1)\,(x-1)$ est divisible par 3.

Exercice 8 :

Résoudre les congruences suivantes :

1. $3x \equiv 7\,[16]$

   → Première chose de remarquable, c'est que 3 est inversible dans $\mathbb{Z}/16\mathbb{Z}$. En effet :

   $$3 \times 11 = 33 \text{ et } 33 \equiv 1\,[16]$$

   → En utilisant la compatibilité de la multiplication avec la relation de congruence, nous avons :

   $$3x \equiv 7\,[16] \iff 11 \times 3x \equiv 11 \times 7 \equiv 13\,[16] \iff x \equiv 13\,[16]$$

   → Nous obtenons donc $x \equiv 13\,[16]$
2. $5x + 7 \equiv 6\,[23]$

   Pour commencer, nous avons $5x + 7 \equiv 6\,[23] \iff 5x \equiv -1 \equiv 22\,[23]$

   → Pour commencer, 5 est inversible dans $\mathbb{Z}/23\mathbb{Z}$. En effet :

   $$5 \times 14 = 70 \text{ et } 70 \equiv 1\,[23]$$

   → En utilisant la compatibilité de la multiplication avec la relation de congruence, nous avons :

   $$5x \equiv 22\,[23] \iff 14 \times 5x \equiv 14 \times 22 \equiv 9\,[23] \iff x \equiv 9\,[23]$$

   → Nous obtenons donc $x \equiv 9\,[23]$
3. $4x \equiv 9\,[13]$

   → Comme précédemment, 4 est inversible dans $\mathbb{Z}/13\mathbb{Z}$. En effet :

   $$5 \times 14 = 70 \text{ et } 70 \equiv 1\,[23]$$

   → En utilisant la compatibilité de la multiplication avec la relation de congruence, nous avons :

   $$5x \equiv 22\,[23] \iff 14 \times 5x \equiv 14 \times 22 \equiv 9\,[23] \iff x \equiv 9\,[23]$$

   → Nous obtenons donc $x \equiv 9\,[23]$
4. $2x + 8 \equiv 5\,[33]$

   → Tout d'abord $2x + 8 \equiv 5\,[33] \iff 2x \equiv 30\,[33]$

   → Comme précédemment, 2 est inversible dans $\mathbb{Z}/30\mathbb{Z}$. En effet :

   $$2 \times 17 = 34 \text{ et } 34 \equiv 1\,[33]$$

   → En utilisant la compatibilité de la multiplication avec la relation de congruence, nous avons :

   $$2x \equiv 30\,[33] \iff 17 \times 2x \equiv 30 \times 17 \equiv 15\,[33] \iff x \equiv 15\,[33]$$

   → Nous obtenons donc $x \equiv 15\,[33]$
5. $3x + 9 \equiv 8x + 61\,[64]$

   Rasoir de toujours faire les mêmes choses ; on trouve $x \equiv 28\,[64]$
6. $4x + 3 \equiv 7x + 2\,[11]$

   On trouvera $x \equiv 4\,[11]$

Exercice 9 :

Montrer que, pour tout entier naturel $n \in \mathbb{N}$, n^3 est de la forme $7k+1$, $7k-1$, $7k$

Nous allons recenser tous les cas en étudiant les congruences modulo 7 ; ces cas sont présentés dans le tableau ci-après.

n	n^2	n^3
0	0	0
1	1	1
2	4	1
3	2	-1
4	2	1
5	4	-1
6	1	-1

Ainsi, pour tout $n \in \mathbb{Z}$, nous avons $n^3 \equiv -1\,[7]$ ou $n^3 \equiv 0\,[7]$ ou $n^3 \equiv 1\,[7]$, ce qui veut dire $n^3 = 7k+1$, $n^3 = 7k-1$ ou $n^3 = 7k$

Exercice 10 :

Calculer les restes, modulo 7, des nombres 2^n et 3^n ; trouver alors $n$tel que $2^n + 3^n \equiv 0\,[7]$

→ On regarde les puissances de 2

$$2^0 \equiv 1\,[7] \quad 2^1 \equiv 2\,[7] \quad 2^2 \equiv 4\,[7] \quad 2^3 \equiv 1\,[7]$$

Ainsi,
- ⋆ Si $n \equiv 0\,[3]$, alors $2^n \equiv 1\,[7]$
- ⋆ Si $n \equiv 1\,[3]$, alors $2^n \equiv 2\,[7]$
- ⋆ Si $n \equiv 2\,[3]$, alors $2^n \equiv 4\,[7]$

→ On regarde les puissances de 3

$$3^0 \equiv 1\,[7] \quad 3^1 \equiv 3\,[7] \quad 3^2 \equiv 2\,[7] \quad 3^3 \equiv 6\,[7] \quad 3^4 \equiv 4\,[7] \quad 3^5 \equiv 5\,[7] \quad 3^6 \equiv 1\,[7]$$

Ainsi,
- ⋆ Si $n \equiv 0\,[6]$, alors $3^n \equiv 1\,[7]$
- ⋆ Si $n \equiv 1\,[6]$, alors $3^n \equiv 3\,[7]$
- ⋆ si $n \equiv 2\,[6]$, alors $3^n \equiv 2\,[7]$
- ⋆ si $n \equiv 3\,[6]$, alors $3^n \equiv 6\,[7]$
- ⋆ si $n \equiv 4\,[6]$, alors $3^n \equiv 4\,[7]$
- ⋆ si $n \equiv 5\,[6]$, alors $3^n \equiv 5\,[7]$

→ Et maintenant, faisons la synthèse :
- ⋆ Si $n \equiv 0\,[6]$, alors $n \equiv 0\,[3]$ et donc $2^n \equiv 1\,[7]$ et $3^n \equiv 1\,[7]$, c'est à dire $2^n + 3^n \equiv 2\,[7]$
- ⋆ Si $n \equiv 1\,[6]$, alors $n \equiv 1\,[3]$ et donc $2^n \equiv 2\,[7]$ et $3^n \equiv 3\,[7]$, c'est à dire $2^n + 3^n \equiv 5\,[7]$
- ⋆ Si $n \equiv 2\,[6]$, alors $n \equiv 2\,[3]$ et donc $2^n \equiv 4\,[7]$ et $3^n \equiv 2\,[7]$ d'où $2^n + 3^n \equiv 6\,[7]$
- ⋆ Si $n \equiv 3\,[6]$, alors $n \equiv 0\,[3]$ et donc $2^n \equiv 1\,[7]$ et $3^n \equiv 6\,[7]$ d'où $2^n + 3^n \equiv 0\,[7]$
- ⋆ Si $n \equiv 4\,[6]$, alors $n \equiv 1\,[3]$ et donc $2^n \equiv 2\,[7]$ et $3^n \equiv 4\,[7]$ d'où $2^n + 3^n \equiv 6\,[7]$
- ⋆ Si $n \equiv 5\,[6]$, alors $n \equiv 2\,[3]$ et donc $2^n \equiv 4\,[7]$ et $3^n \equiv 5\,[7]$, c'est à dire $2^n + 3^n \equiv 2\,[7]$

Et voilà le travail !

Exercice 11 :

Erwann est représentant de commerce. Partant de Vannes, il parcourt la Bretagne en respectant toujours les mêmes étapes :
il va à Nantes, puis à Rennes, puis à saint Brieuc ; de là il va à Brest, ensuite à Quimper et revient à Vannes. En une année, il fait 147 étapes ; où se trouve-t-il à la fin de sa huitième année de travail ?

La figure 4.1 montre que pour revenir à son point de départ, Erwann fait 6 étapes.
S'il fait 147 étapes en un an, en 8 ans, il en fait $147 \times 8 = 1176$ et en 8 ans, pour trouver la ville où il sera arrivé, il faut chercher à quoi est congru 1176 modulo 6.
Or, $1176 \equiv 0\,[6]$; il sera donc de retour sur Vannes !!

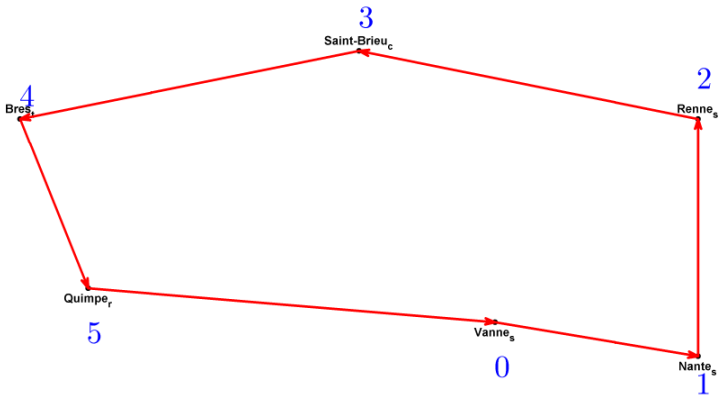

FIGURE 4.1 – Représentation graphique des trajets d'Erwann

Exercice 12 :

1. *Calculer le reste, modulo 7, de* $(32)^{48}$*, de* $(237)^{349}$
   - ▷ *Le reste, modulo 7, de* $(32)^{48}$

     Recherchez le reste de $(32)^{48}$ dans la division par 7, c'est rechercher à quoi est congru $(32)^{48}$ modulo 7
     - ⋆ Tout d'abord, $32 \equiv 4\,[7]$ et donc $32^{48} \equiv 4^{48}\,[7]$
     - ⋆ Nous avons :
     $$4^0 \equiv 1\,[7] \quad 4^1 \equiv 4\,[7] \quad 4^2 \equiv 2\,[7] \quad 4^3 \equiv 1\,[7]$$
     - ⋆ Ainsi :
       - ◇ Si $n \equiv 0\,[3]$ alors $4^n = 4^{3k} = \left(4^3\right)^k$.

         Comme $4^3 \equiv 1\,[7]$, alors $\left(4^3\right)^k \equiv 1^k = 1\,[7]$ et donc $4^n \equiv 1^k = 1\,[7]$
       - ◇ Si $n \equiv 1\,[3]$ alors $n = 3k+1$ et $4^n = 4^{3k+1} = 4^{3k} \times 4$ et $4^n \equiv 4^{3k} \times 4 \equiv 4\,[7]$, c'est à dire $4^n \equiv 4\,[7]$
       - ◇ Si $n \equiv 2\,[3]$ alors $n = 3k+2$ et $4^n = 4^{3k+2} = 4^{3k} \times 4^2$ et $4^n \equiv 4^{3k} \times 4^2 \equiv 2\,[7]$, c'est à dire $4^n \equiv 2\,[7]$

     Comme $48 \equiv 0\,[3]$, nous avons $(32)^{48} \equiv 1\,[7]$. Le reste, modulo 7, de $(32)^{48}$ est donc 1
   - ▷ *Le reste, modulo 7, de* $(237)^{349}$

     Idem, $237 \equiv 6\,[7]$; or $6 \equiv -1\,[7]$ donc : $(237)^{349} \equiv (-1)^{349} \equiv -1 \equiv 6\,[7]$ Le reste, modulo 7, de $(237)^{349}$ est donc 6
2. *Calculer le reste modulo 13 de* $(100)^{100}$

   Pour la résolution, nous prenons la même méthode que ci-dessus :
   $$100 \equiv 9\,[13] \text{ et donc } (100)^{100} \equiv 9^{100}\,[13]$$
   Il faut donc, maintenant étudier les puissance successives de 9 modulo 13
   $$9^0 \equiv 1\,[13] \quad 9^1 \equiv 9\,[13] \quad 9^2 \equiv 3\,[13] \quad 9^3 \equiv 1\,[13]$$
   Ainsi :
   - ◇ Si $n \equiv 0\,[3]$ alors $9^n \equiv 1\,[13]$
   - ◇ Si $n \equiv 1\,[3]$ alors $9^n \equiv 9\,[13]$
   - ◇ Si $n \equiv 2\,[3]$ alors $9^n \equiv 3\,[13]$

   Or, $100 \equiv 1\,[3]$, donc $(100)^{100} \equiv 9^{100} \equiv 9\,[13]$
3. *Montrer que* $2^{70} + 3^{70}$ *est divisible par 13*

→ Nous allons étudier les puissances successives de 2 modulo 13

$$\begin{array}{lllll} 2^0 \equiv 1\,[13] & 2^1 \equiv 2\,[13] & 2^2 \equiv 4\,[13] & 2^3 \equiv 8\,[13] & 2^4 \equiv 3\,[13] \quad 2^5 \equiv 6\,[13] \\ 2^6 \equiv 12\,[13] & 2^7 \equiv 11\,[13] & 2^8 \equiv 9\,[13] & 2^9 \equiv 5\,[13] & 2^{10} \equiv 10\,[13] \quad 2^{11} \equiv 7\,[13] \\ 2^{12} \equiv 1\,[13] & & & & \end{array}$$

En poursuivant le même raisonnement que tout à l'heure, modulo 12, $70 \equiv 10\,[12]$ et donc $2^{70} \equiv 2^{10} \equiv 10\,[13]$

→ Nous allons étudier les puissances successives de 3 modulo 13

$$3^0 \equiv 1\,[13] \quad 3^1 \equiv 3\,[13] \quad 3^2 \equiv 9\,[13] \quad 3^3 \equiv 1\,[13]$$

Comme $70 \equiv 1\,[3]$, nous avons $3^{70} \equiv 3^1 = 3\,[13]$

→ Ainsi, $2^{70} + 3^{70} \equiv 10 + 3 \equiv 0\,[13]$

Donc $2^{70} + 3^{70}$ est divisible par 13

Exercice 13 :

1. *Etudier les congruences de 10^n modulo 9*

   Nous avons $10 \equiv 1\,[13]$, et donc, par compatibilité de la multiplication avec la relation de congruence, pour tout $n \in \mathbb{N}$, nous avons $10^n \equiv 1^n = 1\,[9]$

2. *En déduire qu'un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9*

   En base **dix**, un entier $n \in \mathbb{N}$ sécrit $n = \sum_{k=0}^{p} a_k 10^k$.

   Ainsi, modulo 9, $n \equiv \sum_{k=0}^{p} a_k\,[9]$.

   Et donc, n est divisible par 9 si et seulement si $n \equiv 0\,[9]$, c'est à dire si et seulement si $\sum_{k=0}^{p} a_k \equiv 0\,[9]$.

   Et donc

   Un nombre, écrit en base 10, est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9

Exercice 14 :

Trouver les trois derniers chiffres de $1! + 2! + 3! + \cdots + (2022)! + (2023)! + (2024)!$

Connaître les 3 derniers chiffres d'un entier n, c'est savoir à quoi est congru n modulo 1000.

◇ Regardons, par hasard, à quoi est congru 15! :

$$\begin{aligned} 15! &= 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 \times 13 \times 14 \times 15 \\ &= 2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \times 7 \times 2^3 \times 3^2 \times 2 \times 5 \times 11 \times 2^2 \times 3 \times 13 \times 2 \times 7 \times 3 \times 5 \\ &= 2^{11} \times 3^6 \times 5^3 \times 7^2 \times 11 \times 13 \\ &= \left(2^3 \times 5^3\right) \times K = 1000 \times K \end{aligned}$$

D'où $15! \equiv 0\,[1000]$, et donc, pour $n \geqslant 15$, $n! \equiv 0\,[1000]$, et nous pouvons dire que :

$$1! + 2! + 3! + \cdots + (2022)! + (2023)! + (2024)! \equiv 1! + 2! + 3! + \cdots + (12)! + (13)! + (14)!\,[1000]$$

◇ Et maintenant, que vais-je faire ?... Et bien, je vais regarder les congruences jusque 14!

$$\begin{array}{ll} 1! \equiv 1\,[1000] & 8! \equiv 320\,[1000] \\ 2! \equiv 2\,[1000] & 9! \equiv 880\,[1000] \\ 3! \equiv 6\,[1000] & 10! \equiv 800\,[1000] \\ 4! \equiv 24\,[1000] & 11! \equiv 800\,[1000] \\ 5! \equiv 120\,[1000] & 12! \equiv 600\,[1000] \\ 6! \equiv 720\,[1000] & 13! \equiv 800\,[1000] \\ 7! \equiv 40\,[1000] & 14! \equiv 200\,[1000] \end{array}$$

D'où

$$1!+2!+3!+\cdots+(12)!+(13)!+(14)! \equiv 1+2+6+24+120+720+40+320+880+800+800+600+800+200\,[1000]$$

Et donc $1!+2!+3!+\cdots+(12)!+(13)!+(14)! \equiv 313\,[1000]$
Conclusion : les trois derniers chiffres de $1!+2!+3!+\cdots+(2022)!+(2023)!+(2024)!$ sont 313

Exercice 15 :

1. *Démontrer que* $(\forall k \in \mathbb{N})\,(\forall r \in \mathbb{N})\,\left(7^{4k+r} \equiv 7^r\,[10]\right)$

   Nous avons $7^{4k+r} = 7^{4k} \times 7^r = \left(7^4\right)^k \times 7^r$
   Or, $7^4 = 2401 \equiv 1\,[10]$, et donc $\left(7^4\right)^k \equiv 1^k\,[10] \iff \left(7^4\right)^k \equiv 1\,[10]$
   En conclusion $7^{4k+r} = \left(7^4\right)^k \times 7^r \equiv 7^r\,[10]$
   Ce que nous voulions
2. *Etudier les classes de* 7^n *modulo 4*

   Nous avons :

   $$\text{Si } n = 0 \text{ alors } 7^0 \equiv 1\,[4] \quad \text{Si } n = 1 \text{ alors } 7^1 \equiv 3\,[4] \quad \text{Si } n = 2 \text{ alors } 7^2 \equiv 1\,[4]$$

   Et donc :

   $$\text{Si } n \equiv 0\,[2] \text{ alors } 7^n \equiv 1\,[4] \quad \text{Si } n \equiv 1\,[2] \text{ alors } 7^n \equiv 3\,[4]$$

   En d'autres termes, si n est pair, alors $7^n \equiv 1\,[4]$ et si n est impair, alors $7^n \equiv 3\,[4]$
3. *Quel est le chiffre des unités de* $7^{(7^7)}$ *?*

   Comme toujours dans ces questions, il faut chercher à quoi est congru $7^{(7^7)}$ modulo 10.
   → Nous avons $7^7 \equiv 3\,[4]$, c'est à dire que $7^7 = 4k+3$
   → Et donc, d'après la première question, $7^{(7^7)} \equiv 7^3\,[10]$. Or, comme $7^3 = 343 \equiv 3\,[10]$
   → Donc, le chiffre des unités de $7^{(7^7)}$ est 3

Exercice 16 :

Démontrer que, pour tout $m \in \mathbb{N}$ *et tout* $n \in \mathbb{N}$ *et* $n \geqslant 2$ *:*$(2m+1)^n - (2m+1)^{n-2} \equiv 4m\,\left[4m^2\right]$

Nous allons faire une démonstration par récurrence.

- C'est vrai pour $n = 2$ puisque $(2m+1)^2 - 1 = 4m^2 + 4m$ et nous avons donc bien $(2m+1)^2 - (2m+1)^{2-2} \equiv m\,\left[4m^2\right]$
- Supposons que pour $n \geqslant 2$, nous avons $(2m+1)^n - (2m+1)^{n-2} \equiv 4m\,\left[4m^2\right]$
- Alors, au rang $n+1$, nous avons, et en utilisant l'hypothèse de récurrence :

$$(2m+1)^{n+1} - (2m+1)^{n-1} = (2m+1)\left[(2m+1)^n - (2m+1)^{n-2}\right]$$

Or, par hypothèse de récurrence, $(2m+1)^n - (2m+1)^{n-2} \equiv 4m\,\left[4m^2\right]$ et donc

$$\begin{gathered}(2m+1)^{n+1} - (2m+1)^{n-1} \equiv (2m+1) \times 4m\,\left[4m^2\right] \\ \iff \\ (2m+1)^{n+1} - (2m+1)^{n-1} \equiv 8m^2 + 4m\,\left[4m^2\right] \\ \iff \\ (2m+1)^{n+1} - (2m+1)^{n-1} \equiv 4m + 2 \times 4m^2 \equiv 4m\,\left[4m^2\right]\end{gathered}$$

C'est donc aussi vrai à l'ordre $n+1$
Nous venons donc de montrer que, pour tout $m \in \mathbb{N}$ et tout $n \geqslant 2$, $(2m+1)^n - (2m+1)^{n-2} \equiv 4m\,\left[4m^2\right]$

⇒ Pour démontrer que nous avons $7^n - 7^{n-2} \equiv 12\,[36]$, il suffit de prendre $m = 3$
⇒ Pour démontrer que nous avons $9^n - 9^{n-2} \equiv 16\,[64]$, il suffit de prendre $m = 4$
⇒ Pour démontrer que nous avons $11^n - 11^{n-2} \equiv 12\,[100]$, il suffit de prendre $m = 5$

Exercice 17 :

1. *Montrez que tout nombre entier est congru à la somme de ses chiffres modulo 9*

   Soit $x = \overline{(a_n \cdots a_0)_{10}}$ un nombre écrit en base 10. Alors, $x = \sum_{k=0}^{n} a_k 10^k$

   Or, $10 \equiv 1\,[9]$, et, en utilisant la compatibilité de la multiplication avec la relation de congruence, nous avons, pour tout $k \in \mathbb{N}$: $10^k \equiv 1\,[9]$, et donc $a_k 10^k \equiv a_k\,[9]$. En utilisant la compatibilité de l'addition avec la relation de congruence, nous avons $x = \sum_{k=0}^{n} a_k 10^k \equiv \sum_{k=0}^{n} a_k\,[9]$

   On vient donc de montrer que tout nombre entier est congru à la somme de ses chiffres modulo 9.

2. *Vérifier le calcul suivant en utilisant la preuve par 9 :* $43 \times 164 = 7042$

   Nous avons $43 \equiv 7\,[9]$ et $164 \equiv 2\,[9]$. Donc $43 \times 164 \equiv 7 \times 2 \equiv 5\,[9]$ alors que $7042 \equiv 4\,[9]$; la multiplication est sûrement fausse.

3. *Démontrer la proposition de la preuve par 9*

   Si $a \times b = c$, alors $ab \equiv c\,[9]$. Si nous n'avons pas $ab \equiv c\,[9]$, alors l'opération est sûrement fausse. Mais, ce n'est pas parce que $ab \equiv c\,[9]$ que la multiplication est correcte :
   Si nous trouvons $43 \times 164 = 7142$, nous avons toujours $43 \times 164 \equiv 5\,[9]$, $7142 \equiv 5\,[9]$, mais notre multiplication est fausse *(car, en fait :* $43 \times 164 = 7052$*)* .

En fait, la preuve par 9 ne dit pas si une opération est exacte. Il faut comprendre que si la preuve par 9 n'est pas vérifiée, alors la multiplication est fausse.

Exercice 18 :

Considérons l'anneau $\mathbb{Z}/33\mathbb{Z}$

1. *Soit* $f : \mathbb{Z}/33\mathbb{Z} \longrightarrow \mathbb{Z}/33\mathbb{Z}$ *définie par :*

$$\begin{cases} f : \mathbb{Z}/33\mathbb{Z} & \longrightarrow & \mathbb{Z}/33\mathbb{Z} \\ x & \longmapsto & f(x) = 17x + 9 \end{cases}$$

   ▷ *Trouver l'inverse de 17 dans l'anneau* $\mathbb{Z}/33\mathbb{Z}$

   Il suffit de remarquer que $2 \times 17 = 34 \equiv 1\,[33]$.
   2 est donc l'inverse de 17 dans l'anneau $\mathbb{Z}/33\mathbb{Z}$

   ▷ *Résoudre, dans* $\mathbb{Z}/33\mathbb{Z}$ *l'équation* $f(x) = 0$

   Nous avons :

$$f(x) = 0 \iff 17x + 9 \equiv 0\,[33] \iff 17x \equiv -9 \equiv 24\,[33] \iff 2 \times 17x \equiv 48\,[33] \iff x \equiv 15\,[33]$$

   La solution, dans $\mathbb{Z}/33\mathbb{Z}$, de l'équation $f(x) = 0$ est donc $x = 15$

   ▷ *Montrer que* f *est une bijection dont on donnera la bijection réciproque*

   ▷ f est injective
   Soient $x_1 \in \mathbb{Z}/33\mathbb{Z}$ et $x_2 \in \mathbb{Z}/33\mathbb{Z}$ tels que $f(x_1) = f(x_2)$; alors :

$$\begin{aligned} f(x_1) = f(x_2) &\iff 17x_1 + 9 \equiv 17x_2 + 9\,[33] \\ &\iff 17x_1 \equiv 17x_2\,[33] \\ &\iff 2 \times 17x_1 \equiv 2 \times 17x_2\,[33] \\ &\iff x_1 \equiv x_2\,[33] \end{aligned}$$

   Ce qui veut dire que, dans $\mathbb{Z}/33\mathbb{Z}$, nous avons $x_1 = x_2$.
   f est donc injective

   ▷ f est surjective

Soit $y \in \mathbb{Z}/33\mathbb{Z}$; existe-t-il $x \in \mathbb{Z}/33\mathbb{Z}$ tel que $y = f(x)$? S'il existe, alors :

$$\begin{array}{rcl} y = f(x) & \Longleftrightarrow & y = 17x + 9 \Longleftrightarrow y \equiv 17x + 9\,[33] \\ & \Longleftrightarrow & y - 9 \equiv 17x\,[33] \\ & \Longleftrightarrow & 2 \times (y - 9) \equiv 2 \times 17x\,[33] \\ & \Longleftrightarrow & x \equiv 2y - 18\,[33] \\ & \Longleftrightarrow & x \equiv 2y + 15\,[33] \end{array}$$

f il existe donc $x \in \mathbb{Z}/33\mathbb{Z}$ et $x = 2y + 15$ tel que $y = f(x)$.
f est donc surjective
f étant injective et surjective, est donc bijective et nous avons $f^{-1}(x) = 2x + 15$

2. *Soit $g : \mathbb{Z}/33\mathbb{Z} \longrightarrow \mathbb{Z}/33\mathbb{Z}$ définie par :*

$$\left\{ \begin{array}{rcl} g : \mathbb{Z}/33\mathbb{Z} & \longrightarrow & \mathbb{Z}/33\mathbb{Z} \\ x & \longmapsto & g(x) = 22x + 7 \end{array} \right.$$

Quel est l'ensemble des images des éléments de $\mathbb{Z}/33\mathbb{Z}$ par g ?

Cette fois ci, ce n'est plus le même topo puisque 22 est un véritable diviseur de 0 dans $\mathbb{Z}/33\mathbb{Z}$; en effet, nous avons, dans $\mathbb{Z}/33\mathbb{Z}$

$$3 \times k \times 22 = 3 \times k \times 2 \times 11 = 2k \times 33 = 0 \text{ pour } k = 1, \cdots, 10$$

Ainsi, pour $k = 0, \cdots, 10$,
▷ $g(3k) = 22 \times 3k + 7 = 7$
▷ $g(3k + 1) = 22 \times (3k + 1) + 7 = 29$
▷ $g(3k + 2) = 22 \times (3k + 2) + 7 = 17$
Ainsi, $g(\mathbb{Z}/33\mathbb{Z}) = \{7, 17, 29\}$ et g n'est ni injective, ni surjective