Index des démonstrations rédigées

Chapitre 20 — Structures algébriques usuelles

Chapitre 21 — Arithmétique

Exercice 1 23-01

On considère deux éléments a et b de l'anneau $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$.

L'élément d est un pgcd de a et b si, et seulement si, il existe deux éléments α et β premiers entre eux de A tel que

$$a = d\alpha \qquad \text{et} \qquad b = d\beta.$$

Exercice 2 23-02

Dans l'anneau $A = \mathbb{Z}$ ou dans l'anneau $A = \mathbb{K}[X]$, on considère des éléments $x_1, x_2, \ldots, x_n$ deux à deux premiers entre eux.

On pose $x = x_1 x_2 \cdots x_n$ et

$$\forall\, 1 \leqslant k \leqslant n, \qquad y_k = \prod_{\substack{1 \leqslant i \leqslant n \\ i \neq k}} x_i$$

de telle sorte que

$$\forall\, 1 \leqslant k \leqslant n, \quad x = x_k y_k \quad \text{et} \quad x_k \wedge y_k = 1.$$

Alors les éléments $y_1, \ldots, y_n$ sont premiers dans leur ensemble : il existe des éléments $a_1, a_2, \ldots, a_n$ de A tels que

$$\sum_{k=1}^{n} a_k y_k = 1.$$

Exercice 3 23-03

Soit $n \geqslant 2$, un entier naturel. On note N, le nombre de diviseurs de n (compris entre 1 et n inclus) et P, le produit des diviseurs de n.

1. Le nombre N est impair si, et seulement si, n est un carré parfait.

2. En regroupant deux par deux les diviseurs de n dans le produit P^2 pour former N produits égaux à n, on obtient

$$P^2 = n^N.$$

Exercice 4 23-04

Calculer le pgcd de 1683 et 969. En déduire les couples $(x, y) \in \mathbb{Z}^2$ qui vérifient les équations suivantes :

1. $969x - 1683y = 51$ (on vérifiera que $(7, 4)$ est une solution)

2. $969x - 1683y = 102$

3. $969x - 1683y = 84$

Exercice 5 23-05

1. Déterminer les couples $(x, y) \in \mathbb{Z}^2$ tels que

$$23x + 46y = 3.$$

2. Déterminer les couples $(x, y) \in \mathbb{Z}^2$ tels que

$$23x + 56y = 3.$$

Exercice 6 23-06

1. On considère l'équation

$$13x - 7y = 1$$

d'inconnue $(x, y) \in \mathbb{Z}^2$.

1. a. En remarquant que $x + 1$ est divisible par 7, déterminer une solution particulière (x_0, y_0) avec $0 \leqslant x_0 \leqslant 7$.

1. b. En déduire les autres solutions.

2. Résoudre de même l'équation $13x - 7y = 2$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

Exercice 7 23-07

On considère deux entiers naturels a et b et on note $d = a \wedge b$. Déterminer le pgcd des entiers

$$a' = 13a + 5b \quad \text{et} \quad b' = 5a + 2b.$$

Exercice 8 23-08

Soient n, un entier naturel non nul, et p, un entier premier (distinct de n). Déterminer les nombres complexes z qui vérifient les deux équations suivantes.

$$z^n + 1 = 0 \qquad z^p + 1 = 0$$

On fera intervenir le pgcd $d = n \wedge p$.

Exercice 9 23-09

1. Étudier, suivant la valeur de l'entier n, le reste de la division euclidienne par 6 de l'entier 5^n.

2. Pour quelles valeurs de n le nombre $A_n = 5^n + 5n + 1$ est-il divisible par 6 ?

Exercice 10 23-10

1. Pour tout $n \in \mathbb{N}$, déterminer le reste modulo 7 de 5^n.

2. En déduire le reste modulo 7 de 1972^{57} et les entiers n pour lesquels 1972^n est congru à 4 modulo 7.

Exercice 11 23-11

Déterminer le reste de 8^{1974} modulo 5.

Exercice 12 23-12

Pour tout entier naturel n, l'entier

$$u_n = 3^{n+3} - 4^{4n+2}$$

est divisible par 11.

Exercice 13 23-13

Déterminer les entiers naturels n tels que

$$5^{2n} + 5^n \equiv 0 \pmod{13}.$$

Exercice 14 23-14

Déterminer les restes modulo 13 des entiers 5^k pour tout entier $0 \leqslant k < 5$. En déduire que l'entier

$$u_n = 31^{4n+1} + 18^{4n-1}$$

est divisible par 13 pour tout entier $n \in \mathbb{N}^*$.

Exercice 15 23-15

Pour tout $n \in \mathbb{N}$, l'entier n^2 est congru à 0, à 1 ou à 4 modulo 8. En déduire les entiers relatifs x tels que

$$(5x+3)^2 - 1 = 0 \pmod 8.$$

Exercice 16 23-16

Résoudre l'équation $x^2 + x + 6 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$.

Exercice 17 23-17

Résoudre les systèmes

$$\begin{cases} 2x - 4y = 2 \\ x + 5y = 2 \end{cases} \qquad \begin{cases} 3x + 2y = 1 \\ x - y = 2 \end{cases}$$

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

Exercice 18 23-18

Dresser la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$. Résoudre le système

$$\begin{cases} 3x + y = 3 \\ x + y = 1 \end{cases}$$

dans $(\mathbb{Z}/4\mathbb{Z})^2$.

Exercice 19 23-19

Dresser la table de multiplication de l'anneau $\mathbb{Z}/6\mathbb{Z}$. En déduire les solutions de l'équation $2x = 0$ dans $\mathbb{Z}/6\mathbb{Z}$ et résoudre le système suivant dans $(\mathbb{Z}/6\mathbb{Z})^2$.

$$\begin{cases} 2x + 2y = 4 \\ 5x + 3y = 3 \end{cases}$$

Exercice 20 23-20

1. Dresser la table de multiplication de l'anneau $\mathbb{Z}/5\mathbb{Z}$.
2. En déduire les solutions des équations

$$3x + 4 = 0 \qquad 2x + 1 = 0$$

dans $\mathbb{Z}/5\mathbb{Z}$, puis résoudre le système suivant dans $(\mathbb{Z}/5\mathbb{Z})^2$.

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

3. Démontrer que l'équation $x^2 + x + 1 = 0$ n'a pas de solution dans $\mathbb{Z}/5\mathbb{Z}$.

Exercice 21 23-21

Résoudre l'équation

$$x^3 = x$$

dans $\mathbb{Z}/12\mathbb{Z}$, puis dans $\mathbb{Z}/11\mathbb{Z}$.

Exercice 22 23-22

On considère l'équation

$$x^2 + 2x - 3 = 0.$$

1. Résoudre l'équation dans $\mathbb{Z}/7\mathbb{Z}$.
2. Déterminer les diviseurs de zéro dans $\mathbb{Z}/21\mathbb{Z}$. En déduire les solutions de l'équation dans $\mathbb{Z}/21\mathbb{Z}$.

Exercice 23 23-23

1. Résoudre l'équation

$$x^2 - 3x + 2 = 0$$

dans $\mathbb{Z}/5\mathbb{Z}$.
2. En déduire les entiers relatifs n tels que le reste de la division euclidienne de $n^2 - 3n$ par 5 soit égal à 3.

Exercice 24 23-24

1. Déterminer les entiers relatifs n tels que

$$n^3 + 1 = 0 \pmod 7$$

puis les entiers relatifs n tels que

$$n^3 - 1 = 0 \pmod 7.$$

2. Quel que soit l'entier relatif n, l'entier

$$u_n = n(n^3+1)(n^3-1)$$

est divisible par 42.

Exercice 25 23-25

On pose ici $\mathbb{K} = \mathbb{Z}/3\mathbb{Z}$ et on considère l'équation

$$x^2 + px + q = 0$$

où les coefficients p et q ainsi que l'inconnue x appartiennent au corps $\mathbb{K}$.
1. Déterminer successivement les couples $(p,q) \in \mathbb{K}^2$ tels que l'équation étudiée admette 0 (resp. 1, resp. 2) pour solution.
2. Pour quels couples (p,q) cette équation n'admet-elle aucune solution ?

Exercice 26 23-26

Soient a et b, deux entiers naturels donnés. On cherche les entiers $x \in \mathbb{Z}$ qui vérifient le système suivant.

$$\begin{cases} x \equiv a \pmod 9 \\ x \equiv b \pmod{11} \end{cases}$$

Vérifier que toutes les solutions sont congrues à un même entier x_0 modulo 99. En déduire l'ensemble des solutions du système.

Exercice 27 23-27

On considère l'ensemble E des entiers relatifs x qui vérifient simultanément les relations suivantes.

$$x \equiv 2 \pmod 3 \qquad x \equiv 2 \pmod 5$$
$$x \equiv 2 \pmod 7 \qquad x \equiv 2 \pmod 9$$

1. Donner la forme générale des éléments de E.
2. Déterminer les éléments de E qui sont compris (au sens large) entre -1000 et -500.
3. Quel est le pgcd de deux éléments consécutifs de E ?

Exercice 28 23-28

On note S, l'ensemble des entiers relatifs x tels que

$$x \equiv 1 \pmod 3 \quad \text{et} \quad x \equiv 2 \pmod 5.$$

1. Déterminer un entier $x \in S$ compris entre 0 et 10.
2. Démontrer que

$$\forall\, (a,b) \in S \times S, \quad (a-1) \equiv (a-1)(b-1) \pmod{15}.$$

3. Déterminer les éléments de S.

Exercice 29 23-29

Résoudre le système suivant d'inconnue $x \in \mathbb{Z}$.

$$\begin{cases} 3x \equiv 1 \pmod 4 \\ 2x \equiv 4 \pmod 5 \end{cases}$$

Exercice 30 23-30

Pour tout entier $n \geqslant 2$, on note π_n, le nombre d'entiers premiers compris (au sens large) entre 1 et n et, pour tout entier $n \geqslant 1$, on note p_n, le n-ième entier premier.

On a donc, par exemple,

$$p_1 = 2, p_2 = 3, p_3 = 5, p_5 = 7 \ldots \quad \pi_2 = 1, \pi_3 = \pi_4 = 2, \pi_5 = 3, \pi_6 = \pi_7 = 4 \ldots$$

On admet le *Théorème des nombres premiers* qui énonce :

$$\pi_n \underset{n\to+\infty}{\sim} \frac{n}{\ln n}.$$

En déduire un équivalent de p_n lorsque n tend vers $+\infty$.

Exercice 31 23-31

Un polynôme $P \in \mathbb{K}[X]$ est divisible par son polynôme dérivé P' si, et seulement si, il existe deux scalaires α, β et un entier $n \geqslant 1$ tels que $P = \alpha(X-\beta)^n$.

Exercice 32 23-32

Soit $p \geqslant 2$, un nombre premier. La **valuation p-adique** d'un entier m est, par définition, égale à k si, et seulement si, p^k divise m et p^{k+1} ne divise pas m. Autrement dit, $v_p(m) \geqslant k$ si, et seulement si, p^k divise m.

1. Pour tout entier $n \in \mathbb{N}^*$ et tout nombre premier p, la valuation p-adique de $n!$ est égale à

$$\sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

2. Si n est assez grand, l'écriture décimale de $n!$ se termine par une suite de 0. Combien ?

Exercice 33 23-33

On dit qu'un entier n est **sans facteur carré** lorsqu'il peut se factoriser sous la forme

$$n = p_1 \times p_2 \times \cdots \times p_r$$

où les p_k sont des nombres premiers deux à deux distincts.

Pour tout entier $n \in \mathbb{N}^*$, on pose $\mu(n) = 0$ lorsqu'il existe un nombre premier p tel que p^2 divise n et $\mu(n) = (-1)^r$ lorsque n est le produit de r nombres premiers deux à deux distincts.

1. On considère la factorisation d'un entier $n \geqslant 2$ en produits de facteurs premiers :

$$n = \prod_{k=1}^{s} p_k^{\alpha_k}$$

où les α_k sont des entiers naturels non nuls.

Alors l'entier n admet 2^s diviseurs sans facteur carré et

$$\sum_{d|n} \mu(d) = \sum_{r=0}^{s} \binom{s}{r} (-1)^r = 0.$$

2. On définit une partition dénombrable de $I = \mathbb{N}^* \times \mathbb{N}^*$ en posant

$$\forall\, n \in \mathbb{N}^*, \quad I_n = \{(p,q) \in I \,:\, pq = n\}.$$

On en déduit que

$$\left(\sum_{p=1}^{+\infty} \frac{1}{p^2}\right)\left(\sum_{q=1}^{+\infty} \frac{\mu(q)}{q^2}\right) = \sum_{n=1}^{+\infty}\left(\sum_{d|n} \frac{\mu(d)}{n^2}\right) = 1.$$

Exercice 34 23-34

Le système

$$\begin{cases} 6x + 7y = 30 \\ 3x - 7y = 0 \end{cases}$$

admet $(28, 12)$ pour seule solution dans $\mathbb{Z}/37\mathbb{Z}$.

Exercice 35 23-35

Soient $I = \mathbb{N}^* \times \mathbb{N}^*$ et

$$\forall\, n \in \mathbb{N}^*, \quad I_n = \{(p,q) \in I \,:\, p \wedge q = n\}.$$

Alors $(I_n)_{n\geqslant 1}$ est une partition de I et comme l'application

$$[(\alpha, \beta) \mapsto (n\alpha, n\beta)]$$

est une bijection de I_1 sur I_n, alors

$$\sum_{(p,q)\in I} \frac{1}{p^2q^2} = \left(\sum_{(p,q)\in I_1} \frac{1}{p^2q^2}\right)\left(\sum_{n=1}^{+\infty} \frac{1}{n^4}\right).$$

Exercice 36 23-36

Un entier $n \geqslant 2$ est un **nombre de Carmichael** lorsque

$$\forall\, a \in \mathbb{N}^*, \quad a^n = a \pmod n$$

sans être un nombre premier.

1. Rédiger une procédure en langage Python qui vérifie si un entier n donné est, ou non, un nombre de Carmichael.

2. On suppose qu'un nombre de Carmichael n admet un facteur carré : il existe donc deux entiers p et m tels que $n = p^2m$. Avec $a = 1 + pm$, on obtient

$$a^n = 1 \pmod n = 1 + pm \pmod n,$$

ce qui est absurde : les nombres de Carmichael n'admettent pas de facteur carré.

Exercice 37 23-37

Il y a 24 éléments inversibles dans $\mathbb{Z}/78\mathbb{Z}$.

Exercice 38 23-38

Soit $\varphi : A \to B$, un isomorphisme d'anneaux.
La bijection réciproque φ^{-1} est un morphisme d'anneaux de $(B, \oplus, \otimes)$ dans $(A, +, \star)$.

Exercice 39 23-39

Soit $(A, +, *, \cdot)$, une algèbre. Le **commutant** C_a d'un élément $a \in A$, défini par

$$C_a = \{b \in A : a * b = b * a\},$$

est une sous-algèbre de A (pas nécessairement commutative).

Exercice 40 23-40

On sait que $(\mathbb{R}_+^*, \times)$ est un groupe. Démontrer que l'ensemble G défini par

$$G = \{x + \sqrt{3}y : x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$$

est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

Exercice 41 23-41

Soit φ, un morphisme d'anneaux de $(A, +, \star)$ dans $(B, +, \otimes)$.
1. L'image de φ est un sous-anneau de $(B, +, \otimes)$.
2. Un élément $x \in A$ est inversible si, et seulement si, son image $\varphi(x) \in B$ est inversible.

Exercice 42 23-42

Si $\varphi : A \to B$ est un isomorphisme d'algèbres, alors $a \in A$ et $\varphi(a) \in B$

Exercice 43 23-43

Un entier $a \in \mathbb{Z}$ est **congru** à $b \in \mathbb{Z}$ modulo $n \in \mathbb{N}^*$ si, et seulement si, il existe un entier $q \in \mathbb{Z}$ tel que

$$a = qn + b.$$

✍ *D'après* `https://www.cnrtl.fr/definition/congru`, *ce qui est* congru *"convient exactement", est "calculé au plus juste".*

La relation de congruence modulo $n \in \mathbb{N}^*$ est une relation d'équivalence sur $\mathbb{Z}$.

Exercice 44 dm1608

Une racine n-ième de l'unité est une **racine primitive** lorsqu'elle engendre le groupe $\mathbb{U}_n$.
Soit $n \geqslant 1$, fixé. Pour $0 \leqslant k < n$, on pose

$$\zeta_k = e^{2ik\pi/n} \in \mathbb{U}_n$$

et on note G_k, le sous-groupe de $\mathbb{U}_n$ engendré par ζ_k :

$$G_k = \langle \zeta_k \rangle = \{\zeta_k^m,\ m \in \mathbb{Z}\}.$$

1. Le nombre complexe ζ_k est une racine n-ième primitive si, et seulement si, les entiers k et n sont premiers entre eux.
2. Décrire le sous-groupe de $\mathbb{U}_n$ engendré par ζ_k.

Exercice 45 rms128-198

Soit G, un sous-groupe du groupes des fonctions affines (non constantes) de $\mathbb{R}$ dans $\mathbb{R}$ tel que toute fonction de G possède un point fixe.
Démontrer qu'il existe un réel ω qui est fixe pour tous les éléments de G.

Exercice 46 rms128-436

On note φ, l'indicatrice d'Euler. Trouver les $n \in \mathbb{N}^*$ tels que $\varphi(n)$ divise n.

Exercice 47 rms128-454

Soient A et B, deux matrices de $\mathfrak{M}_n(\mathbb{Z})$. On suppose que leurs déterminants, respectivement notés a et b, sont premiers entre eux. Démontrer qu'il existe deux matrices U et V dans $\mathfrak{M}_n(\mathbb{R})$ telles que

$$AU + BV = I_n.$$

Exercice 48 rms130-468

1. Soit φ, un isomorphisme du groupe G sur le groupe H. Démontrer que x est un générateur de G si, et seulement si, $\varphi(x)$ est un générateur de H.
2. Démontrer qu'un sous-groupe d'un groupe monogène est lui-même monogène.

Exercice 49 rms130-469

Soient $n \in \mathbb{N}^*$ et $\gamma \in \mathfrak{S}_n$, un cycle. Écrire γ comme un produit de transpositions.

Exercice 50 rms130-470

Soit $n \in \mathbb{N}^*$. Déterminer les morphismes de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Exercice 51 rms130-471

Soit G, un sous-groupe fini de $GL_2(\mathbb{C})$ tel que $G \cap SL_2(\mathbb{C}) = \{I_2\}$. Démontrer que G est cyclique.

Exercice 52 rms130-1127

On considère un **nombre algébrique** α, c'est-à-dire un nombre complexe qui est racine d'un polynôme non nul à coefficients dans $\mathbb{Z}$.
1. Démontrer qu'il existe un, et un seul, polynôme $\Pi \in \mathbb{Q}[X]$, unitaire et irréductible sur $\mathbb{Q}$, tel que $\Pi(\alpha) = 0$. On notera d, le degré du polynôme Π.
2. On pose

$$\mathbb{Q}_{d-1}[\alpha] = \{P(\alpha),\ P \in \mathbb{Q}_{d-1}[X]\},$$
$$\mathbb{Q}[\alpha] = \{P(\alpha),\ P \in \mathbb{Q}[X]\}.$$

Démontrer que $\mathbb{Q}[\alpha] = \mathbb{Q}_{d-1}[\alpha]$.
3. Démontrer que $\mathbb{Q}_{d-1}[\alpha]$ est un sous-corps de $\mathbb{C}$.

Exercice 53 rms130-1128

Soient m et n, deux entiers naturels non nuls.

1. Démontrer que : si m divise n, alors $X^m - 1$ divise $X^n - 1$.

2. Étudier la réciproque.

Exercice 54 rms133-984

Soit $(G, \cdot)$, un groupe commutatif fini de neutre e et de cardinal n. On écrit

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

la décomposition du cardinal n en produit de facteurs premiers (les α_i sont des entiers naturels non nuls). Pour alléger les notations, on posera $\pi_i = p_i^{\alpha_i}$.

Pour tout entier $d \in \mathbb{N}^*$, on pose

$$G_d = \{x \in G \,:\, x^d = e\}.$$

1. Vérifier que G_d est un sous-groupe de $(G, \cdot)$.

2. On suppose que l'entier d est premier à n. Que dire du sous-groupe G_d ?

3. On considère le groupe produit

$$\Gamma = \prod_{i=1}^{r} G_{\pi_i}.$$

Démontrer que l'application f définie par

$$\forall\, (x_1, \dots, x_r) \in \Gamma, \qquad f(x_1, \dots, x_r) = \prod_{i=1}^{r} x_i$$

est un isomorphisme du groupe produit Γ sur le groupe G.

4. On suppose que $\#(G_d) \leqslant d$ pour tout diviseur d de n.

4. a. Démontrer que, pour tout $1 \leqslant i \leqslant r$, il existe un élément g_i d'ordre π_i dans G.

4. b. En déduire que le groupe $(G, \cdot)$ est cyclique.

Exercice 55 rms135-489

Soit $n \in \mathbb{N}^*$. Déterminer et dénombrer les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 56 rms135-490

Soit $(G, *)$, un groupe fini d'élément neutre e. On suppose que

$$\forall\, x \in G, \qquad x^2 = e.$$

1. Le groupe $(G, *)$ est abélien.

2. Soient H, un sous-groupe strict de G et $a \in G \setminus H$. On pose

$$aH = \{a * x,\ x \in H\}.$$

2. a. Les ensembles H et aH ont même cardinal.

2. b. Les ensembles H et aH sont disjoints.

2. c. L'ensemble $H \cup aH$ est un sous-groupe de G.

3. Le cardinal de G est une puissance de 2.

4. Calculer le produit des éléments de G.

Exercice 57 rms135-492

Soit $(G, \cdot)$, un groupe abélien. On considère deux éléments x et y de G en supposant que l'ordre $a \in \mathbb{N}^*$ de x et l'ordre $b \in \mathbb{N}^*$ de y sont premiers entre eux.

1. Démontrer que l'ordre de xy est égal à ab.

2. Démontrer que le sous-groupe $\langle xy \rangle$ engendré par le produit xy est l'ensemble

$$H = \{x^m \cdot y^n,\ 0 \leqslant m < a, 0 \leqslant n < b\}.$$

Exercice 58 rms135-493

Soit G, un ensemble muni d'une loi de composition interne associative $*$. On suppose qu'il existe un élément $e \in G$ tel que

$$\forall\, x \in G, \quad x * e = x$$

et que

$$\forall\, x \in G,\ \exists\, x' \in G, \quad x * x' = e.$$

Démontrer que $(G, *)$ est un groupe.

Structures algébriques (Solutions)

Solution 1 — 23-01

Si d est un pgcd de a et b, alors

$$aA + bA = dA \tag{1}$$

donc $aA \subset dA$ et $bA \subset dA$. Ainsi, d divise a et b, donc il existe deux éléments α et β de A tels que

$$a = d\alpha \qquad \text{et} \qquad b = d\beta.$$

Mais on déduit aussi de (1) qu'il existe deux éléments u et v de A tels que

$$d = au + bv = d(\alpha u + \beta v).$$

▶ Si $d \neq 0$, alors on peut simplifier par d et en déduire que

$$\alpha u + \beta v = 1.$$

D'après le Théorème de Bézout, les éléments α et β sont premiers entre eux.

✍ *Dans un anneau intègre (comme $\mathbb{Z}$ ou comme $\mathbb{K}[X]$), on peut simplifier par tout facteur non nul – qu'il soit inversible ou non.*

▶ Si $d = 0$, alors $a = b = 0$ et on peut choisir $\alpha = \beta = 1$.

✍ *Ce second cas est sans aucun intérêt mathématique, mais ce n'est pas une raison pour l'ignorer.*

❧ Réciproquement, supposons qu'il existe deux éléments α et β de A, premiers entre eux, tels que $a = d\alpha$ et $b = d\beta$. Il est alors clair que d divise a et b, donc

$$aA \subset dA \qquad \text{et} \qquad bA \subset dA.$$

Ainsi, dA est un idéal qui contient les deux idéaux aA et bA, donc

$$aA + bA \subset dA.$$

✍ *Si I et J sont deux idéaux de A, alors $I + J$ est le plus petit idéal de A (pour la relation d'ordre partiel $\subset$) qui contienne à la fois I et J.*

Par ailleurs, d'après le Théorème de Bézout, il existe deux éléments u et v de A tels que

$$\alpha u + \beta v = 1.$$

On en déduit que

$$d = d(\alpha u + \beta v) = au + bv \in aA + bA$$

et donc que

$$dA \subset aA + bA.$$

✍ *L'idéal dA engendré par d est le plus petit idéal (pour la relation $\subset$) qui contienne d. Il est donc contenu dans $aA + bA$, qui est un idéal qui contient d.*

On a ainsi démontré que $dA = aA + bA$ et donc que d était un pgcd de a et b.

Solution 2 — 23-02

On procède par récurrence sur n.

❧ **Initialisation pour** $n = 2$
Si x_1 et x_2 sont premiers entre eux, alors $y_1 = x_2$ et $y_2 = x_1$ sont premiers entre eux.

❧ **Hérédité**
On suppose que, pour un certain entier $n \geqslant 2$, si les éléments $x_1, \ldots, x_n$ sont deux à deux premiers entre eux, alors les éléments $y_1, \ldots, y_n$ sont premiers dans leur ensemble.

On considère alors un élément x_{n+1} tels que $x_1, x_2, \ldots, x_n$ et x_{n+1} soient deux à deux premiers entre eux et on pose

$$\forall\, 1 \leqslant k \leqslant n, \quad \overline{y_k} = \prod_{\substack{1 \leqslant i \leqslant n+1 \\ i \neq k}} x_i = y_k \cdot x_{n+1} \qquad \text{et} \qquad \overline{y_{n+1}} = \prod_{\substack{1 \leqslant i \leqslant n+1 \\ i \neq n+1}} x_i = x.$$

Par hypothèse, x_{n+1} est premier à x_k pour tout $1 \leqslant k \leqslant n$, donc x_{n+1} est premier à leur produit :

$$x_{n+1} \wedge \overline{y_{n+1}} = 1.$$

Il existe donc deux éléments a_{n+1} et b_{n+1} de A tels que

$$b_{n+1}x_{n+1} + a_{n+1}\overline{y_{n+1}} = 1.$$

Par hypothèse de récurrence, les éléments $y_1, \ldots, y_n$ sont premiers dans leur ensemble et, d'après le Théorème de Bézout, il existe deux éléments $a_1, \ldots, a_n$ tels que

$$\sum_{k=1}^{n} a_k y_k = 1.$$

On en déduit que

$$1 = \left(\sum_{k=1}^{n} a_k y_k\right) b_{n+1}x_{n+1} + a_{n+1}\overline{y_{n+1}} = \sum_{k=1}^{n} a_k b_{n+1}\overline{y_k} + a_{n+1}\overline{y_{n+1}}$$

et donc (réciproque du Théorème de Bézout) que les éléments $\overline{y_1}, \ldots, \overline{y_n}, \overline{y_{n+1}}$ sont premiers dans leur ensemble.

✍ *Ce Théorème sert d'une part à démontrer le Lemme chinois des restes (dont la mise en œuvre pratique repose, comme cette démonstration, sur la relation de Bézout) et d'autre part à démontrer le Théorème de décomposition des noyaux.*

Solution 3 — 23-03

1.

✍ *La première question repose sur la* ***décomposition d'un entier en produit de facteurs premiers****. Il est important de bien comprendre en quels sens cette décomposition est unique. (Veuillez noter le pluriel.)*

❧ *Cette décomposition est naturellement unique quand on l'écrit sous la forme d'un produit infini où apparaissent tous les nombres premiers : pour tout entier naturel $n \in \mathbb{N}^*$, il existe une, et une seule, famille $(v_p)_{p \in \mathscr{P}}$ d'entiers naturels presque tous nuls tels que*

$$n = \prod_{p \in \mathscr{P}} p^{v_p}.$$

La condition "presque tous nuls" signifie qu'il n'existe qu'un nombre fini de nombres premiers p de valuation non nulle ($v_p \geqslant 1$) et, puisqu'il n'y a donc qu'un nombre fini de facteurs p^{v_p} différents de 1, cette condition assure l'existence du produit.

❧ *Une autre écriture est possible et consiste à ne faire apparaître que les facteurs premiers nécessaires à la décomposition de n, c'est-à-dire ceux dont la valuation est supérieure à 1. Dans ce cas, on écrit*

$$n = \prod_{k=1}^{d} p_k^{\alpha_k}$$

où les α_k sont des entiers au moins égaux à 1 (les valuations), les p_k sont des nombres premiers ($p_k \in \mathscr{P}$) deux à deux distincts et d, un entier naturel qui donne le nombre de facteurs premiers de n (qui dépend donc de n et est par exemple nul pour $n = 1$).

Cette expression est alors unique à l'ordre près :

$$\forall\, \sigma \in \mathfrak{S}_d, \quad \prod_{k=1}^{d} p_k^{\alpha_k} = \prod_{k=1}^{d} p_{\sigma(k)}^{\alpha_{\sigma(k)}}$$

mais je n'imagine pas qu'on puisse être assez agité du bonnet pour s'aventurer à de telles permutations.

❧ *Si on ne se limite pas aux seuls facteurs premiers nécessaires, la décomposition de n n'est plus unique :*

$$n = \prod_{k=1}^{d} p_k^{\alpha_k} = \prod_{k=1}^{d} p_k^{\alpha_k} \times \prod_{k=d+1}^{d+q} p_k^{0}.$$

Mais là encore, je ne vois pas pour quelle raison on s'amuserait à faire apparaître des facteurs fantômes.

❧ *En revanche, on peut décider arbitrairement de choisir une famille finie de nombres premiers deux à deux distincts $(p_k)_{1\leqslant k\leqslant d}$ et de considérer tous les entiers naturels non nuls n qu'on peut décomposer à l'aide de ces seuls nombres premiers (et seulement ces entiers n).*

On s'intéresse alors à un ensemble $E \subset \mathbb{N}^*$ tel que

$$\forall\, n \in E,\ \exists\,!\,(\alpha_k)_{1\leqslant k\leqslant d} \in \mathbb{N}^d, \quad n = \prod_{k=1}^{d} p_k^{\alpha_k}.$$

Cette factorisation est alors unique car les facteurs premiers qui interviennent ont été fixés une fois pour toutes.

❧ *En résumé, la décomposition d'un entier en produit de facteur premier est unique dès lors qu'on impose une contrainte sur les nombres premiers qui apparaissent :*

- *ils doivent tous apparaître lorsque le produit est indexé par $\mathscr{P}$ (et ils apparaissent alors presque tous avec une valuation nulle) ;*
- *on se restreint aux seuls facteurs nécessaires à la décomposition de n (ils apparaissent alors tous avec une valuation non nulle) ;*
- *on choisit une famille finie $(p_k)_{1\leqslant k\leqslant d}$ de nombres premiers deux à deux distincts et on se limite aux entiers qu'on peut factoriser à l'aide des nombres qu'on a choisis.*

On considère un entier naturel non nul n et on le décompose en produit de facteurs premiers :

$$n = \prod_{k=1}^{d} p_k^{\alpha_k}.$$

On sait alors qu'un entier m est un diviseur de n si, et seulement si, il existe une famille d'entiers $(\beta_k)_{1\leqslant k\leqslant d}$ tels que

$$m = \prod_{k=1}^{d} p_k^{\beta_k} \quad \text{et} \quad \forall\, 1 \leqslant k \leqslant d, \quad 0 \leqslant \beta_k \leqslant \alpha_k.$$

❧ L'unicité de la décomposition de m en produit de facteurs premiers assure qu'il y a autant de diviseurs de n que de familles $(\beta_k)_{1\leqslant k\leqslant d}$.

✍ *Ici, on a imposé une contrainte sur la décomposition de m : utiliser tous les facteurs qui ont servi à décomposer n et seulement ces facteurs. Il y a donc bien unicité de la décomposition de m.*

Pour chaque indice k, il y a donc $(\alpha_k + 1)$ choix possibles pour β_k, il y a donc

$$N = \prod_{k=1}^{d} (\alpha_k + 1)$$

diviseurs de n.

✍ *Si un galopin s'amusait à introduire des facteurs fantômes dans la décomposition de n (c'est-à-dire des facteurs $p_k^{\alpha_k}$ avec $\alpha_k = 0$), cela ne changerait rien à la valeur de N : si $\alpha_k = 0$, alors $(\alpha_k + 1) = 1$...*

❧ Si l'entier N est impair, alors chacun des facteurs dans cette décomposition est impair, donc chacune des valuations α_k est paire :

$$\forall\, 1 \leqslant k \leqslant d,\ \exists\, a_k \in \mathbb{N}, \quad \alpha_k = 2a_k.$$

L'entier n peut alors se décomposer sous la forme

$$n = \prod_{k=1}^{d} p_k^{2a_k} = \left(\prod_{k=1}^{d} p_k^{a_k}\right)^2,$$

c'est donc un carré parfait.

Réciproquement, si n est un carré parfait, alors il existe un entier m tel que $n = m^2$. De la décomposition du facteur m :

$$m = \prod_{k=1}^{d} p_k^{a_k},$$

on peut déduire que

$$n = m^2 = \prod_{k=1}^{d} p_k^{2a_k}$$

et donc que le nombre N de diviseurs de n est impair :

$$N = \prod_{k=1}^{d} (2a_k + 1).$$

2. On considère la famille $\mathscr{D} = (d_k)_{1 \leqslant k \leqslant N}$ des diviseurs de N, rangés par ordre croissant :

$$1 = d_1 < d_2 < \cdots < d_{N-1} < d_N = n.$$

On peut démontrer (voir plus loin) que

$$\forall\, 1 \leqslant k \leqslant N, \quad d_k d_{N+1-k} = n.$$

✍ *Cette propriété permet de retrouver le résultat précédent.*

❧ *Si l'entier N est pair : $N = 2q$, alors la somme des deux indices est impaire*

$$k + (N + 1 - k) = 2q + 1$$

ce qui prouve que les deux indices k et $(N + 1 - k)$ sont distincts ! Les deux facteurs d_k et d_{N+1-k} sont alors distincts et cela prouve que n n'est pas un carré parfait.

❧ *Si l'entier N est impair : $N = 2q+1$, alors on peut choisir $k = (q+1)$ et dans ce cas, $N+1-k = (2q+1)+1-(q+1) = q+1$. On a alors $n = d_k d_{N+1-k} = d_{q+1}^2$ et n est un carré parfait.*

En posant

$$P = \prod_{k=1}^{N} d_k,$$

on obtient

$$P^2 = \left(\prod_{k=1}^{N} d_k \right)^2 = \prod_{k=1}^{N} d_k \times \prod_{\ell=1}^{N} d_\ell.$$

Avec le changement d'indice $\ell = N + 1 - k$,

$$P^2 = \prod_{k=1}^{N} d_k \times d_{N+1-k} = \prod_{k=1}^{N} d_k d_{N+1-k} = n^N.$$

✍ *La relation $d_k d_{N+1-k} = n$ est plus simple à deviner (sur une figure) qu'à démontrer !*
Elle est évidente pour $k = 1$: le plus petit diviseur d_1 de n est égal à 1 et le plus grand diviseur d_N de n est égal à n.
Supposons qu'il existe un entier $1 \leqslant k < N$ tel que

$$d_k d_{N+1-k} = n.$$

Comme d_{k+1} est un diviseur de n, il existe un entier q tel que $d_{k+1} q = n$. Ce quotient q est aussi un diviseur de n, donc il existe un indice $1 \leqslant j \leqslant N$ tel que $q = d_j$ et on a

$$n = d_{k+1} d_j.$$

Si $j \geqslant N + 1 - k$, alors $d_j \geqslant d_{N+1-k}$ et donc

$$n = d_{k+1} d_j > d_k d_j \geqslant d_k d_{N+1-k} \overset{\text{HR}}{=} n.$$

C'est impossible ! Donc $j \leqslant N + 1 - k$.

Si $j < N - k$, alors $d_j < d_{N-k} = d_{(N+1)-(k+1)}$. Comme d_{N-k} est un diviseur de n, il existe un quotient $q' = d_\ell$ tel que $n = d_\ell d_{N-k}$. Si $\ell < k$, alors $d_\ell < d_k$ et

$$n = d_\ell d_{N-k} < d_k d_{N-k} < d_k d_{N+1-k} \overset{\text{HR}}{=} n.$$

C'est impossible ! Donc $j \geqslant N - k$ et finalement $j = N - k$.

Solution 4 — 23-04

1. Appliquons l'algorithme d'Euclide dans sa version Blankinship pour trouver le pgcd et résoudre simultanément l'équation de Bézout.

$$\begin{pmatrix}1&0&1683\\0&1&969\end{pmatrix} \underset{L_1\leftarrow L_1-L_2}{\sim} \begin{pmatrix}1&-1&714\\0&1&969\end{pmatrix} \underset{L_2\leftarrow L_2-L_1}{\sim} \begin{pmatrix}1&-1&714\\-1&2&255\end{pmatrix} \underset{L_1-2L_2}{\sim} \begin{pmatrix}3&-5&204\\-1&2&255\end{pmatrix}$$
$$\underset{L_2\leftarrow L_2-L_1}{\sim} \begin{pmatrix}3&-5&204\\-4&7&51\end{pmatrix} \underset{L_1\leftarrow L_1-4L_2}{\sim} \begin{pmatrix}19&-33&0\\-4&7&51\end{pmatrix}$$

On a ainsi démontré que

$$19\cdot 1683 - 33\cdot 969 = 0 \qquad \text{et que} \qquad -4\cdot 1683 + 7\cdot 969 = 51.$$

✍ *L'algorithme de Blankinship consiste à écrire une succession de matrices de la forme*

$$\begin{pmatrix}A_k & C_k\end{pmatrix} \in \mathfrak{M}_{n,n+1}(\mathbb{Z}) \qquad \textit{avec} \qquad A_k \in \mathfrak{M}_n(\mathbb{Z}) \quad \textit{et} \quad C_k \in \mathfrak{M}_{n,1}(\mathbb{Z})$$

et comme ***invariant de boucle*** $A_kC_0 = C_k$.

Ici, on a donc démontré que

$$\begin{pmatrix}19&-33\\-4&7\end{pmatrix}\begin{pmatrix}1683\\969\end{pmatrix} = \begin{pmatrix}0\\51\end{pmatrix}.$$

✍ *Il est important de remarquer que les opérations effectuées sur les lignes lors de cet algorithme se traduisent matriciellement par des multiplications à gauche par des matrices dont le déterminant est égal à 1 (des transvections uniquement). Comme $A_0 = I_2$, on en déduit que $\det A_k = 1$ pour tout k et donc que les matrices A_k sont des matrices inversibles dont l'inverse est aussi une matrice à coefficients dans $\mathbb{Z}$.*

Cette propriété signifie que, pour toutes les matrices A_k, toutes les lignes sont constituées d'entiers qui sont premiers dans leur ensemble (développer l'égalité $\det A_k = 1$ par une ligne quelconque et interpréter avec le Théorème de Bézout).

Par conséquent, $1683 \wedge 969 = 51$ mais aussi $1683 = 33\cdot 51$ et $969 = 19\cdot 51$.
Un couple $(x,y) \in \mathbb{Z}^2$ vérifie donc $969x - 1683y = 51$ si, et seulement si,

$$969\cdot(x-7) - 1683\cdot(y-4) = 0 \qquad \text{c'est-à-dire} \qquad 19\cdot(x-7) = 33\cdot(y-4)$$

après simplification par 51. Comme 19 et 33 sont premiers entre eux, on en déduit que $(x,y) \in \mathbb{Z}^2$ vérifie $969x - 1683y = 51$ si, et seulement si, il existe un entier $k \in \mathbb{Z}$ tel que

$$x = 7 + 33k \qquad \text{et} \qquad y = 4 + 19k.$$

2. Il suffit de remarquer que $102 = 2\cdot 51$. Une solution particulière de cette équation est donc $(2\cdot 7, 2\cdot 4)$ et, pour les raisons exposées à la question précédentes, un couple $(x,y) \in \mathbb{Z}^2$ est solution de $1683x - 969y = 102$ si, et seulement si, il existe un entier $k \in \mathbb{Z}$ tel que

$$x = 14 + 33k \qquad \text{et} \qquad y = 8 + 19k.$$

3. Comme $969 \wedge 1683 = 51$, on sait que

$$\{969x - 1683y,\ (x,y) \in \mathbb{Z}^2\} = 969\mathbb{Z} + 1683\mathbb{Z} = 51\mathbb{Z}.$$

Or $51 < 84 < 2\cdot 51$, donc 84 n'est pas divisible par 51 et par conséquent l'équation $969x - 1683y = 84$ n'a pas de solution dans $\mathbb{Z}^2$.

Solution 5 — 23-05

1. Comme $46 = 2\cdot 23$, l'expression $23x + 46y$ est divisible par 23, quels que soient les entiers x et y. Or 3 n'est pas divisible par 23, donc l'équation n'a pas de solution.

2. On applique l'algorithme d'Euclide-Blankinship en effectuant successivement les opérations

$$L_1 \leftarrow L_1 - 2L_2, \quad L_2 \leftarrow L_2 - 2L_1, \quad L_1 \leftarrow L_1 - 3L_2 \quad \text{et} \quad L_2 \leftarrow L_2 - 3L_1.$$

$$\begin{pmatrix}1&0&56\\0&1&23\end{pmatrix}\sim\begin{pmatrix}1&-2&10\\0&1&23\end{pmatrix}\sim\begin{pmatrix}1&-2&10\\-2&5&3\end{pmatrix}\sim\begin{pmatrix}7&-17&1\\-2&5&3\end{pmatrix}\sim\begin{pmatrix}7&-17&1\\-23&56&0\end{pmatrix}$$

On a ainsi démontré que 23 et 56 étaient premiers entre eux et que $-17\cdot 23+7\cdot 56=1$. Par conséquent, $(x_0,y_0)=(3\cdot(-17),3\cdot 7)=(-51,21)$ est une solution particulière de l'équation $23x+56y=3$ et, plus généralement, $(x,y)\in\mathbb{Z}^2$ est une solution si, et seulement si, $23(x-x_0)=-56(y-y_0)$, donc $(x,y)\in\mathbb{Z}^2$ est une solution si, et seulement si, il existe un entier $k\in\mathbb{Z}$ tel que

$$x=-51+56k \qquad \text{et} \qquad y=21-23k.$$

✍ *La solution particulière la plus simple est donc $(5,-2)$ (avec $k=1$).*

Solution 6 — 23-06

1. a. Si $13x-7y=1$, alors $13(x+1)=1+7y+13=7(2+y)$. Ainsi, 7 divise le produit $13(x+1)$ et comme $7\wedge 13=1$, alors 7 divise $(x+1)$ (Théorème de Gauss). Avec $0\leqslant x\leqslant 7$, la somme $x+1$ est divisible par 7 si, et seulement si, $x=6$, ce qui nous donne $7y=13\cdot 6-1=77$, c'est-à-dire $y=11$.

Le couple $(x_0,y_0)=(6,11)$ est une solution particulière.

✍ *L'algorithme d'Euclide-Blankinship donne une autre solution particulière.*

$$\begin{pmatrix}1&0&13\\0&1&7\end{pmatrix}\underset{L_1\leftarrow -L_1+2L_2}{\sim}\begin{pmatrix}-1&2&1\\0&1&7\end{pmatrix}\sim\begin{pmatrix}-1&2&1\\*&*&0\end{pmatrix}$$

On voit ainsi (sans qu'il soit nécessaire de calculer les coefficients de la deuxième ligne) que $(-1)\cdot 7+2\cdot 13=1$ et donc que $(-1,-2)$ est une solution particulière.

1. b. Le couple $(x,y)\in\mathbb{Z}^2$ est une solution si, et seulement si, $13(x-x_0)=7(y-y_0)$. Comme 7 et 13 sont premiers entre eux, on en déduit que $(x,y)\in\mathbb{Z}^2$ est une solution si, et seulement si, il existe un entier $k\in\mathbb{Z}$ tel que

$$x=x_0+7k=6+7k \qquad \text{et} \qquad y=y_0+13k=11+13k.$$

✍ *Avec $k=-1$, on retrouve la solution particulière $(-1,-2)$.*

2. Une solution particulière de $13x-7y=2$ est donc $(-2,-4)$ et $(x,y)\in\mathbb{Z}^2$ est une solution si, et seulement si, il existe un entier $k\in\mathbb{Z}$ tel que

$$x=-2+7k \qquad \text{et} \qquad y=-4+13k.$$

✍ *Avec $k=1$, on trouve la solution particulière $(5,9)$.*

Solution 7 — 23-07

Notons d', le pgcd de a' et b'.

Comme d divise a et b, il est clair que d divise aussi a' et b', donc d divise d'.

Réciproquement, on doit remarquer que

$$\begin{pmatrix}a'\\b'\end{pmatrix}=A\begin{pmatrix}a\\b\end{pmatrix} \qquad \text{avec} \qquad A=\begin{pmatrix}13&5\\5&2\end{pmatrix}.$$

Il est clair que $\det A=1$ et comme 1 est inversible dans $\mathbb{Z}$, on en déduit que la matrice A est inversible et que son inverse est aussi à coefficients dans $\mathbb{Z}$:

$$A^{-1}=\begin{pmatrix}2&-5\\-5&13\end{pmatrix}$$

si bien que

$$\begin{pmatrix}a\\b\end{pmatrix}=A^{-1}\begin{pmatrix}a'\\b'\end{pmatrix}=\begin{pmatrix}2a'-5b'\\-5a'+13b'\end{pmatrix}.$$

Comme d' divise a' et b', on en déduit que d' divise également a et b et donc que d' divise d.

On a ainsi démontré (par "double divisibilité") que les pgcd d et d' étaient égaux.

Solution 8 23-08

Considérons un nombre complexe z tel que $z^n = z^p = -1$.

Le pgcd $d = n \wedge p$ est, par définition, un diviseur de p. Comme p est premier, il n'y a que deux cas possibles :

— ou bien $d = 1$ et, dans ce cas, n et p sont premiers entre eux ;

— ou bien $d = p$ et, dans ce cas, n est divisible par d, c'est-à-dire par p.

Premier cas

Si n et p sont premiers entre eux, alors (Théorème de Bézout) il existe deux entiers a et b tels que $an + bp = 1$. On en déduit que

$$z = z^1 = z^{an+bp} = (z^n)^a \cdot (z^p)^b = (-1)^{a+b}.$$

Si $a + b$ est pair, alors $z = 1$, ce qui contredit l'hypothèse initiale $z^n = z^p = -1$. Si $a + b$ est impair, alors la seule possibilité restante est $z = -1$, ce qui est cohérent avec l'hypothèse de départ si n et p sont impairs.

Deuxième cas

Si n est un multiple de p distinct de p, alors il existe un entier $q \geqslant 2$ tel que $n = qp$ et

$$z^n = (z^p)^q = (-1)^q.$$

Si q est pair, on obtient $z^n = 1$, ce qui contredit l'hypothèse $z^n = -1$. Si q est impair, alors la propriété $z^p = -1$ entraîne nécessairement $z^n = -1$.

Conclusion

On distingue finalement trois cas.

— Si n ou p est pair, alors il n'existe aucun complexe z tel que $z^n = z^p = -1$;

— Si p et n sont impairs, alors

  — ou bien n et p sont premiers entre eux et $z = -1$ est le seul complexe qui vérifie $z^n = z^p = -1$;

  — ou bien n est un multiple impair de p et dans ce cas, les nombres complexes z qui vérifient $z^n = z^p = -1$ sont les p racines p-ièmes complexes de -1 :

$$\exp \frac{i(2k+1)\pi}{p} \qquad (0 \leqslant k < p).$$

Solution 9 23-09

1. Dans $\mathbb{Z}/6\mathbb{Z}$, on a $5 = -1$, donc $5^n = (-1)^n$ pour tout $n \in \mathbb{N}$.

2. Dans $\mathbb{Z}/6\mathbb{Z}$, on a donc $A_n = (-1)^n - n + 1$ et les deux applications $[n \mapsto (-1)^n]$ et $[n \mapsto -n]$, considérées comme des applications de $\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$ admettent 6 pour période commune.

✍ *Si deux fonctions périodiques f et g admettent des périodes* entières T_1 *et* T_2*, alors elles admettent le ppcm $T_0 = T_1 \vee T_2$ pour période commune.*

Il suffit donc d'écrire les six valeurs possibles de A_n modulo 6.

n	0	1	2	3	4	5
5^n	1	-1	1	-1	1	-1
$-n$	0	-1	-2	3	2	1
A_n	2	-1	0	3	4	1

On constate ainsi que A_n est divisible par 6 si, et seulement si, n est congru à 2 modulo 6.

Solution 10 23-10

1. On calcule les puissances dans $\mathbb{Z}/7\mathbb{Z}$ de proche en proche tant que c'est nécessaire.

✍ *On sait que la suite des puissances a^n calculées dans $\mathbb{Z}/N\mathbb{Z}$ est périodique à partir d'un certain rang. Il suffit donc de les calculer jusqu'à ce qu'on retrouve une valeur déjà obtenue pour les connaître toutes.*

Dans $\mathbb{Z}/7\mathbb{Z}$, on calcule en fait les puissances successives de -2.

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

On déduit de $5^6 = 5^0$ que $5^{k+6} = 5^k \cdot 5^6 = 5^k$ pour tout $k \in \mathbb{N}$. Par conséquent, si $n = 6q + r$, alors $5^n = (5^6)^n \cdot 5^r = 5^r$.

✍ *Comme 7 est premier, l'anneau $\mathbb{Z}/7\mathbb{Z}$ est un corps et le groupe (multiplicatif) de ses éléments inversibles contient six éléments (= tous les éléments non nuls).*

Autrement dit, $\varphi(7) = 6$ et $5^6 = 1$ d'après le Théorème d'Euler. On pouvait anticiper le fait qu'il suffisait de calculer 5^n pour $0 \leqslant n < 7$ pour connaître toutes les puissances de 5.

Mieux ! Comme le Théorème de Lagrange nous assure que l'ordre d'un élément divise l'ordre du groupe, on savait que l'ordre de 5 était égal à 1, 2, 3 ou 6 et il suffisait donc de calculer 5^2 et 5^3 pour conclure. (Il est clair que $5^1 \neq 1$ et on sait déjà, sans calcul ! que $5^6 = 1$.)

Cela dit, nos calculs ont montré que les puissances de 5 engendraient le groupe multiplicatif $(\mathbb{Z}/7\mathbb{Z})^\times$, qui est donc isomorphe au groupe additif $\mathbb{Z}/6\mathbb{Z}$ (puisque tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$).

2. On vérifie sans peine que $1972 = 281 \cdot 7 + 5$. Par conséquent, $1972^{57} = 5^{57} \pmod 7$ et comme $57 = 9 \cdot 6 + 3$, on déduit de la question précédente que $5^{57} = 5^3 \pmod 7$, puis que

$$1972^{57} = -1 = 6 \pmod 7.$$

❧ De même, si $n = 6q + r$, alors $1972^n = 5^r \pmod 7$ et d'après la question précédente, $5^r = 4 \pmod 7$ avec $0 \leqslant r < 6$ si, et seulement si, $r = 2$.

Autrement dit, $1972^n = 4 \pmod 7$ si, et seulement si, l'exposant n est congru à 2 modulo 6.

Solution 11 — 23-11

Comme 5 est premier, $\varphi(5) = 4$, donc $x^4 = 1$ pour tout $x \in \mathbb{Z}/5\mathbb{Z}$. Pour tout exposant $n = 4q + r$, on a donc $x^n = (x^4)^q \cdot x^r = x^r$ et comme $1974 = 2 \pmod 4$, on a donc $8^{1974} = 3^{1974} = 3^2 = 4 \pmod 5$.

✍ *On sait que $1974 = 2 \pmod 4$ car c'est un nombre pair et qu'il y a eu une Coupe du monde de football en 1974 (les Jeux Olympiques, c'était en 1972 et en 1976).*

En effectuant les calculs, on obtient : $3^0 = 1$, $3^1 = 3$, $3^2 = 4$ et $3^3 = 2$, ce qui prouve que le groupe multiplicatif $(\mathbb{Z}/5\mathbb{Z})^\times$ est engendré par 3. Il s'agit ainsi d'un groupe cyclique d'ordre 4, il est donc isomorphe au groupe (additif) $\mathbb{Z}/4\mathbb{Z}$ et au groupe (multiplicatif) $\mathbb{U}_4$.

Solution 12 — 23-12

Dans $\mathbb{Z}/11\mathbb{Z}$,

$$3^2 = 9 = -2, \qquad 3^3 = -6 = 5, \qquad 4^2 = 5, \qquad 4^4 = 5^2 = 3.$$

Par conséquent,

$$u_n = 3^3 \cdot 3^n - 4^2 \cdot (4^4) = 5 \cdot 3^n - 5 \cdot 3^n = 0.$$

Autrement dit, u_n est divisible par 11.

Solution 13 — 23-13

Dans $\mathbb{Z}/13\mathbb{Z}$, on a $5^0 = 1$, $5^1 = 5$, $5^2 = -1$, $5^3 = -5$ et $5^4 = 1$. Par conséquent, modulo 13, la suite de terme général 5^k est périodique de période 4.

Posons donc la division euclidienne de n par 4 :

$$n = 4q + r \quad \text{et par conséquent} \quad 2n = 4(2q) + 2r.$$

On a donc

$$5^{2n} + 5^n = (5^4)^q \cdot 5^r + (5^4)^{2q} \cdot 5^{2r} = 5^r + 5^{2r} = 5^r + (-1)^r \pmod{13}.$$

Le reste r peut prendre quatre valeurs seulement, il suffit de les passer en revue !

$$5^0 + (-1)^0 = 2 \pmod{13}, \qquad 5^1 + (-1)^1 = 4 \pmod{13},$$
$$5^2 + (-1)^2 = 0 \pmod{13}, \qquad 5^3 + (-1)^3 = -6 = 7 \pmod{13}.$$

Par conséquent, l'entier $5^{2n} + 5^n$ est divisible par 13 si, et seulement si, l'entier n est congru à 2 modulo 4.

Solution 14 — 23-14

Dans $\mathbb{Z}/13\mathbb{Z}$,

$$5^0 = 1, \quad 5^1 = 5, \quad 5^2 = -1, \quad 5^3 = -5, \quad 5^4 = 1.$$

Par conséquent, la suite de terme général 5^k est périodique de période 4.

De plus, $31 = 5 + 26 = 5 \pmod{13}$ et $18 = 5 + 13 = 5 \pmod{13}$ et donc, puisque $5^4 = 1$,

$$u_n = 5^{4n+1} + 5^{4n-1} = (5^4)^n \cdot 5 + (5^4)^n \cdot 5^{-1} = 5 + 5^{-1}.$$

✍ *Comme 13 est premier, l'anneau $\mathbb{Z}/13\mathbb{Z}$ est un corps et tout élément non nul est inversible, ce qui nous autorise à écrire 5^{-1} sans avoir calculé cet inverse au préalable.*

On remarque que $5 \times 8 = 1 \pmod{13}$, donc $5^{-1} = 8 \pmod{13}$ et finalement $u_n = 0 \pmod{13}$.

✍ *Comme d'habitude, si on n'est pas bon aux devinettes, on peut trouver l'inverse modulo p d'un entier n premier à p en résolvant l'équation de Bézout $an + bp = 1$.*

Solution 15 — 23-15

Dans $\mathbb{Z}/8\mathbb{Z}$, on a : $0^2 = 0$, $(\pm1)^2 = 1$, $(\pm2)^2 = 4$, $(\pm3)^2 = 1$ et $4^2 = 0$.
Par conséquent, $(5x+3)^2 = 1 \pmod 8$ si, et seulement si, $5x + 3 = \pm1$ ou $5x + 3 = \pm3$.
Comme 5 et 8 sont premiers entre eux, alors 5 est inversible modulo 8 et on vérifie sans peine que $5^2 = 1 \pmod 8$.

✍ *Si on n'a pas d'inspiration, on peut résoudre rapidement l'équation de Bézout $5a + 8b = 1$, qui nous dit que (la classe modulo 8 de) a est l'inverse de (la classe modulo 8 de) 5.*

Par conséquent, l'équation $5x + 3 = c$ équivaut à $x + 15 = 5c$, c'est-à-dire $x = 5c + 1$.
L'équation admet donc quatre solutions : 0, 2, 4 et 6.

✍ ***Variante***
Comme $5 = -3 \pmod 8$ et que $3^2 = 1 \pmod 8$,

$$\forall\, x \in \mathbb{Z}/8\mathbb{Z}, \quad (5x+3)^2 - 1 = (-3x+3)^2 - 1 = 3^2(x-1)^2 - 1 = (x-1)^2 - 1 = (x-2)x.$$

Les entiers n et $(n-2)$ ont même parité, quel que soit $n \in \mathbb{Z}$. Par conséquent,
- *si n est impair, alors le produit $n(n-2)$ est impair et ne peut donc être divisible par 8 ;*
- *si au contraire n est pair, alors $n(n-2)$ est le produit de deux entiers pair consécutifs, donc l'un des deux est divisible par 4 et le produit est divisible par 8.*

Les solutions sont donc (les classes modulo 8 de) 0, 2, 4 et 6.

Solution 16 — 23-16

Dans $z/13z$, on a $2 \cdot 7 = 1$, ce qui permet d'écrire le polynôme du second degré sous forme canonique et de le factoriser.
Pour tout $x \in \mathbb{Z}/13\mathbb{Z}$,

$$x^2 + x + 6 = x^2 + 2 \cdot 7x + 6 = (x+7)^2 - 43 = (x+7)^2 - 2^2 = \big((x+7)-2\big)\big((x+7)+2\big) = (x+5)(x+9).$$

Comme 13 est premier, l'anneau $\mathbb{Z}/13\mathbb{Z}$ est un corps et $x^2 + x + 6 = 0$ si, et seulement si, $x = -5$ ou $x = -9 = 4$.

✍ *Il n'y a pas de diviseur de zéro dans un corps. Par conséquent, un produit est nul si, et seulement si, l'un des facteurs est nul.*

Solution 17 — 23-17

Comme $4 = -2 \pmod 6$ et $5 = -1 \pmod 6$, le premier système est équivalent à

$$\begin{cases} 2x + 2y = 2 \\ x - y = 2 \end{cases} \underset{L_1 \leftarrow L_1 - 2L_2}{\sim} \begin{cases} 4y = -2 \\ x - y = 2 \end{cases}$$

Dans $\mathbb{Z}/6\mathbb{Z}$, l'élément 4 n'est pas inversible. En écrivant la liste des éléments de la forme $4q$, on constate que l'équation $4y = -2 = 4$ admet deux solutions : $y = 1$ et $y = 4$. La seconde équation nous donne $x = 2 + y$, donc le système admet deux solutions : $(3,1)$ et $(0,4)$.

❧ En effectuant l'opération $L_1 \leftarrow L_1 - 3L_2$ sur le second système, on obtient

$$\begin{cases} 5y = 1 \\ x - y = 2 \end{cases}$$

et donc $y = -1$ (puisque $5 = -1$) et $x = 2 + y = 1$. Ce second système admet donc une seule solution : $(1,-1)$.

✍ *La différence entre les deux systèmes s'explique par leurs déterminants : le déterminant du premier système est égal à 2 (modulo 6) et n'est donc pas inversible ; le déterminant du second système est égal à 1 (modulo 6) et donc inversible, ce qui permet de résoudre le système à l'aide des formules de Cramer.*

Solution 18 23-18

Voici la partie significative de la table.

$y=$	2	3
$x=2$	0	2
$x=3$	2	1

On y retrouve que 3 est inversible dans $\mathbb{Z}/4\mathbb{Z}$ et que $3\cdot 3=1$. L'opération $L_1 \leftarrow 3L_1$ est donc licite sur ce système d'équations, qui est donc équivalent au système

$$\begin{cases} x-y=1 \\ x+y=1 \end{cases} \quad \text{c'est-à-dire à} \quad \begin{cases} x-y=1 \\ 2y=0 \end{cases} \qquad (L_2 \leftarrow L_2-L_1)$$

Comme 2 n'est pas inversible dans $\mathbb{Z}/4\mathbb{Z}$, il faut se fier à la table de multiplication pour résoudre : l'équation $2y=0$ admet deux solutions (0 et 2) et $x=1+y$.

Le système admet donc deux solutions : $(1,0)$ et $(3,2)$.

Solution 19 23-19

On calcule comme une machine...

$y=$	2	3	4	5
$x=2$	4	0	2	4
$x=3$	0	3	0	3
$x=4$	2	0	4	2
$x=5$	4	3	2	1

On lit sur la table que l'équation $2x=0$ admet (exactement) deux solutions dans $\mathbb{Z}/6\mathbb{Z}$: 0 et 3.

❧ On applique l'algorithme du pivot en respectant les particularités du calcul dans $\mathbb{Z}/6\mathbb{Z}$.

✍ *Les éléments 2, 3 et 4 ne sont pas inversibles !*

$$\begin{cases} 2x+2y=4 \\ 5x+3y=3 \end{cases} \underset{L_2\leftarrow L_2-2L_1}{\sim} \begin{cases} 2x+2y=4 \\ x-y=1 \end{cases} \underset{L_1\leftarrow L_1-2L_2}{\sim} \begin{cases} 4y=2 \\ x-y=1 \end{cases}$$

D'après la table de multiplication, l'équation $4y=2$ admet deux solutions : $y=2$ et $y=5=-1$. Comme $x=y+1$, on en déduit que les solutions sont les couples $(3,2)$ et $(0,5)$.

✍ *Le déterminant du système est égal à 4, qui n'est pas inversible dans $\mathbb{Z}/6\mathbb{Z}$. C'est pourquoi on trouve plus d'une solution. (Avec un second membre différent, on aurait pu n'avoir aucune solution.)*

Solution 20 23-20

1.

$y=$	2	3	4
$x=2$	4	1	3
$x=3$	1	4	2
$x=4$	3	2	1

2. On déduit de la table de multiplication que $3\times 2=1$, donc 2 et 3 sont inverses l'un de l'autre dans $\mathbb{Z}/5\mathbb{Z}$.

✍ ***Rappels de cours***

Dans $\mathbb{Z}/n\mathbb{Z}$, la classe de a est inversible si, et seulement si, a et n sont premiers entre eux.

Pour trouver un représentant de la classe inverse, il suffit de résoudre l'équation de Bézout : si $au+nv=1$, alors la classe de u modulo n est l'inverse de la classe de a modulo n.

Il n'y a donc aucune nécessité à calculer la table de multiplication de $\mathbb{Z}/5\mathbb{Z}$ pour traiter cette question !

❧ Par conséquent, $3x=-4$ équivaut à $x=-8=-3$ (multiplication par 2) et $2x=-1$ équivaut à $x=-3=2$ (multiplication par 3).

❧ On applique l'algorithme du pivot avec les règles de calcul spécifiques à $\mathbb{Z}/5\mathbb{Z}$.

$$\begin{cases} 3x + 4y = 1 \\ 2x + 3y = 2 \end{cases} \sim \begin{cases} x + 3y = 2 \\ 2x + 3y = 2 \end{cases} \qquad (L_1 \leftarrow 2L_1)$$

$$\sim \begin{cases} x + 3y = 2 \\ 3y = 2 \end{cases} \qquad (L_2 \leftarrow -L_2 + 2L_1)$$

On en déduit que $x = 0$ ($L_1 \leftarrow L_1 - L_2$) et $y = 4$ (multiplication par 2).

✍ *Les opérations de pivot pour résoudre un système "linéaires" sont les mêmes dans tous les anneaux :*
— *échange de deux lignes ;*
— *transvection $L_i \leftarrow L_i + \sum_{j\neq i} a_j L_j$;*
— *multiplication par un élément **inversible** $L_i \leftarrow aL_i$.*
Dans un corps, il suffit que $a \neq 0$ pour que a soit inversible.

✍ *De même, les formules de Cramer sont vraies dans tous les anneaux, à condition de remplacer $\det S \neq 0$ (condition spécifique aux corps) par $\det S$ **inversible**.*
Il est facile de vérifier que le déterminant du système résolu ici est égal à 1, ce qui nous donne

$$x = 1^{-1} \cdot \begin{vmatrix} 1 & 4 \\ 2 & 3 \end{vmatrix} = -5 = 0, \qquad y = 1^{-1} \cdot \begin{vmatrix} 3 & 1 \\ 2 & 2 \end{vmatrix} = 4.$$

3. Comme 3 est l'inverse de 2,

$$x^2 + x + 1 = x^2 + 2.(3x) + 1 = (x+3)^2 - 9 + 1 = (x+3)^2 - 2.$$

Par conséquent, $x^2 + x + 1 = 0$ si, et seulement si, $(x+3)^2 = 2$.

✍ *La mise sous forme canonique d'un polynôme de degré deux est possible dans tout anneau de nombres où 2 est inversible. On est alors ramené à trouver les éléments de l'anneau qui sont des carrés (pour résoudre une équation de la forme $y^2 = a$).*

Mais pour tout $y \in \mathbb{Z}/5\mathbb{Z}$, on a $y^2 \in \{0, 1, -1\}$, donc l'équation $y^2 = 2$ n'a pas de solution dans $\mathbb{Z}/5\mathbb{Z}$ et l'équation $x^2 + x + 1 = 0$ non plus.

Solution 21 23-21

Dans $\mathbb{Z}/12\mathbb{Z}$, le plus simple est de calculer le cube de chaque élément et de comparer. En remarquant que $x^3 = x$ si, et seulement si, $(-x)^3 = (-x)$, il suffit d'étudier la moitié des éléments de $\mathbb{Z}/12\mathbb{Z}$.

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

L'équation $x^3 = x$ admet donc neuf solutions : 0, ± 1, ± 3, ± 4, ± 5.

✍ *Comme 12 n'est pas premier, l'anneau $\mathbb{Z}/12\mathbb{Z}$ compte des diviseurs de 0, il n'est donc pas étonnant qu'une équation polynomiale de degré 3 admette plus de trois diviseurs.*
On peut aussi remarquer que $12 = 2^2.3$ est composé avec un facteur de valuation supérieure à 2. De ce fait, l'élément $6 = 2.3$ est nilpotent (d'indice 2) dans $\mathbb{Z}/12\mathbb{Z}$.

❧ Comme 11 est premier, l'anneau $\mathbb{Z}/11\mathbb{Z}$ est un corps et n'a donc pas de diviseur de zéro. Il est donc plus efficace de factoriser le polynôme que de passer en revue les différentes valeurs de x.
Comme $X^3 - X = X(X^2 - 1) = X(X-1)(X+1)$, l'équation $x^3 = x$ admet trois solutions dans $\mathbb{Z}/11\mathbb{Z}$: 0, 1 et -1.

Solution 22 23-22

1. Dans $\mathbb{Z}/7\mathbb{Z}$,

$$x^2 + 2x - 3 = x^2 + 2x + 1 - 4 = (x+1)^2 - 2^2 = \big((x+1) - 2\big)\big((x+1) + 2\big) = (x-1)(x+3).$$

Comme 7 est premier, alors $\mathbb{Z}/7\mathbb{Z}$ est un corps et n'a donc pas de diviseur de zéro. Par conséquent, $x^2 + 2x - 3 = 0$ si, et seulement si, $x = 1$ ou $x = -3$.

2. Comme $21 = 3 \times 7$, les multiples de 3 et les multiples de 7 sont des diviseurs de 0 :

$$\forall\, x \in \mathbb{Z}, \quad (3 \times x) \times 7 = (7 \times x) \times 3 = 0 \pmod{21}.$$

Ainsi, 3, 6, 7, 9, $12 = -9$, $14 = -7$, $15 = -6$ et $18 = -3$ sont des diviseurs de zéro dans $\mathbb{Z}/21\mathbb{Z}$. Plus précisément,

$$3 \times 7 = 6 \times 7 = 9 \times 7 = 9.$$

Par conséquent, $x^2 + 2x - 3 = (x-1)(x+3) = 0$ dans $\mathbb{Z}/21\mathbb{Z}$ si, et seulement si, $x = 1$ ou $x = -3$ ou

$$(x-1, x+3) \in \big\{(\pm 3, \pm 7), (\pm 6, \pm 7), (\pm 7, \pm 3), (\pm 7, \pm 6), (\pm 7, \pm 9), (\pm 9, \pm 7)\big\}.$$

✍ *En tout, 24 possibilités ! Il serait ridicule de les passer en revue une par une, puisqu'il n'y a que 21 éléments dans l'anneau $\mathbb{Z}/21\mathbb{Z}$! On va donc discuter sur la première composante de chaque couple : il n'y a que 8 possibilités.*

$x-1$	3	-3	6	-6	7	-7	9	-9
$x+3$	7	1	10	-2	-10	-3	-8	-5
Solution	oui	non	non	non	non	oui	non	non

On a donc quatre solutions dans $\mathbb{Z}/21\mathbb{Z}$: 1, $-3 = 18$, 4 et $15 = -6$.

Solution 23 23-23

1. Dans $\mathbb{Z}/5\mathbb{Z}$, on a $3 \times 2 = 1$, donc 2 admet $3 = -2$ pour inverse.

✍ *Comme 5 est premier, tout élément non nul de $\mathbb{Z}/5\mathbb{Z}$ est inversible. Mais cela ne nous garantit pas de savoir trouver rapidement son inverse !*

Par conséquent, pour tout $x \in \mathbb{Z}/5\mathbb{Z}$,

$$x^2 - 3x + 2 = x^2 + 2x + 2 = (x+1)^2 + 1$$

donc

$$x^2 - 3x + 2 = 0 \iff (x+1)^2 = -1.$$

✍ *La mise sous forme canonique d'un polynôme de degré deux est possible dans n'importe quel anneau, il suffit que 2 soit inversible.*

Il reste donc à résoudre $y^2 = -1$ dans $\mathbb{Z}/5\mathbb{Z}$. Or $1^2 = (-1)^2 = 1$ et $2^2 = 3^2 = -1$, donc

$$x^2 - 3x + 2 = 0 \iff x + 1 = 2 \quad \text{ou} \quad x + 1 = 3.$$

Les solutions sont donc $x = 1$ et $x = 2$.

✍ *Si $\mathbb{K}$ est un corps, l'équation $P(x) = 0$, où P est un polynôme de degré d à coefficients dans $\mathbb{K}$, admet au plus d racines distinctes dans $\mathbb{K}$.*

En revanche, si A est un anneau, une équation polynomiale de degré d à coefficients dans A peut avoir plus de d solutions. (Contrairement à un corps, un anneau peut avoir des diviseurs de zéro.)

2. Le reste de la division euclidienne de $n^2 - 3n$ par 5 est égal à 3 si, et seulement si,

$$n^2 - 3n + 2 = n^2 - 3n - 3 = 0 \pmod{5}.$$

D'après la question précédente, les solutions de cette équation sont les entiers de la forme $1 + 5k$ ou de la forme $2 + 5k$ pour $k \in \mathbb{Z}$.

Solution 24 23-24

1. Le plus simple consiste à calculer x^3 lorsque x parcourt $\mathbb{Z}/7\mathbb{Z}$.

x	0	1	2	3	-3	-2	-1
x^2	0	1	4	2	2	4	1
x^3	0	1	1	-1	1	-1	-1

On voit alors que $n^3+1=0 \pmod 7$ si, et seulement si, $n=3$, $n=5$ ou $n=6$ modulo 7, puis que $n^3-1=0 \pmod 7$ si, et seulement si, $n=1$, $n=2$ ou $n=4$ modulo 7.

✍ *Comme 7 est premier, alors $\mathbb{Z}/7\mathbb{Z}$ est un corps et par conséquent une équation polynomiale de degré 3 admet au plus trois racines distinctes.*

Bien entendu, $x^3=1$ si, et seulement si, $(-x)^3=-x^3=-1$: il suffit de résoudre une équation pour en déduire les solutions de l'autre.

2. D'après la question précédente, quel que soit $n\in\mathbb{Z}$, l'un des trois facteurs de u_n est congru à 0 modulo 7, donc u_n est divisible par 7.

Par ailleurs, $X^3-1=(X-1)(X^2+X+1)$ et $X^3+1=(X+1)(X^2-X+1)$ (souvenirs de la somme géométrique), ce qui prouve que

$$u_n=(n-1)n(n+1)(n^2+n+1)(n^2-n+1).$$

En particulier, u_n est divisible par trois entiers consécutifs : $(n-1)$, n et $(n+1)$. Au moins l'un de ces trois entiers est pair ; exactement l'un de ces entiers est divisible par 3. Comme 2 et 3 sont premiers entre eux, le produit $(n-1)n(n+1)$ est donc divisible par $2\times3=6$.

Comme 6 et 7 sont premiers entre eux, on en déduit que u_n est divisible par $6\times7=42$.

Solution 25 23-25

1. L'élément 0 est solution si, et seulement si, $q=0$ (et p quelconque). On a donc trois couples solutions : $(0,0)$, $(1,0)$ et $(2,0)$.

❧ L'élément 1 est solution si, et seulement si, $1+p+q=0$. On a donc encore trois couples solutions : $(0,2)$, $(1,1)$ et $(2,0)$.

❧ Dans $\mathbb{Z}/3\mathbb{Z}$, on sait que $2^2=1$ et $2=-1$. L'élément 2 est donc solution si, et seulement si, $p=q+1$. On a donc trois couples solutions : $(1,0)$, $(2,1)$ et $(0,2)$.

2. Il y a trois éléments dans le corps $\mathbb{Z}/3\mathbb{Z}$, donc les couples (p,q) pour lesquels il existe au moins une solution ont tous été trouvés : ce sont les six couples précédents.

Il y a neuf couples dans $\mathbb{K}^2$, les couples pour lesquels il n'y a aucune solution sont donc :

$$(0,1),\quad (1,2),\quad (2,2).$$

✍ *Dans $\mathbb{Z}/3\mathbb{Z}$, il y a deux carrés : $0=0^2$ et $1=1^2=(-1)^2$, mais 2 n'est pas un carré. Les couples pour lesquels il n'y a pas de solution sont aussi ceux pour lesquels le discriminant $\Delta=p^2-q$ est égal à -1.*

Solution 26 23-26

Si l'entier $x_0\in\mathbb{Z}$ est une solution de ce système, alors l'entier $x\in\mathbb{Z}$ est une solution si, et seulement si, la différence $(x-x_0)$ est congrue à 0 modulo 9 et modulo 11.

Comme 9 et 11 sont premiers entre eux, un entier est divisible par 9 et par 11 si, et seulement si, il est divisible par $9\times11=99$.

❧ Un entier x est donc solution si, et seulement si, il existe un entier $k\in\mathbb{Z}$ tel que $x=x_0+99k$.

Solution 27 23-27

1. Il est clair que 2 appartient à E !

❧ Comme 9 est un multiple de 3, si $x=2 \pmod 9$, alors $x=2 \pmod 3$. La première équation est donc sans objet et il s'agit donc de résoudre un système de trois équations.

$$x=2 \pmod 5,\qquad x=2 \pmod 7,\qquad x=2 \pmod 9.$$

❧ Un entier $x\in\mathbb{Z}$ appartient donc à E si, et seulement si, la différence $(x-2)$ est congrue à 0 modulo 5, modulo 7 et modulo 9. Comme 5, 7 et 9 sont deux à deux premiers entre eux, un entier est divisible par 5, par 7 et par 9 si, et seulement si, il est divisible par le produit $5\times7\times9=315$.

Par conséquent, un entier $x \in \mathbb{Z}$ appartient à E si, et seulement si, il existe un entier $k \in \mathbb{Z}$ tel que $x = 2 + 315k$.

✍ *Comme* $p_1 = 5$, $p_2 = 7$ *et* $p_3 = 9$ *sont deux à deux premiers entre eux, les produits* $q_1 = p_2p_3 = 63$, $q_2 = p_1p_3 = 45$ *et* $q_3 = p_1p_2 = 35$ *sont premiers dans leur ensemble. L'algorithme de Blankinship nous donne*

$$-3 \times 63 - 2 \times 45 + 8 \times 35 = 1.$$

On pose donc $e_1 = -3 \times 63 = -189$, $e_2 = -2 \times 45 = -90$ *et* $e_3 = 8 \times 35 = 280$ *pour avoir*

$$(e_1, e_2, e_3) = (1, 0, 0) \pmod 5, \quad (e_1, e_2, e_3) = (0, 1, 0) \pmod 7, \quad (e_1, e_2, e_3) = (0, 0, 1) \pmod 9.$$

On en déduit que l'entier $a \cdot e_1 + b \cdot e_2 + c \cdot e_3$ *est une solution particulière du système*

$$x = a \pmod 5, \qquad x = b \pmod 7, \qquad x = c \pmod 9,$$

quels que soient les entiers a, b *et* c.

2. Pour k variant de -4 à -1, l'entier $2 + 315k$ prend les valeurs -1258, -943, -628, -313. Les éléments de E compris au sens large entre -1000 et -500 sont donc -943 et -628.

3. Si $x < y$ sont deux éléments consécutifs de E, alors la différence $y - x$ est égale à 315.
Le pgcd d de x et de y divise (par définition !) x et y, donc il divise la différence $y - x = 5 \times 7 \times 9$.
Par définition, un entier appartenant à E n'est divisible ni par 3, ni par 5, ni par 7.

✍ *Un entier* n *est divisible par* p *si, et seulement si,* $n = 0 \pmod p$.

Comme 3, 5 et 7 sont des nombres premiers, on en déduit que x est en fait premier à 5, à 7 et à $9 = 3^2$.

✍ *Si* p *est un nombre premier, alors il n'y a que deux possibilités : ou bien un entier* n *est un multiple de* p *; ou bien cet entier* n *est premier à* p.
En effet, le pgcd $n \wedge p$ *est un diviseur de* p, *donc il ne peut qu'être égal à* 1 *ou à* p.

Donc d, qui est en particulier un diviseur de x, est premier à 5, à 7 et à 9. Et comme d divise $5 \times 7 \times 9$, on en déduit finalement que $d = 1$.
Ainsi, deux entiers consécutifs de E sont premiers entre eux.

Solution 28 — 23-28

1. Les entiers congrus à 2 modulo 5 compris entre 0 et 10 sont 2 et 7. Il est clair que 7 est aussi congru à 1 modulo 3.

2. Soient a et b, deux entiers appartenant à S. Par définition, $a - 1 = 0 \pmod 3$ et $b - 2 = 0 \pmod 5$. Par conséquent,

$$(a-1)(b-2) = 0 \pmod 3 \qquad \text{et} \qquad (a-1)(b-2) = 0 \pmod 5.$$

Comme 3 et 5 sont premiers entre eux, un entier est divisible par 3 et par 5 si, et seulement si, il est divisible par $3 \times 5 = 15$. Par conséquent,

$$(a-1)(b-2) = 0 \pmod{15}$$

c'est-à-dire

$$(a-1)\big[(b-1)-1\big] = (a-1)(b-1) - (a-1) = 0 \pmod{15}$$

ou encore

$$(a-1)(b-1) = a - 1 \pmod{15}.$$

3. Comme $7 \in S$, un entier x appartient à S si, et seulement si,

$$x = 7 \pmod 3 \quad \text{et} \quad x = 7 \pmod 5$$

c'est-à-dire si la différence $(x - 7)$ est divisible par 3 et par 5, c'est-à-dire (voir plus haut) divisible par 15.
Un entier $x \in \mathbb{Z}$ appartient donc à S si, et seulement si, il existe un entier $k \in \mathbb{Z}$ tel que $x = 7 + 15k$.

Solution 29 23-29

Dans $\mathbb{Z}/4\mathbb{Z}$, l'élément $3 = -1$ est son propre inverse, donc

$$3x = 1 \pmod 4 \iff x = -1 \pmod 4.$$

Dans $\mathbb{Z}/5\mathbb{Z}$, il est clair que $2 \times 3 = 1$, donc

$$2x = 4 \pmod 5 \iff 2x = -1 \pmod 5 \iff x = -3 = 2 \pmod 5.$$

Il s'agit donc de résoudre le système suivant.

$$\big\{x = -1 \pmod 4, \quad x = 2 \pmod 5\big\}.$$

❧ Si $x_0 \in \mathbb{Z}$ est une solution de ce système, alors x est une solution si, et seulement si,

$$x - x_0 = 0 \pmod 4 \qquad \text{et} \qquad x - x_0 = 0 \pmod 5.$$

Comme 4 et 5 sont premiers entre eux, cela équivaut au fait que la différence $x - x_0$ soit divisible par $4 \times 5 = 20$.

❧ Pour trouver une solution particulière x_0, on résout l'équation de Bézout associée aux entiers 4 et 5. Comme $5 - 4 = 1$, on pose $e_1 = 5$ et $e_2 = -4$ de telle sorte que

$$e_1 = 1 \pmod 4, \quad e_1 = 0 \pmod 5, \qquad e_2 = 0 \pmod 4, \quad e_2 = 1 \pmod 5.$$

On en déduit que

$$x_0 = -1 \cdot e_1 + 2 \cdot e_2 = -13 = 7 \pmod{20}$$

est une solution particulière.

On a démontré que $x \in \mathbb{Z}$ est une solution du système considéré si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $x = 7 + 20k$.

Solution 30 23-30

Il est prudent de traduire cet équivalent sous la forme d'une limite :

$$\lim_{n\to+\infty} \frac{\pi_n \ln n}{n} = 1.$$

✍ *On peut toujours composer des limites, on ne peut pas toujours composer des équivalents.*

Par définition, $\pi_{p_n} = n$ pour tout entier $n \geqslant 1$ et comme l'ensemble des nombres premiers est infini, on sait que la suite (p_n) tend vers $+\infty$. Par composition de limites, on a donc

$$\lim_{n\to+\infty} \frac{n \ln p_n}{p_n} = 1 \tag{$\star$}$$

et aussi

$$\lim_{n\to+\infty} \frac{\ln \ln p_n}{\ln p_n} = 0 \tag{$\dagger$}$$

puisque $\ln \ln x = o(\ln x)$ lorsque x tend vers $+\infty$.

À nouveau par composition de limites (continuité de $\ln$ en 1), on déduit de $(\star)$ que

$$\lim_{n\to+\infty} \ln n + \ln \ln p_n - \ln p_n = 0,$$

ce qu'on peut aussi écrire sous la forme

$$\ln n - \ln p_n + o(\ln p_n) \underset{n\to+\infty}{=} o(1)$$

en tenant compte de $(\dagger)$.

Comme $\ln n$ et $\ln p_n$ tendent vers $+\infty$, on en déduit que

$$\ln n = \ln p_n + o(\ln p_n), \qquad \text{c'est-à-dire} \qquad \ln p_n \sim \ln n.$$

En revenant à $(\star)$, on en déduit enfin que

$$p_n \underset{n\to+\infty}{\sim} n \ln n.$$

Solution 31 23-31

Si le polynôme P est constant, alors P' est le polynôme nul et, dans ce cas, P' divise P si, et seulement si, $P = 0$. On supposera dans la suite que P n'est pas constant.

❧ Par linéarité de la dérivation, on peut supposer que le polynôme P est unitaire.

❧ On considère un polynôme P de degré $n \geqslant 1$.

Le polynôme dérivé P' divise le polynôme P si, et seulement si, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = QP'$. En comparant les degrés, on obtient $\deg Q = 1$ et en comparant les coefficients dominants de P et de P', on montre qu'il existe $\beta \in \mathbb{K}$ tel que

$$P = \frac{X-\beta}{n} P'. \qquad (\star)$$

❧ **Première méthode.** Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, on peut identifier le polynôme P à une application polynomiale de $\mathbb{R}$ dans $\mathbb{C}$ et l'équation $(\star)$ peut alors être traduite en équation différentielle :

$$\forall x \in \mathbb{R}, \quad y'(x) - \frac{x-\beta}{n} y(x) = 0$$

ce qui nous donne

$$\forall x \in \mathbb{R}, \quad y(x) = (x-\beta)^n.$$

✍ *On a supposé que le polynôme P était unitaire, ce qui détermine la constante d'intégration dans la résolution de l'équation différentielle.*

❧ **Deuxième méthode.** Quel que soit le corps $\mathbb{K}$, le polynôme (unitaire !) P admet une décomposition en produit de polynômes irréductibles unitaires :

$$P = \prod_{k=1}^{r} R_k^{m_k}$$

d'où on déduit

$$\frac{P'}{P} = \sum_{k=1}^{r} m_k \frac{R_k'}{R_k} \qquad (\dagger)$$

avec la formule de Leibniz.

Comme les R_k sont irréductibles, $R_k \wedge R_k' = 1$ et l'égalité $(\dagger)$ donne en fait la décomposition en éléments simples de la fraction rationnelle P'/P.

Mais la relation $(\star)$ nous donne une autre expression de cette décomposition en éléments simples :

$$\frac{P'}{P} = \frac{n}{X-\beta}.$$

L'unicité de cette décomposition prouve alors que la factorisation de P ne fait apparaître qu'un seul facteur irréductible : $R_1 = (X-\beta)$ avec la multiplicité $m_1 = n$. Donc $P = (X-\beta)^n$.

❧ **Troisième méthode.** *Proposée par Thomas Heinrich*

Partant de la relation $(\star)$, on démontre par récurrence que

$$\forall k \in \mathbb{N}, \qquad P^{(k)} = \frac{X-\beta}{n-k} P^{(k+1)}.$$

Comme P est un polynôme unitaire de degré n, alors $P^{(n)} = n!$ et

$$\begin{aligned} P &= \frac{X-\beta}{n} \cdot \frac{X-\beta}{n-1} \cdot \cdots \cdot \frac{X-\beta}{n-(n-1)} \cdot P^{(n)} \\ &= \frac{(X-\beta)^n}{n!} \cdot n! = (X-\beta)^n. \end{aligned}$$

❧ **Quatrième méthode.** On suppose que la caractéristique de $\mathbb{K}$ est strictement supérieure à n. L'application

$$\begin{array}{rcl} \varphi : \mathbb{K}_n[X] & \longrightarrow & \mathbb{K}_n[X] \\ P & \longmapsto & (X-\beta)P' \end{array}$$

est un endomorphisme de $\mathbb{K}_n[X]$. Dans la base

$$\mathscr{B}_\beta = \big(1, (X-\beta), (X-\beta)^2, \ldots, (X-\beta)^n\big),$$

la matrice de φ est diagonale :

$$\mathfrak{Mat}_{\mathscr{B}_\beta}(\varphi) = \mathrm{Diag}(0, 1, 2, \dots, n)$$

et comme les valeurs propres sont deux à deux distinctes, chaque sous-espace propre de φ est une droite vectorielle :

$$\forall\, 0 \leqslant k \leqslant n, \qquad \mathrm{Ker}(\varphi - k\,\mathrm{I}) = \mathbb{K} \cdot (X - \beta)^k.$$

La relation $(\star)$ signifie que P est un vecteur propre de φ associé à la valeur propre n. Par conséquent, les solutions de $(\star)$ sont les vecteurs du sous-espace propre

$$\mathrm{Ker}(\varphi - n\,\mathrm{I}) = \mathbb{K} \cdot (X - \beta)^n.$$

Solution 32 — 23-32

1. L'entier $n \in \mathbb{N}^*$ est fixé.

❧ Pour tout entier $k \in \mathbb{N}$, on considère les ensembles

$$C_k = \big\{m \in [\![1, n]\!] \,:\, \nu_p(m) = k\big\}$$
$$D_k = \big\{m \in [\![1, n]\!] \,:\, \nu_p(m) \geqslant k\big\} = \bigsqcup_{\ell \geqslant k} C_\ell.$$

Ces ensembles possèdent les propriétés suivantes :

(P_1) Si l'entier k est assez grand pour que $p^k > n$, les deux ensembles C_k et D_k sont vides.

(P_2) La famille $(C_k)_{k\in\mathbb{N}}$ est une recouvrement disjoint de l'intervalle $[\![1, n]\!]$.

(P_3) Pour tout $k \in \mathbb{N}$,

$$D_k = C_k \sqcup D_{k+1} \qquad \text{et donc} \qquad \#(D_k) = \#(C_k) + \#(D_{k+1}).$$

✍ *Un **recouvrement disjoint** de Ω est une famille $(E_i)_{i\in I}$ de parties deux à deux disjointes de Ω telles que*

$$\Omega = \bigsqcup_{i\in I} E_i.$$

*Une **partition** de Ω est un recouvrement disjoint $(E_i)_{i\in I}$ où chaque E_i est distinct de l'ensemble vide.*

❧ On en déduit que

$$\begin{aligned}
\nu_p(n!) &= \sum_{m=1}^{n} \nu_p(m) && \text{(p est un nombre \textit{premier})}\\
&= \sum_{k=0}^{+\infty} k\#(C_k) && \text{(sommation par paquets avec } (P_1) \text{ et } (P_2))\\
&= \sum_{k=1}^{+\infty} k\big(\#(D_k) - \#(D_{k+1})\big) && \text{(transformation d'Abel avec } (P_3))\\
&= \sum_{k=1}^{+\infty} k\#(D_k) - \sum_{k=2}^{+\infty} (k-1)\#(D_k) && (\text{(}P_1\text{)} \text{ et changement d'indice})\\
&= \#(D_1) + \sum_{k=2}^{+\infty} \#(D_k) = \sum_{k=1}^{+\infty} \#(D_k).
\end{aligned}$$

❧ L'ensemble D_k est constitué des multiples de p^k inférieurs à n. Le cardinal de D_k est donc égal à q si, et seulement si,

$$1 \leqslant 1 \cdot p^k < 2 \cdot p^k < q \cdot p^k \leqslant n < (q+1) \cdot p^k.$$

Autrement dit,

$$\forall\, k \in \mathbb{N}, \qquad \#(D_k) = \lfloor n \rfloor\, p^k.$$

✍ *On avait observé que D_k était vide lorsque $p^k > n$.*

On en déduit enfin que

$$\forall\, n \in \mathbb{N}^*, \qquad \nu_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

pour tout nombre premier p.

2. L'entier $n!$ est divisible par 10 si, et seulement si, il est divisible par 2 et par 5, donc pour tout entier $n \geqslant 5$.

La formule de Legendre nous dit que $v_p(n!)$ est une fonction croissante de n et une fonction décroissante de p. Par conséquent,

$$\forall\, n \in \mathbb{N}^*, \qquad v_5(n!) \leqslant v_2(n!).$$

De ce fait, si $v_5(n!) \geqslant d$, alors $n!$ est divisible par 2^d et par 5^d, donc par 10^d (puisque 2 et 5 sont premiers entre eux).

L'écriture décimale de $n!$ se termine donc par $v_5(n!)$ chiffres 0.

Solution 33 — 23-33

1. Les diviseurs de n sont les entiers de la forme

$$\prod_{k=1}^{s} p_k^{\beta_k}$$

où les exposants β_k sont des entiers tels que $0 \leqslant \beta_k \leqslant \alpha_k$. Ce sont des diviseurs sans facteur carré si, et seulement si,

$$\forall\, 1 \leqslant k \leqslant s, \qquad 0 \leqslant \beta_k \leqslant 1.$$

Il y a donc 2 valeurs possibles (0 et 1) pour chaque exposant β_k et comme il y a s exposants, il y a donc exactement 2^s diviseurs de n sans facteur carré.

❧ Parmi les diviseurs d de n, on distingue donc :
- — les diviseurs d ayant au moins un facteur carré, pour lesquels $\mu(d) = 0$;
- — les diviseurs d sans facteur carré, au nombre de 2^s, pour lesquels $\mu(d) = \pm 1$.

Classons les diviseurs sans facteur carré en fonction du nombre de leurs facteurs premiers (c'est-à-dire en fonction du nombre r d'exposants β_k égaux à 1) :
- — il y a un seul diviseur sans facteur premier : 1 (tous les β_k sont nuls) ;
- — il y a $s = \binom{s}{1}$ diviseur avec un seul facteur premier : les p_k (l'exposant β_k est égal à 1 et tous les autres β_ℓ sont nuls) ;
- — en général, il y a $\binom{s}{r}$ diviseurs avec r facteurs premiers (on choisit r exposants β_k parmi les s exposants possibles pour leur affecter la valeur 1, les autres exposants prenant la valeur 0) ;
- — il y a un seul diviseur avec s facteurs premiers : $d = \prod_{k=1}^{s} p_k$ (tous les β_k sont égaux à 1).

On a ainsi réalisé une partition de l'ensemble des diviseurs sans facteur premier de n et par conséquent

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \sum_{\substack{d|n \\ \text{avec facteur carré}}} 0 + \sum_{\substack{d|n \\ \text{sans facteur carré}}} \mu(d) \\
&= \sum_{r=0}^{s} \sum_{\substack{d|n \\ \text{sans facteur carré} \\ \text{avec } r \text{ facteurs premiers}}} \mu(d) \\
&= \sum_{r=0}^{s} \sum_{\substack{d|n \\ \text{sans facteur carré} \\ \text{avec } r \text{ facteurs premiers}}} (-1)^r \\
&= \sum_{r=0}^{s} \binom{s}{r} (-1)^r.
\end{aligned}$$

❧ Si $n \geqslant 2$, alors $s \geqslant 1$ et d'après la formule du binôme,

$$\sum_{r=0}^{s} \binom{s}{r} (-1)^r = [1 + (-1)]^s = 0.$$

Attention, l'entier $n = 1$ n'admet aucun facteur premier et la discussion précédente est sans objet dans ce cas. On constate seulement que

$$\sum_{d|1} \mu(d) = \mu(1) = 1$$

(puisque 1 est le produit de $r = 0$ nombres premiers deux à deux distincts).

2. L'application

$$[(p, q) \mapsto pq]$$

va de $I = \mathbb{N}^* \times \mathbb{N}^*$ dans $\mathbb{N}^*$, donc la famille $(I_n)_{n\in\mathbb{N}^*}$ réalise bien une partition de I (chaque élément de I appartient à un, et à un seul, des sous-ensembles I_n).

❧ Considérons la famille réelle

$$(u_{p,q})_{(p,q)\in I} = \left(\frac{\mu(q)}{p^2q^2}\right)_{(p,q)\in I}$$

et la partition $(C_p)_{p\in\mathbb{N}^*}$ de I définie par

$$\forall\, p \in \mathbb{N}^*, \quad C_p = \left\{(p,q),\ q \in \mathbb{N}^*\right\}$$

(on aura compris que C_p est la *Colonne* d'abscisse p).

Pour tout $p \in \mathbb{N}^*$,

$$\forall\, (p,q) \in C_p, \quad |u_{p,q}| = \frac{1}{p^2}\cdot\frac{|\mu(q)|}{q^2} \leqslant \frac{1}{q^2}$$

donc la sous-famille $(|u_{p,q}|)_{(p,q)\in C_p}$ est sommable, de somme

$$\sigma_p = \frac{1}{p^2}\cdot\sum_{q=1}^{+\infty}\frac{|\mu(q)|}{q^2} \leqslant \frac{\pi^2}{6}\cdot\frac{1}{p^2}$$

puisque $|\mu(q)| \leqslant 1$ pour tout entier $q \geqslant 1$.

Comme la série $\sum \sigma_p$ est absolument convergente, on en déduit que la famille $(u_{p,q})_{(p,q)\in I}$ est sommable (premier théorème de Fubini).

❧ D'après le second théorème de Fubini appliqué à la partition $(C_p)_{p\in\mathbb{N}^*}$ de I,

$$\begin{aligned}\sum_{(p,q)\in I} u_{p,q} &= \sum_{p=1}^{+\infty}\left(\sum_{(p,q)\in C_p} u_{p,q}\right)\\ &= \sum_{p=1}^{+\infty}\left(\frac{1}{p^2}\sum_{q=1}^{+\infty}\frac{\mu(q)}{q^2}\right)\\ &= \left(\sum_{p=1}^{+\infty}\frac{1}{p^2}\right)\left(\sum_{q=1}^{+\infty}\frac{\mu(q)}{q^2}\right).\end{aligned}$$

❧ Comme la famille $(u_{p,q})_{(p,q)\in I}$ est sommable, alors pour chaque $n \in \mathbb{N}^*$, la sous-famille $(u_{p,q})_{(p,q)\in I_n}$ est sommable et sa somme vaut

$$\sum_{(p,q)\in I_n} u_{p,q} = \sum_{(p,q)\in I_n}\frac{\mu(q)}{n^2} = \sum_{q\mid n}\frac{\mu(q)}{n^2}.$$

D'après le second théorème de Fubini appliqué à la partition $(I_n)_{n\in\mathbb{N}^*}$,

$$\begin{aligned}\sum_{(p,q)\in I} u_{p,q} &= \sum_{n=1}^{+\infty}\left(\sum_{(p,q)\in I_n} u_{p,q}\right)\\ &= \sum_{n=1}^{+\infty}\left(\sum_{q\mid n}\frac{\mu(q)}{n^2}\right).\end{aligned}$$

D'après la première question,

$$\sum_{q\mid 1}\frac{\mu(q)}{1^2} = 1 \quad \text{et} \quad \forall\, n \geqslant 2, \quad \sum_{q\mid n}\frac{\mu(q)}{n^2} = 0.$$

❧ On a ainsi démontré la **Formule d'inversion de Möbius** :

$$\left(\sum_{p=1}^{+\infty}\frac{1}{p^2}\right)\left(\sum_{q=1}^{+\infty}\frac{\mu(q)}{q^2}\right) = 1.$$

Solution 34 23-34

Comme 37 est premier, alors $\mathbb{K} = \mathbb{Z}/37\mathbb{Z}$ est un corps et la théorie des systèmes linéaires s'applique sur $\mathbb{K}$ comme elle s'applique sur $\mathbb{R}$ ou sur $\mathbb{C}$.

Par la méthode du pivot

Dans le *corps* $\mathbb{Z}/37\mathbb{Z}$, on a $\mathscr{C}(3) \neq \mathscr{C}(0)$, donc $\mathscr{C}(3)$ est inversible et l'opération de pivot $(L_1 \leftarrow [\mathscr{C}(3)]^{-1}L_1)$ en $\star$ est donc légitime. Remarquer que, comme 21 et 30 sont multiples de 3 dans $\mathbb{Z}$, il est inutile à ce stade de calculer explicitement $[\mathscr{C}(3)]^{-1}$.

$$\begin{aligned}
\begin{cases} 6x + 7y = 30 \\ 3x - 7y = 0 \end{cases} &\sim \begin{cases} 21y = 30 \\ 3x - 7y = 0 \end{cases} && (L_1 \leftarrow L_1 - 2L_2)\\
&\sim \begin{cases} 7y = 10 \\ 3x - 7y = 0 \end{cases} && \star\\
&\sim \begin{cases} 7y = 10 \\ 3x = 10 \end{cases} && (L_2 \leftarrow L_2 + L_1)
\end{aligned}$$

Le système est maintenant découplé, il ne reste plus qu'à résoudre (séparément) les deux équations qui le constituent.

Comme $\mathscr{C}(3) \neq \mathscr{C}(0)$ et $\mathscr{C}(7) \neq \mathscr{C}(0)$, alors les deux coefficients $\mathscr{C}(3)$ et $\mathscr{C}(7)$ sont inversibles dans $\mathbb{Z}/37\mathbb{Z}$, donc le système admet une, et une seule, solution qu'on obtient en explicitant les inverses de $\mathscr{C}(3)$ et de $\mathscr{C}(7)$ par résolution de l'équation de Bézout.

Avec une méthode quelconque (éventuellement le concours de la calculatrice), on obtient

$$3 \times 25 - 2 \times 37 = 1 \quad \text{et} \quad 7 \times 16 - 3 \times 37 = 1$$

donc $[\mathscr{C}(3)]^{-1} = \mathscr{C}(25)$ et $[\mathscr{C}(7)]^{-1} = \mathscr{C}(16)$. Par conséquent, l'unique solution du système est

$$(25 \times 10, 16 \times 10) = (28, 12) \pmod{37}.$$

Avec les formules de Cramer

Le système étudié a pour matrice

$$A = \begin{pmatrix} 6 & 7 \\ 3 & -7 \end{pmatrix}$$

dont le déterminant est égal à

$$6 \times (-7) - 3 \times 7 = -63 = 11 \pmod{37}.$$

Comme $\mathscr{C}(11) \neq \mathscr{C}(0)$, alors $\mathscr{C}(11)$ est inversible dans $\mathbb{Z}/37\mathbb{Z}$, donc le système admet une, et une seule, solution, qui est donnée par les formules de Cramer.

$$\begin{aligned}
11x &= \begin{vmatrix} 30 & 7 \\ 0 & -7 \end{vmatrix} = 12 \pmod{37}\\
11y &= \begin{vmatrix} 6 & 30 \\ 3 & 0 \end{vmatrix} = 21 \pmod{37}
\end{aligned}$$

Il reste à calculer $[\mathscr{C}(11)]^{-1}$: les opérations de pivot

$$\begin{aligned}
\begin{pmatrix} 1 & 0 & 37 \\ 0 & 1 & 11 \end{pmatrix} &\sim \begin{pmatrix} 1 & -3 & 4 \\ 0 & 1 & 11 \end{pmatrix} && (L_1 \leftarrow L_1 - 3L_2)\\
&\sim \begin{pmatrix} 1 & -3 & 4 \\ -3 & 10 & -1 \end{pmatrix} && (L_2 \leftarrow L_2 - 3L_1)
\end{aligned}$$

montrent que $3 \times 37 - 10 \times 11 = 1$ et donc que $[\mathscr{C}(11)]^{-1} = \mathscr{C}(-10)$. Par conséquent,

$$x = -10 \times 12 = 28 \pmod{37} \quad \text{et} \quad y = -10 \times 21 = 12 \pmod{37}.$$

Solution 35 — 23-35

Quels que soient les entiers naturels *non nuls* p et q, le pgcd de p et q est supérieur à 1, donc il existe un, et un seul, entier naturel $n = p \wedge q \in \mathbb{N}^*$ tel que $(p, q) \in I_n$. La famille $(I_n)_{n\in\mathbb{N}^*}$ est donc une *partition dénombrable* de I.

❧ Soit $(\alpha, \beta) \in I_1$. On pose $(a, b) = (n\alpha, n\beta)$.

Quels que soient x et y dans $\mathbb{Z}$,

$$ax + by = n(\alpha x + \beta y) \in n\mathbb{Z}$$

donc $a\mathbb{Z} + b\mathbb{Z} \subset n\mathbb{Z}$.

Réciproquement, comme α et β sont premiers entre eux, il existe deux entiers u et v tels que $\alpha u + \beta v = 1$. On en déduit que

$$n = n \times 1 = n(\alpha u + \beta v) = au + bv \in a\mathbb{Z} + b\mathbb{Z}.$$

Par conséquent, $n\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.

Finalement, on a $n\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, ce qui prouve que $(a, b) \in I_n$ et donc que l'application est bien définie de I_1 dans I_n.

❧ Comme l'entier n n'est pas nul et que l'anneau $\mathbb{Z}$ est intègre, l'application $(\alpha, \beta) \mapsto (n\alpha, n\beta)$ est *injective*.

❧ Enfin, si $(a, b) \in I_n$, alors il existe deux entiers α et β tels que $a = n\alpha$ et $b = n\beta$. En outre (Bézout), il existe deux entiers u et v tels que

$$n = au + bv = n(\alpha u + \beta v).$$

Comme $n \neq 0$ et que l'anneau $\mathbb{Z}$ est intègre, on en déduit que

$$\alpha u + \beta v = 1$$

et donc que $(\alpha, \beta) \in I_1$.

Cela prouve que l'application $(\alpha, \beta) \mapsto (n\alpha, n\beta)$ est surjective de I_1 sur I_n.

❧ Pour tout $(p, q) \in I$, on note $u_{p,q} = 1/p^2q^2$. On remarque (une fois pour toute) que $(u_{p,q})_{(p,q)\in I}$ est une famille de *réels positifs* et on considère la partition $(J_p)_{p\in\mathbb{N}^*}$ de I définie par

$$\forall\, p \in \mathbb{N}^*, \quad J_p = \{(p, q),\ q \in \mathbb{N}^*\}.$$

❧ Pour tout $q \in \mathbb{N}$ *fixé*,

$$u_{p,q} = \mathcal{O}\Big(\frac{1}{p^2}\Big)$$

et comme $\sum 1/p^2$ est une série convergente de terme général positif, on en déduit que la sous-famille $(u_{p,q})_{(p,q)\in J_p}$ est sommable.

❧ Pour tout entier $p \geqslant 1$,

$$\sigma_p = \sum_{(p,q)\in J_p} u_{p,q} = \frac{\zeta(2)}{p^2}$$

ce qui prouve que la famille de réels positifs $(\sigma_p)_{p\in\mathbb{N}^*}$ est sommable.

D'après le théorème de Fubini, la famille $(u_{p,q})_{(p,q)\in I}$ est sommable et

$$\sum_{(p,q)\in I} u_{p,q} = \sum_{p=1}^{+\infty} \sigma_p = [\zeta(2)]^2.$$

❧ Comme la famille $(u_{p,q})_{(p,q)\in I}$ est sommable, alors pour chaque entier $n \geqslant 1$, la sous-famille $(u_{p,q})_{(p,q)\in I_n}$ est sommable et

$$\begin{aligned}[\zeta(2)]^2 &= \sum_{n=1}^{+\infty}\Big[\sum_{(p,q)\in I_n} u_{p,q}\Big] = \sum_{n=1}^{+\infty}\Big[\frac{1}{n^4}\sum_{(p,q)\in I_1} u_{p,q}\Big] \\ &= \zeta(4)\sum_{(p,q)\in I_1} u_{p,q}\end{aligned}$$

puisque, en utilisant la bijection étudiée plus haut,

$$\sum_{(a,b)\in I_n} \frac{1}{a^2b^2} = \sum_{(\alpha,\beta)\in I_1} \frac{1}{(n\alpha)^2(n\beta)^2} = \frac{1}{n^4}\sum_{(\alpha,\beta)\in I_1} \frac{1}{\alpha^2\beta^2}.$$

Solution 36 — 23-36

1. Il s'agit, semble-t-il, de vérifier une infinité de propriétés (*pour tout* $a \in \mathbb{N}^*$...), ce qu'un ordinateur ne sait pas faire !

Cependant, si $a = b \pmod n$, alors $a^k = b^k \pmod n$ pour tout entier $k \in \mathbb{N}$. Par conséquent, pour vérifier que $a^n = a \pmod n$ pour tout $a \in \mathbb{N}^*$, il suffit de vérifier cette relation pour tout $0 \leqslant a < n$. Il n'y a donc qu'un nombre *fini* de vérifications à effectuer.

❧ On suppose connue une fonction booléenne `estPremier(n)` qui retourne `True` si, et seulement si, l'entier n est premier.

❧ La fonction suivante calcule a^n comme le terme de rang n de la suite géométrique de raison a et de premier terme 1.

```
def puissance(a, n):
  p = 1                # Initialisation : p_0 = 1
  for i in range(n):   # Itération : ∀ 0 ⩽ i < n,
    p = p*a            #                 p_{i+1} = a p_i
  return p             # p_n = a^n
```

On modifie cette fonction pour calculer a^n modulo n en réduisant modulo n *chaque* puissance calculée, de manière à ne manipuler que des entiers compris entre 0 et $(n-1)$.

```
def puissanceModn(a, n):
  p = 1
  for i in range(n):
    p = (p*a)%n        # Réduction modulo n
  return p
```

On pourrait rendre ce calcul plus efficace avec l'algorithme d'exponentiation rapide, d'autant plus efficace que l'exposant n est grand.

❧ Si l'entier n est premier, ce n'est pas un nombre de Carmichael.
S'il est composé, on vérifie si $a^n = a \pmod n$ pour chaque entier $2 \leqslant a < n$.
— S'il existe un entier a tel que $a^n \neq a \pmod n$, on sort de la boucle dès qu'on en trouve un (en retournant `False`).
— Sinon, la boucle va jusqu'à son terme et on termine en retournant `True`.

```
def estCarmichael(n):
  if estPremier(n):
    return False
  else:
  # Cas où l'entier ?n? est composé
    for a in range(2, n):
    # La vérification échoue pour a^n ≠ a (mod n).
      echec = (puissanceModn(a, n)!=a)
      # On arrête la vérification au premier échec.
      if echec:
        return False
    # On n'arrive ici que si a^n = a (mod n)
    # pour tout 0 ⩽ a < n.
    return True
```

2. On suppose qu'il existe deux entiers p et m tels que $n = p^2m$ et on pose $a = 1+pm$. D'après la formule du binôme,

$$a^n = (1+pm)^n = 1 + \binom{n}{1}pm + \sum_{k=2}^{n}\binom{n}{k}(pm)^k.$$

Or $\binom{n}{1} = n$, donc $\binom{n}{1}pm$ est divisible par n et pour tout entier $k \geqslant 2$, le terme

$$\binom{n}{k}(pm)^k = (p^2m)\underbrace{\left[\binom{n}{k}p^{k-2}m^{k-1}\right]}_{\in\mathbb{N}}$$

est divisible par $n = p^2m$. Ainsi $a^n = 1 \pmod n$.

Mais par hypothèse, $a^n = a \pmod n$, c'est-à-dire

$$a^n = 1 + pm \pmod n.$$

Comme $p \geqslant 2$, alors $0 < pm < p^2m = n$, donc $pm \neq 0 \pmod n$, donc

$$1 + pm \neq 1 \pmod n$$

et la contradiction est établie.

Ainsi, un nombre de Carmichael n'est pas divisible par le carré d'un entier et en particulier, la décomposition en produit de facteurs premiers d'un tel nombre est de la forme $p_1p_2\cdots p_r$ où les facteurs premiers $p_1, \ldots, p_r$ sont deux à deux distincts.

❧ Pour information, les nombres de Carmichael inférieurs à 10 000 sont les suivants.

$561 = 3.11.17$
$1\,105 = 5.13.17$
$1\,729 = 7.13.19$
$2\,465 = 5.17.29$
$2\,821 = 7.13.31$
$6\,601 = 7.23.41$
$8\,911 = 7.19.67$

Solution 37 23-37

On cherche la liste des éléments inversibles de $\mathbb{Z}/78\mathbb{Z}$, c'est-à-dire des entiers $0 \leqslant a < 78$ qui sont premiers à 78.

Or $78 = 2 \cdot 3 \cdot 13$, donc a est premier à 78 si, et seulement si, a est premier à 2, à 3 et à 13.

Comme 2, 3 et 13 sont premiers, l'entier a est premier à 78 si, et seulement si, $a \notin 2\mathbb{Z}$ et $a \notin 3\mathbb{Z}$ et $a \notin 13\mathbb{Z}$.

❧ On va donc procéder de la manière suivante :
- on constitue la liste des entiers $0 \leqslant a < 78$;
- on supprime de cette liste les entiers multiples de 2 ;
- puis les multiples de 3
- et enfin les multiples de 13.

❧ En pratique, on considère une liste de booléens $(b_i)_{0\leqslant i<78}$ et supprimer l'entier i consiste à affecter la valeur `False` au booléen b_i.

```
n = 78
diviseurs = [2, 3, 13]
premiers = [True]*n
# Pour chaque diviseur d de n,
for d in diviseurs:
  # l'entier m parcourt l'ensemble des multiples de d
  # qui sont strictement inférieurs à n.
  m = 0          # m_0 = 0
  while (m<n):
    premiers[m] = False
    m += d       # m_{k+1} = m_k + d = (k+1)m
```

❧ Il reste à constituer la liste des indices $0 \leqslant i < 78$ pour lesquels le booléen b_i est resté à la valeur `True`.

```
inversibles = [i for i in range(n) if premiers[i]]
```

❧ **Variante**

On peut aussi parcourir la liste des entiers $0 \leqslant i < 78$ et, pour chacun d'eux, vérifier s'il s'agit d'un multiple d'un des diviseurs de 78 : l'entier i est un multiple d'un diviseur de 78 si, et seulement si,

$$\exists\, d \in \{2,3,13\}, \qquad i = 0 \pmod{d}$$

```
for i in range(n):
  multiple = False
  for d in diviseurs:
    multiple = multiple or (i%d==0)
  premiers[i] = not(multiple)
```

ou encore :

$$\forall\, d \in \{2,3,13\}, \qquad i \neq 0 \pmod{d}.$$

```
for i in range(n):
  premier = True
  for d in diviseurs:
    premier = premier and (i%d!=0)
  premiers[i] = premier
```

❧ **Généralisation**

❧ Pour étendre le calcul précédent au cas d'un entier naturel n quelconque, il faut savoir calculer la liste de ses facteurs premiers.

En admettant que la fonction `diviseurs_premiers(n)` retourne la liste des diviseurs premiers de n, l'étude précédente conduit à la fonction suivante.

```
def inversibles_modulo(n):
  diviseurs = diviseurs_premiers(n)
  premiers = [True]*n
  for d in diviseurs:
    m = 0
    while (m<n):
      premiers[m] = False
      m += d
  return [i for i in range(n) if premiers[i]]
```

❧ Chaque entier n peut se décomposer en produit de facteurs premiers :

$$n = 2^{m_2} \cdot 3^{m_3} \cdot 5^{m_5} \cdot \dots$$

où les multiplicités m_i sont des entiers naturels presque tous nuls.

❧ Pour chaque nombre premier p, on va effectuer la division de n par p : si cette division tombe juste, on enregistre l'entier p et on continue la recherche.

❧ Pour l'entier

$$x_1 = n = p_1^{\mu_1} \cdot p_2^{\mu_2} \cdot \dots \cdot p_r^{\mu_r}$$

(où $p_1 < p_2 < \dots < p_r$), on va passer en revue les nombres premiers jusqu'à p_1, enregistrer la valeur de p_1, remplacer x_1 par

$$x_2 = p_2^{\mu_2} \cdot \dots \cdot p_r^{\mu_r},$$

passer en revue les nombres premiers jusqu'à p_2, enregistrer la valeur de p_2, remplacer x_2 par

$$x_3 = p_3^{\mu_3} \cdot \dots \cdot p_r^{\mu_r}$$

et ainsi de suite.

❧ On a besoin d'une fonction qui retourne le quotient de $n = x_k$ par $p_k^{\mu_k}$ lorsque $p = p_k$ est un facteur premier de n. Pour cela, il est inutile de calculer μ_k : il suffit de diviser n par $p = p_k$ *tant que* c'est possible.

```
def purger(n, p):
  q = n//p
  while (q%p==0):
    q = q//p
  return q
```

Le code précédent suppose que l'argument n est divisible par l'argument p puisqu'il calcule le quotient de n par p sans vérifier si le reste est nul.

❧ **Terminaison de l'algorithme**

— Si l'entier x_k est composé, on sait qu'il admet un diviseur premier p_k tel que

$$p_{k-1} < p_k \quad \text{et} \quad p_k^2 \leqslant n_k.$$

En particulier, si x_r est composé, alors $x_r = p_r^{\mu_r}$ avec $\mu_r \geqslant 2$ et l'algorithme s'arrête à l'étape suivante avec $x_{r+1} = 1$.

— Si l'entier x_k n'est pas composé, c'est qu'il est premier $x_k = x_k$. Dans ce cas, $k = r$, $x_r = p_r^1$ et $\mu_r = 1$: la recherche des facteurs premiers est alors finie.

```
def diviseurs_premiers(n):
  L = []
  x = n
  if (x%2==0):
  L.append(2)
  x = purger(x,2)
p = 3
while (p**2<=x):  # Tant que x est composé...
  if (x%p==0):
    L.append(p)
    x = purger(x,p)
    # Si μ_r ⩾ 2, alors x_{r+1} = 1.
    # Si μ_r = 1, alors x_r = p_r < p_r^2.
  p += 2
if (x>1):   # Cas μ_r = 1
  L.append(x)
return L
```

❧ **Efficacité de l'algorithme**

Après avoir trouvé $p_1, \dots, p_{k-1}$, on passe en revue les entiers impairs supérieurs à p_{k-1} : le plus petit diviseur de

$$x_k = p_k^{\mu_k} \cdot \dots \cdot p_r^{\mu_r}$$

est forcément premier, puisqu'il s'agit de p_k. Autrement dit, deux cas peuvent se présenter :

— si p divise x, il est forcément premier ;

— si p ne divise pas x, peu importe que p soit premier ou non !

Ainsi, pour chaque nombre impair p, on effectue seulement

— une division euclidienne (pour vérifier si p divise x)

— et une multiplication (pour vérifier si la boucle `while` doit se poursuivre).

On ne cherche surtout pas à vérifier si p est premier ou non : ce serait aussi long qu'inutile.

Solution 38 23-38

On considère un isomorphisme d'anneaux

$$\varphi : (A, +, \star) \to (B, \oplus, \otimes).$$

Cette bijection admet une bijection réciproque

$$\psi : B \to A$$

telle que

$$\forall x \in A, \quad \psi \circ \varphi(x) = x, \tag{2}$$
$$\forall y \in B, \quad \varphi \circ \psi(y) = y. \tag{3}$$

❧ **Additions**

Soient y_1 et y_2 dans B. On pose alors

$$x_1 = \psi(y_1) \in A \quad \text{et} \quad x_2 = \psi(y_2) \in A$$

de telle sorte que

$$y_1 = \varphi(x_1) \quad \text{et} \quad y_2 = \varphi(x_2)$$

par (3).

Alors

$$\begin{aligned} \psi(y_1 \oplus y_2) &= \psi\big(\varphi(x_1) \oplus \varphi(x_2)\big) \\ &= \psi\big(\varphi(x_1 + x_2)\big) && \text{(a)} \\ &= x_1 + x_2 && \text{(par (2))} \\ &= \psi(y_1) + \psi(y_2) \end{aligned}$$

où l'égalité (a) provient du fait que φ est un morphisme d'anneaux.

❧ **Multiplications**

On reprend les mêmes notations.

$$\begin{aligned} \psi(y_1 \otimes y_2) &= \psi\big(\varphi(x_1) \otimes \varphi(x_2)\big) \\ &= \psi\big(\varphi(x_1 \star x_2)\big) && \text{(b)} \\ &= x_1 \star x_2 && \text{(par (2))} \\ &= \psi(y_1) \star \psi(y_2) \end{aligned}$$

où l'égalité (b) provient elle aussi de la propriété de morphisme de φ.

❧ **Unités**

Enfin, comme $\varphi(1_A) = 1_B$ (puisque $\varphi : A \to B$ est un morphisme d'anneaux), on peut déduire de (2) que

$$\psi(1_B) = \psi \circ \varphi(1_A) = 1_A.$$

❧ Ces trois propriétés montrent que ψ, bijection réciproque de φ, est bien un morphisme d'anneaux de $(B, \oplus, \otimes)$ dans $(A, +, \star)$.

Solution 39 23-39

Il est clair que $\mathscr{C}_a \subset A$.

❧ Par définition de l'élément neutre (pour $*$),

$$a * 1_A = 1_A * a$$

donc $1_A \in \mathscr{C}_a$.

❧ Quels que soient x et y dans $\mathscr{C}_a$,

$$\begin{aligned} a*(x*y) &= (a*x)*y && \text{(associativité)}\\ &= (x*a)*y && (\text{car } x\in\mathscr{C}_a)\\ &= x*(a*y) && \text{(associativité)}\\ &= x*(y*a) && (\text{car } y\in\mathscr{C}_a)\\ &= (x*y)*a && \text{(associativité)} \end{aligned}$$

donc le produit $x*y$ appartient aussi à $\mathscr{C}_a$.

❧ Dans une algèbre, les deux lois internes $+$ et $*$ sont associatives mais il existe une sorte d'*associativité étendue* qui assure que

$$(\lambda\cdot x)*y = \lambda\cdot(x*y) = x*(\lambda\cdot y)$$

quels que soient les vecteurs x et y, quel que soit le scalaire λ. Cette propriété sera notée (AE) dans le raisonnement suivant.

Quels que soient x et y dans $\mathscr{C}_a$, quel que soit $\lambda\in\mathbb{K}$,

$$\begin{aligned} (\lambda\cdot x+y)*a &= (\lambda\cdot x)*a+(y*a) && \text{(distributivité)}\\ &= \lambda\cdot(x*a)+(y*a) && \text{(AE)}\\ &= \lambda\cdot(a*x)+(a*y) && (\text{car } x\in\mathscr{C}_a \text{ et } y\in\mathscr{C}_a)\\ &= a*(\lambda\cdot x)+(a*y) && \text{(AE)}\\ &= a*(\lambda\cdot x+y) && \text{(distributivité)} \end{aligned}$$

donc la combinaison linéaire $\lambda\cdot x+y$ appartient aussi à $\mathscr{C}_a$.

❧ Ainsi, le commutant $\mathscr{C}_a$ est bien une sous-algèbre de $(A,+,*,\cdot)$.

✍ *Dans $\mathscr{C}_a$, tous les vecteurs commutent au vecteur de référence a (par définition même de $\mathscr{C}_a$), ce qui ne veut pas dire que les vecteurs commutent entre eux !*

Dans $A=\mathfrak{M}_3(\mathbb{R})$, si on prend $a=I_3$, alors $\mathscr{C}_a=\mathfrak{M}_3(\mathbb{R})$, ce qui montre bien que le commutant de a n'est pas toujours une sous-algèbre commutative.

Cela dit, les règles de calcul sur les puissances montrent que

$$\forall\, a\in A,\quad \mathbb{K}[a]\subset\mathscr{C}_a$$

et il arrive que $\mathscr{C}_a=\mathbb{K}[a]$. Dans ce cas, $\mathscr{C}_a$ est bien une sous-algèbre commutative (car la sous-algèbre $\mathbb{K}[a]$ des polynômes en a est, elle, toujours commutative.)

Solution 40 — 23-40

Pour des raisons techniques, nous allons procéder dans le désordre, en commençant par établir les propriétés les plus simples et non pas par ce qui serait logique, c'est-à-dire en vérifiant que l'ensemble G est une partie de $\mathbb{R}_+^*$ qui est stable par $\times$.

❧ Comme la multiplication est associative sur $\mathbb{R}$, elle est en particulier associative sur G.

❧ Il est clair que $1=1+\sqrt{3}\cdot 0$ et que $1^2-3\cdot 0^2=1$, donc $1\in G$.

❧ Supposons que le réel $x+\sqrt{3}y$ appartienne à l'ensemble G. Il est alors clair que le réel $x-\sqrt{3}y$ appartient aussi à G et comme

$$x^2-3y^2=(x-\sqrt{3}y)(x+\sqrt{3}y)=1>0,$$

les deux facteurs sont non nuls et de même signe.

Si $y\in\mathbb{N}$, alors $x+\sqrt{3}y>0$ (puisque x et y sont positifs) et par conséquent $x-\sqrt{3}y>0$.

Si, au contraire, $-y\in\mathbb{N}$, alors $x-\sqrt{3}y>0$ (puisque x et $-y$ sont positifs) et par conséquent $x+\sqrt{3}y>0$.

Bref, tout élément de G appartient à $\mathbb{R}_+^*$ et son inverse en tant qu'élément de $\mathbb{R}_+^*$:

$$(x+\sqrt{3}y)^{-1}=x-\sqrt{3}y$$

appartient aussi à G.

❧ Considérons enfin deux éléments $z_1=x_1+\sqrt{3}y_1$ et $z_2=x_2+\sqrt{3}y_2$ dans G et calculons leur produit :

$$z_1z_2=\underbrace{(x_1x_2+3y_1y_2)}_{\in\mathbb{Z}}+\sqrt{3}\underbrace{(x_1y_2+x_2y_1)}_{\in\mathbb{Z}}.$$

Comme z_1 et z_2 sont strictement positifs, alors

$$0 \leqslant \sqrt{3}|y_1| < x_1 \quad \text{et} \quad 0 \leqslant \sqrt{3}|y_2| < x_2$$

donc, par produit,

$$3|y_1 y_2| < x_1 x_2$$

et donc $x_1x_2 + 3y_1y_2 \in \mathbb{N}$.

D'autre part,

$$\begin{aligned}(x_1x_2 + 3y_1y_2)^2 - 3(x_1y_2 + x_2y_1)^2 &= x_1^2x_2^2 + 9y_1^2y_2^2 - 3x_1^2y_2^2 - 3x_2^2y_1^2\\ &= x_1^2(x_2^2 - 3y_2^2) - 3y_1^2(x_2^2 - 3y_2^2)\\ &= x_1^2 - 3y_1^2 = 1.\end{aligned}$$

On a bien prouvé que le produit z_1z_2 appartenait à G et donc que G était un sous-groupe de $(\mathbb{R}_+^*, \times)$.

✍ *On peut vérifier que* G *est le sous-groupe engendré par* $2+\sqrt{3}$*, c'est-à-dire*

$$G = \left\{(2+\sqrt{3})^n,\ n \in \mathbb{Z}\right\}$$

(en vérifiant que $H = \{\ln z,\ z \in G\}$ *est un sous-groupe discret de* $(\mathbb{R}, +)$*).*

Solution 41 — 23-41

1. Soit $B_0 = \varphi_*(A)$, l'image de l'anneau A par le morphisme φ. Nous allons montrer que B_0 est un sous-anneau de $(B, \oplus, \otimes)$ avec la caractérisation habituelle.

- Tout d'abord, il est clair que $\varphi_*(A)$ est contenu dans B.
- Ensuite, par définition des morphismes d'anneaux,

$$1_B = \varphi(1_A) \in \varphi_*(A).$$

- Enfin, quels que soient x et y dans B_0, il existe u et v dans A tels que

$$x = \varphi(u) \quad \text{et} \quad y = \varphi(v).$$

D'après les propriétés des morphismes,

$$\begin{aligned}x - y &= \varphi(u) - \varphi(v)\\ &= \varphi(u - v) && \text{car } u - v = u + n\cdot v \text{ avec } n = -1\\ &\in \varphi_*(A) && \text{car A est stable par différence}\\ x \otimes y &= \varphi(u) \otimes \varphi(v)\\ &= \varphi(u \star v) && \text{morphisme}\\ &\in \varphi_*(A) && \text{car A est stable par } \star\end{aligned}$$

Tout cela prouve que $\varphi_*(A)$ est un sous-anneau de $(B, \oplus, \otimes)$.

2. Si $x \in A$ est inversible, alors il existe $y \in A$ tel que $x \star y = y \star x = 1_A$ et comme φ est un morphisme d'anneaux,

$$\varphi(x) \otimes \varphi(y) = \varphi(x \star y) = \varphi(y \star x) = \varphi(y) \otimes \varphi(x) = \varphi(1_A) = 1_B$$

donc $\varphi(x)$ est un élément inversible de B, dont l'inverse est $\varphi(x^{-1})$.

- Réciproquement, si $\varphi(x)$ est un élément inversible de B, alors $x = \varphi^{-1}\left[\varphi(x)\right]$ est un élément inversible de A (en tant qu'image d'un élément inversible de B par un morphisme d'anneaux de B dans A, on vient de le vérifier).

On en déduit que : si $\varphi : A \to B$ est un isomorphisme d'anneaux, alors $x \in A$ est inversible si, et seulement si, $\varphi(x)$ est un élément inversible dans B.

Solution 42 — 23-42

ont même polynôme minimal (s'ils en ont un).

Comme φ est un morphisme d'algèbres, on sait que

$$\forall\, P \in \mathbb{K}[X], \quad \varphi\big(P(a)\big) = P\big(\varphi(a)\big).$$

Première version

Si P_0 est le polynôme minimal de a, alors $P_0(a) = 0_A$ et par suite

$$P_0\big(\varphi(a)\big) = \varphi(0_A) = 0_B,$$

donc P_0 est un polynôme annulateur de $b = \varphi(a)$. De ce fait, b admet un polynôme minimal et ce polynôme minimal divise P_0.

Réciproquement, si Q_0 est le polynôme minimal de b, alors $Q_0(b) = 0_B$ et comme φ est un *iso*morphisme d'algèbres,

$$Q_0(a) = Q_0\big(\varphi^{-1}(b)\big) = \varphi^{-1}\big(Q_0(b)\big) = \varphi^{-1}(0_B) = 0_A$$

donc Q_0 est un polynôme annulateur de a. Comme précédemment, on en déduit que le polynôme P_0 (= polynôme minimal de a) divise le polynôme Q_0.

On a ainsi démontré que P_0 et Q_0 étaient associés (ils se divisent l'un l'autre). Comme ils sont tous deux unitaires (par convention), ils sont en fait égaux.

Deuxième version

Pour tout polynôme P, on sait que

$$\varphi\big(P(a)\big) = P\big(\varphi(a)\big)$$

et par conséquent,

$$\begin{aligned} P(b) = 0_B &\iff P(a) \in \operatorname{Ker}\varphi \\ &\iff P(a) = 0_A \qquad \text{(car } \varphi \text{ est injective)} \end{aligned}$$

ce qui prouve que les idéaux annulateurs de a et de b sont égaux.

Or le polynôme minimal est l'unique générateur unitaire de l'idéal annulateur (en supposant que cet idéal ne soit pas réduit à $\{0\}$), donc a et b ont même polynôme minimal.

Solution 43 23-43

Réflexivité

Pour tout entier $a \in \mathbb{Z}$,

$$a = 0 \times n + a,$$

donc a est congru à a modulo n.

Symétrie

Si a est congru à b, alors il existe $q \in \mathbb{Z}$ tel que

$$a = qn + b$$

et par conséquent

$$b = (-q)n + a.$$

Comme $-q \in \mathbb{Z}$, on en déduit que b est congru à a.

✍ *Grâce à cette propriété de symétrie, on dit plutôt* a ***et*** b ***sont congrus modulo*** n *que* a ***est congru à*** b ***modulo*** n.

Transitivité

Si a est congru à b et si b est congru à c, alors il existe deux entiers relatifs q_1 et q_2 tels que

$$a = q_1 n + b \quad \text{et} \quad b = q_2 n + c.$$

Par conséquent,

$$a = \underbrace{(q_1 + q_2)}_{\in\mathbb{Z}} n + c$$

donc a est congru à c.

❧ La relation *"est congru modulo n à"* est donc une relation d'équivalence.

Solution 44 dm1608

1. Si ζ_k engendre $\mathbb{U}_n$, c'est-à-dire si $G_k = \mathbb{U}_n$, alors en particulier $\zeta_1 \in G_k$, donc il existe un entier $m \in \mathbb{Z}$ tel que

$$\exp\frac{2i\pi}{n} = \zeta_1 = \zeta_k^m = \exp\frac{2ikm\pi}{n}$$

c'est-à-dire

$$\exp\frac{2i(km-1)\pi}{n} = 1$$

donc $2i(km-1)\pi/n$ est un multiple entier de 2π : il existe un entier q tel que $km-1 = qn$. Comme il existe deux entiers m et q tels que

$$km - nq = 1,$$

alors k et n sont premiers entre eux (BÉZOUT).

Réciproquement, comme $\zeta_k \in \mathbb{U}_n$, le groupe engendré par ζ_k est un sous-groupe de $\mathbb{U}_n$. Et si k et n sont premiers entre eux, alors (BÉZOUT encore) il existe deux entiers m et q tels que $km + nq = 1$, donc

$$\zeta_1 = \exp\frac{2i\pi}{n} = \exp\frac{2i(km+nq)\pi}{n} = \left(\exp\frac{2ik\pi}{n}\right)^m \exp 2iq\pi = \zeta_k^m \in G_k.$$

Comme $\mathbb{U}_n$ est engendré par ζ_1, pour tout élément $u \in G_k$, il existe un entier ℓ tel que

$$u = \zeta_1^\ell = (\zeta_k^m)^\ell = \zeta_k^{m\ell} \in G_k,$$

ce qui prouve que $\mathbb{U}_n \subset G_k$. Finalement, on a bien $\mathbb{U}_n = G_k$.

2. Passons au cas général : si d est le pgcd de k et n, alors il existe deux entiers n_0 et $0 \leqslant k_0 < n_0$, *premiers entre eux*, tels que $n = dn_0$ et $k = dk_0$. Dans ces conditions,

$$\zeta_k = \exp\frac{2ik\pi}{n} = \exp\frac{2ik_0\pi}{n_0}$$

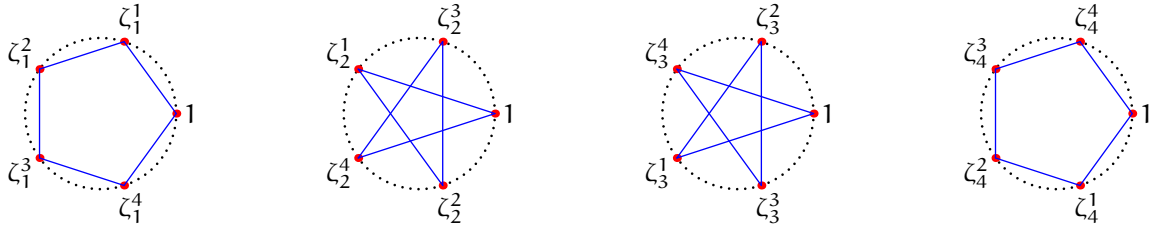
et la question précédente montre que ζ_k engendre le groupe $\mathbb{U}_{n_0}$.

✍ *On a en quelque sorte démontré que les sous-groupes de $\mathbb{U}_n$ sont les groupes de la forme $\mathbb{U}_m$, où m divise n.*

❧ On présente maintenant quelques exemples.

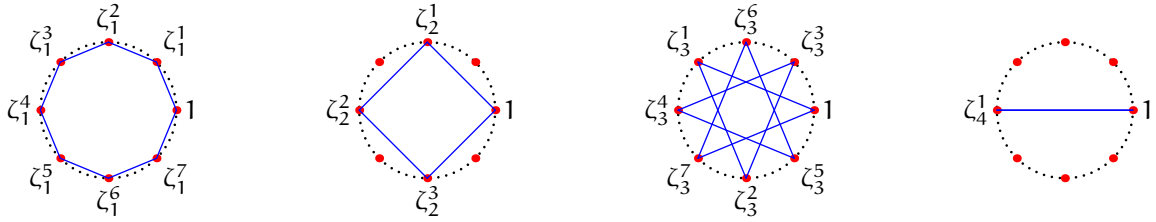
Les racines cinquièmes de l'unité

Tous les entiers $1 \leqslant k < 5$ sont premiers à 5, donc ζ_k engendre $\mathbb{U}_5$.



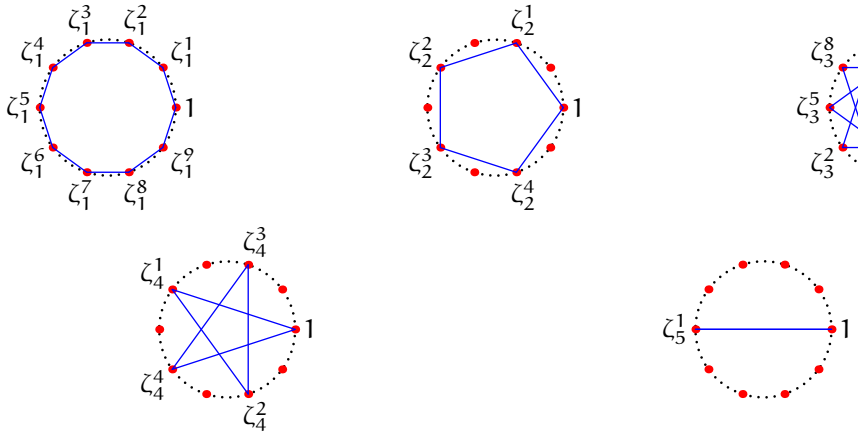
Les racines huitièmes de l'unité

Les entiers 2, 4 et 6 ne sont pas premiers à 8, donc les sous-groupes engendrés par ζ_2, ζ_4 et $\zeta_6 = \overline{\zeta_2}$ sont des sous-groupes *stricts* de $\mathbb{U}_8$.



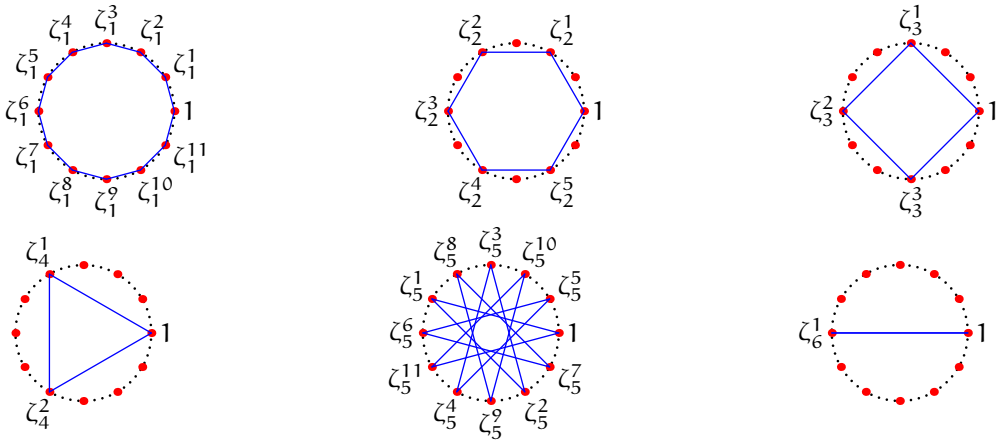
Les racines dixièmes de l'unité

Les entiers 2, 4, 5, 6 et 8 ne sont pas premiers à 10. Seuls les sous-groupes engendrés par ζ_1, ζ_3, $\zeta_7 = \overline{\zeta_3}$ et $\zeta_9 = \overline{\zeta_1}$ sont égaux à $\mathbb{U}_{10}$.



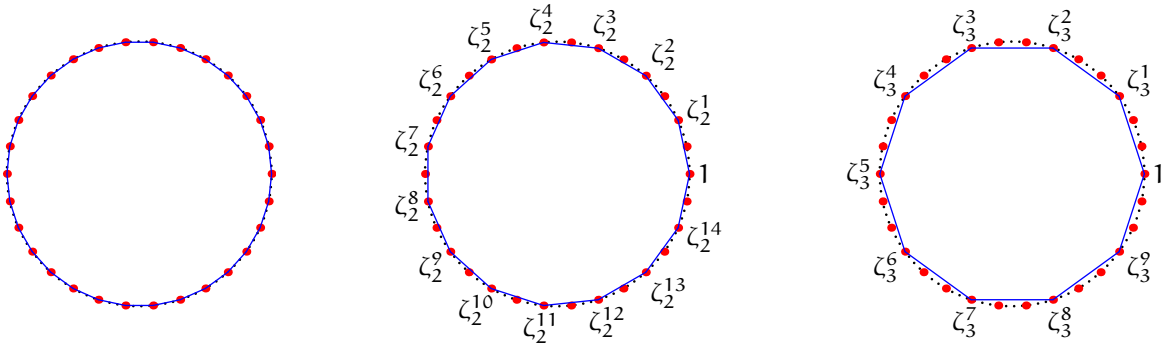
Les racines douzièmes de l'unité

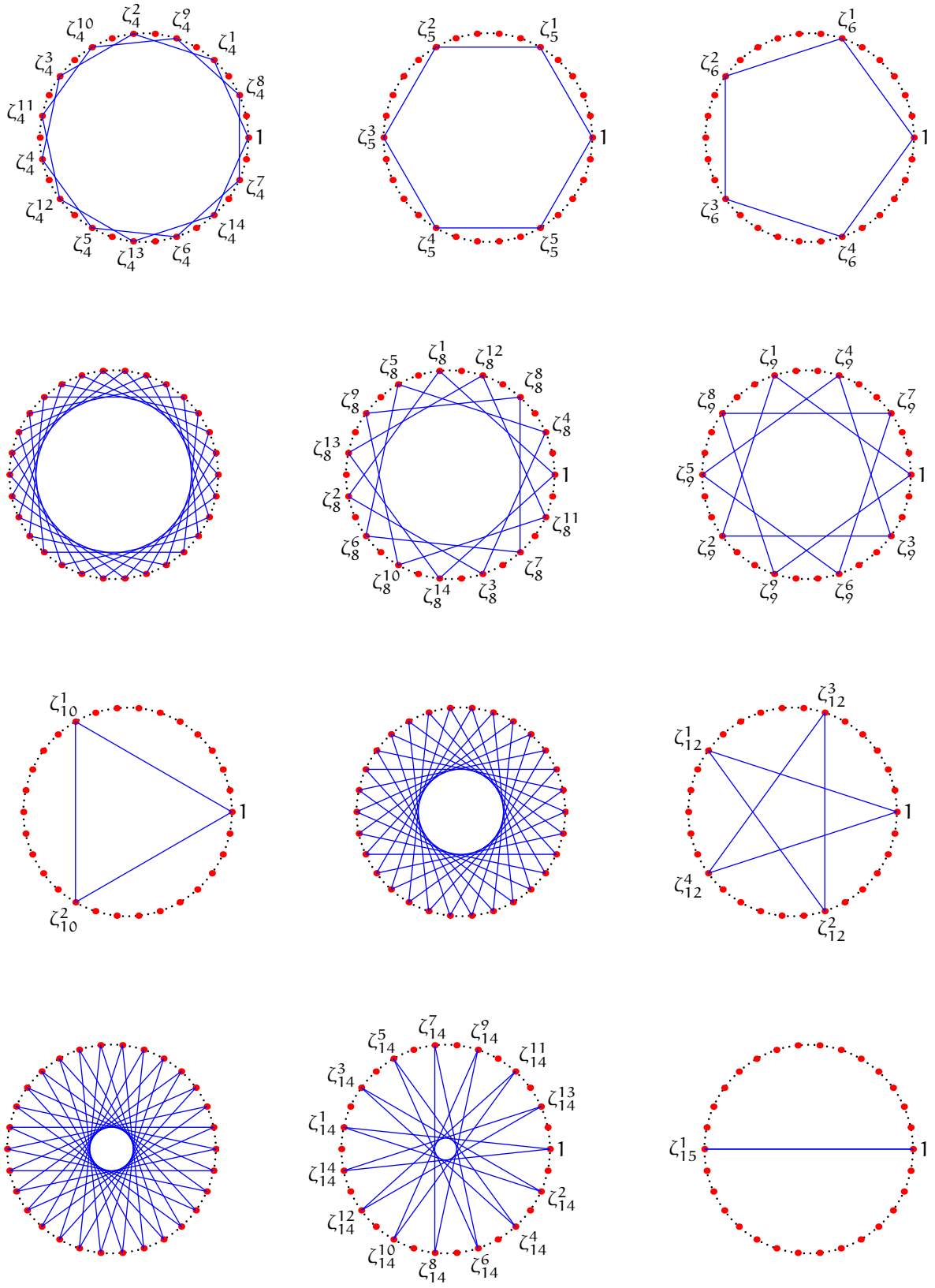
Seuls 1, 5, 7 et 11 sont premiers à 12, donc seuls les sous-groupes engendrés par ζ_1, ζ_5, $\zeta_7 = \overline{\zeta_5}$ et $\zeta_{11} = \overline{\zeta_1}$ sont égaux à $\mathbb{U}_{12}$.



Les racines trentièmes de l'unité

Comme $30 = 2 \times 3 \times 5$, seuls les entiers 1, 7, 11, 13, 17, 19, 23 et 29 sont premiers à 30. Les figures qui correspondent à ζ_1, ζ_7, ζ_{11} et ζ_{13} ne sont pas légendées, faute de place !





Solution 45 rms128-198

Considérons $f \in G$: il existe un réel $a \neq 0$ et un réel b tels que

$$\forall\, x \in \mathbb{R}, \qquad f(x) = ax + b.$$

Si $a = 1$, alors :

— ou bien $b = 0$ et tous les réels sont fixes par $f = I_{\mathbb{R}}$;
— ou bien $b \neq 0$ et f n'a pas de point fixe, ce qui contredit l'hypothèse $f \in G$.
Si $a \neq 1$, alors f admet un, et un seul, point fixe $\alpha = \frac{b}{1-a}$.

✍ *Une application affine non constante réalise une bijection de $\mathbb{R}$ dans $\mathbb{R}$, il faut donc comprendre que la loi de composition interne considérée ici est le produit de composition $\circ$.*
Si $f(x) = ax + b$ (avec $a = 0$), alors la bijection réciproque de f s'exprime : $f^{-1}(x) = {}^{x}/_{a} - {}^{b}/_{a}$.
Si on adjoint les fonctions constantes à G, l'ensemble des fonctions affines de $\mathbb{R}$ dans $\mathbb{R}$ est muni d'une structure de groupe pour l'addition des fonctions.

❧ Considérons deux éléments f et g de G, distincts de $I_{\mathbb{R}}$ (en supposant que le groupe G n'est pas réduit au neutre : $G \neq \{I_{\mathbb{R}}\}$). Il existe donc quatre réels $a \notin \{0, 1\}$, b, $c \notin \{0, 1\}$ et d tels que

$$\forall\, x \in \mathbb{R}, \qquad f(x) = ax + b \quad \text{et} \quad g(x) = cx + d.$$

Comme G est un groupe pour $\circ$, on en déduit que le **commutateur** $f^{-1} \circ g^{-1} \circ f \circ g$ appartient aussi à G. Or

$$\forall\, x \in \mathbb{R}, \qquad (f^{-1} \circ g^{-1} \circ f \circ g)(x) = x + \frac{ad - d + b - bc}{ac}.$$

D'après la discussion initiale, cette fonction affine appartient à G si, et seulement si,

$$ad - d + b - bc = 0$$

ce qui revient à supposer que

$$\frac{b}{1-a} = \frac{d}{1-c}$$

ou encore à supposer que f et g ont même point fixe.
❧ On a ainsi démontré que : si f et g sont deux éléments de G qui ont des points fixes distincts, alors $f^{-1} \circ g^{-1} \circ f \circ g$ est un élément de G qui n'a pas de point fixe — ce qui contredit l'hypothèse sur G.
Autrement dit, deux éléments quelconques de G distincts de l'élément neutre $I_{\mathbb{R}}$ ont même point fixe. Il existe donc un réel ω tel que

$$\forall\, f \in G, \qquad f(\omega) = \omega.$$

✍ *Réciproquement, considérons un réel ω quelconque et notons G_ω, l'ensemble des fonctions affines non constantes $f : \mathbb{R} \to \mathbb{R}$ telles que $f(\omega) = \omega$.*
De la sorte, une fonction f appartient à G_ω si, et seulement si, il existe un réel $a \neq 0$ tel que

$$\forall\, x \in \mathbb{R}, \qquad f(x) = \omega + a(x - \omega)$$

et on vérifie sans peine que l'application

$$[a \mapsto [x \mapsto \omega + a(x - \omega)]]$$

est un isomorphisme de $(\mathbb{R}^*, \times)$ sur $(G_\omega, \circ)$. (En particulier, G_ω est nécessairement un groupe commutatif.)
Les groupes $(G, \circ)$ étudiés ici sont donc isomorphes à un sous-groupe de $(\mathbb{R}^*, \times)$.

Solution 46 rms128-436

On sait exprimer $\varphi(n)$ au moyen de la décomposition de n en produit de facteurs premiers : s'il existe des nombres premiers

$$p_1 < p_2 < \cdots < p_r$$

et des entiers naturels non nuls

$$\alpha_1, \alpha_2, \ldots, \alpha_r$$

tels que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

alors

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \cdots (p_r - 1)p_r^{\alpha_r - 1}.$$

On a donc

$$n = p_1 \cdots p_r \prod_{k=1}^{r} p_k^{\alpha_k - 1} \quad \text{et} \quad \varphi(n) = (p_1 - 1) \cdots (p_r - 1) \prod_{k=1}^{r} p_k^{\alpha_k - 1}$$

et par conséquent $\varphi(n)$ divise n si, et seulement si, le produit

$$(p_1-1)\cdots(p_r-1) \qquad \text{divise} \qquad p_1\cdots p_r.$$

❧ En particulier, si $\varphi(n)$ divise n, il faut que (p_1-1) divise le produit $p_1\cdots p_r$.
Or $1 \leqslant p_1-1 < p_1 < p_2 < \cdots < p_r$ où les p_k sont des nombres premiers, donc (p_1-1) est premier à tous les p_k et donc premier au produit $p_1\cdots p_r$.
Il n'y a qu'une seule possibilité : $p_1-1=1$, c'est-à-dire $p_1=2$.
❧ Reprenons : $\varphi(n)$ divise n si, et seulement si, le produit

$$(p_2-1)\cdots(p_r-1) \qquad \text{divise} \qquad 2p_2\cdots p_r.$$

Or, pour $k \geqslant 2$, les p_k sont des nombres premiers strictement supérieurs à $p_1=2$, donc des nombres *impairs* et les facteurs (p_k-1) sont tous pairs.
Au second membre, la valuation de 2 est égale à 1 (puisque les p_k sont impairs pour tout $k \geqslant 2$). Il faut donc que $r \leqslant 2$!
❧ Si $r=2$, alors il faut que (p_2-1) divise $2p_2$. Comme (p_2-1) et p_2 sont premiers entre eux, il faut donc que p_2-1 divise 2 et donc que $p_2=3$.

✍ *L'astuce taupinale $1\times p_2 - 1\times(p_2-1)=1$ s'interprète ici comme la relation de Bézout !*

❧ Réciproquement, si $n=2^\alpha$, alors $\varphi(n)=(2-1).2^{\alpha-1}=2^{\alpha-1}$ divise effectivement n et si $n=2^\alpha.3^\beta$, alors $\varphi(n)=(1.2^{\alpha-1}).(2.3^{\beta-1})=2^\alpha.3^{\beta-1}$ divise effectivement n.
Les entiers n tels que $\varphi(n)$ sont donc les entiers qui se factorisent sous la forme 2^α ou $2^\alpha.3^\beta$.

Solution 47 rms128-454

Comme les coefficients de la matrice $A=(a_{i,j})_{1\leqslant i,j\leqslant n}$ sont des entiers relatifs, son déterminant

$$a=\det A=\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)a_{1,\sigma(1)}a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}$$

est également un entier relatif.
Pour les mêmes raisons, les coefficients des comatrices $\mathrm{Com}(A)$ et $\mathrm{Com}(B)$ sont des entiers relatifs.
❧ D'après la propriété de Bézout, il existe deux entiers u et v tels que

$$au+bv=1.$$

D'après les formules de Cramer,

$$A.[\mathrm{Com}(A)]^\top = a\cdot I_n \quad \text{et} \quad B.[\mathrm{Com}(B)]^\top = b\cdot I_n$$

donc

$$A.\big(u[\mathrm{Com}(A)]^\top\big)+B.\big(v[\mathrm{Com}(B)]^\top\big)=I_n.$$

Solution 48 rms130-468

1. Si x est un générateur de G, alors

$$G=\{x^k,\ k\in\mathbb{Z}\}.$$

Comme φ est un morphisme, alors

$$\varphi_*(G)=\{\varphi(x^k),\ k\in\mathbb{Z}\}=\{[\varphi(x)]^k,\ k\in\mathbb{Z}\}$$

et comme φ est surjectif, alors

$$H=\varphi_*(G)=\{[\varphi(x)]^k,\ k\in\mathbb{Z}\}.$$

Donc H est engendré par $\varphi(x)$.
❧ Réciproquement, si H est engendré par $\varphi(x)$, alors

$$H=\{[\varphi(x)]^k,\ k\in\mathbb{Z}\}\underset{\text{morph.}}{=}\{\varphi(x^k),\ k\in\mathbb{Z}\}.$$

Soit $g\in G$. Alors $h=\varphi(g)\in H$ et la description précédente de H nous assure qu'il existe un entier $k\in\mathbb{Z}$ tel que

$$\varphi(g)=\varphi(x^k).$$

Comme $\varphi : G \to H$ est injectif, alors

$$g = x^k$$

ce qui prouve que

$$G \subset \{x^k,\ k \in \mathbb{Z}\}$$

et donc que x engendre G (*l'inclusion réciproque est évidente* puisque G est un groupe multiplicatif qui contient x).

2. On considère un groupe monogène :

$$G = \langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}$$

et un sous-groupe $H \subset G$.

L'application $\varphi : \mathbb{Z} \to G$ définie par

$$\forall\, k \in \mathbb{Z}, \quad \varphi(k) = a^k$$

est un morphisme de groupes. L'image réciproque du sous-groupe H par φ :

$$I = \{k \in \mathbb{Z} : \varphi(k) \in H\} = \{k \in \mathbb{Z} : a^k \in H\}$$

est donc un sous-groupe de $(\mathbb{Z}, +)$. On sait donc qu'il existe un entier $n_0 \in \mathbb{N}$ tel que

$$I = n_0\mathbb{Z}.$$

Comme $\varphi : \mathbb{Z} \to G$ est surjectif, alors

$$\forall\, h \in H,\ \exists\, k \in I, \quad \varphi(k) = a^k = h.$$

► Si $n_0 = 0$, alors $I = \{0\}$ et $H = \{1_G\}$: dans ce cas (inintéressant au possible...), il est clair que H est monogène, engendré par 1_G.

► Si $n_0 \geqslant 1$, alors

$$H = \{a^{pn_0},\ p \in \mathbb{Z}\} = \{(a^{n_0})^p,\ p \in \mathbb{Z}\} = \langle a^{n_0} \rangle$$

et H est monogène.

✍ *J'ai pris le parti d'une démonstration abstraite (on n'a pas souvent l'occasion d'utiliser le théorème sur l'image réciproque d'un sous-groupe par un morphisme) en supposant connue la structure générale des sous-groupes de $(\mathbb{Z}, +)$.*

On aurait pu démontrer le théorème de manière plus terre à terre en imitant l'étude des sous-groupes de $(\mathbb{Z}, +)$ — et donc sans supposer connue leur structure générale. L'étude des sous-groupes de $(\mathbb{Z}, +)$ mérite d'être connue.

Solution 49 rms130-469

✍ *Une chose est de savoir comment le groupe symétrique $\mathfrak{S}_n$ est engendré (par les transpositions, par les cycles...), autre chose est de savoir expliciter une factorisation d'une permutation σ !*

Soit $\sigma \in \mathfrak{S}_n$.

❧ Si $\sigma(n) = n$, alors on pose $\sigma_1 = \sigma$. Sinon, on considère la transposition

$$\tau_n = \begin{pmatrix} n & \sigma(n) \end{pmatrix}$$

et on pose

$$\sigma_1 = \tau_n \circ \sigma.$$

Dans les deux cas, on observe que

$$\sigma_1(n) = n.$$

❧ Il ne reste plus qu'à continuer le processus, en augmentant à chaque étape le nombre de points fixés par la permutation.

❧ (HR) En supposant connue une permutation σ_k telle que

$$\forall\, n-k+1 \leqslant i \leqslant n, \quad \sigma_k(i) = i,$$

— ou bien $\sigma_k(n-k) = n-k$, c'est-à-dire que σ_k fixe $k+1$ points (tous les entiers compris entre n et $(n-k)$ inclus) et on pose directement $\sigma_{k+1} = \sigma_k$;

— ou bien $\sigma_k(n-k) \neq n-k$, donc $\sigma_k(n-k) < n-k$ (HR et injectivité de σ_k) et on pose alors $\sigma_{k+1} = \tau_{n-k} \circ \sigma_k$ où τ_{n-k} est la transposition définie par :

$$\tau_{n-k} = \begin{pmatrix} n-k & \sigma_k(n-k) \end{pmatrix}.$$

Dans les deux cas, on dispose d'une permutation σ_{k+1} qui fixe $(k+1)$ points :

$$\forall\, n-(k+1)+1 \leqslant i \leqslant n, \quad \sigma_{k+1}(i) = i.$$

❧ Le processus s'arrête avec la permutation σ_{n-1} qui fixe $(n-1)$ points : les entiers $2, \ldots, n$ et qui fixe par conséquent aussi 1 (puisque $1 \leqslant \sigma_{n-1}(1) < 2$).

En notant $\tau_{i_1}, \ldots, \tau_{i_r}$, les transpositions introduites dans ce processus (avec $0 \leqslant r < n$), on a donc

$$\sigma_{n-1} = \mathrm{Id} = (\tau_{i_r} \circ \cdots \circ \tau_{i_1}) \circ \sigma$$

c'est-à-dire

$$\sigma^{-1} = \tau_{i_r} \circ \cdots \circ \tau_{i_1}$$

et par conséquent

$$\begin{aligned}\sigma &= \tau_{i_1}^{-1} \circ \cdots \circ \tau_{i_r}^{-1} \\ &= \tau_{i_1} \circ \cdots \circ \tau_{i_r}\end{aligned}$$

puisqu'une transposition est son propre inverse (élément d'ordre deux).

✍ *L'exercice* ***[130–470]*** *montre que toutes les transpositions de $\mathfrak{S}_n$ sont conjuguées. En particulier, pour quels que soient les entiers $i \neq j$, les transpositions*

$$(i \quad j) \quad \textit{et} \quad (1 \quad j)$$

sont conjuguées. En suivant au plus près les explications du ***[130–470]****, on constate que*

$$\forall\, i \neq j, \quad (i \quad j) = (1 \quad i) \circ (1 \quad j) \circ (1 \quad i)\,,$$

ce qui prouve que le groupe symétrique est aussi engendré par les transpositions de la forme $(1 \quad i)$.

✍ *On rappelle la méthode pour factoriser en produit de cycles de supports deux à deux disjoints.*

Les supports des différents cycles sont les orbites de la permutation σ : chaque entier $1 \leqslant k \leqslant n$ appartient à une, et à une seule, orbite sous l'action de σ et la restriction de σ à chacune de ces orbites est un cycle.

On commence par identifier l'orbite de 1, ce qui définit un premier cycle. On continue en identifier l'orbite du plus petit entier qui n'appartient pas à l'orbite de 1, ce qui définit un second cycle. Etc.

Solution 50 rms130-470

✍ *On connaît un morphisme trivial de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$: l'identité! Et aussi un morphisme beaucoup moins trivial : la signature. Nous allons démontrer qu'il n'en existe pas d'autre.*

On considère un morphisme de groupes

$$\varphi \,:\, (\mathfrak{S}_n, \circ) \to (\mathbb{C}^*, \times).$$

❧ Soit τ, une transposition (ou 2-cycle). Comme $\tau^2 = \mathrm{Id}$ et que φ est un morphisme de groupes, on a donc

$$\big[\varphi(\tau)\big]^2 = \varphi(\mathrm{Id}) = 1$$

et donc $\varphi(\tau) = \pm 1$.

❧ Nous allons maintenant vérifier que la valeur de $\varphi(\tau)$ est la même pour toutes les transpositions.

Considérons quatre entiers $i \neq j$ et $k \neq \ell$ compris entre 1 et n et les transpositions

$$\tau_1 = (i \quad j) \quad \text{et} \quad \tau_2 = (k \quad \ell)\,.$$

Comme $i \neq j$ et $k \neq \ell$, il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que

$$\sigma(k) = i \quad \text{et} \quad \sigma(\ell) = j$$

et nous allons vérifier que

$$\tau_2 = \sigma^{-1} \circ \tau_1 \circ \sigma.$$

✍ *La transformation*

$$\tau \mapsto \sigma^{-1} \circ \tau \circ \sigma$$

est la conjugaison par σ et est l'analogue exact de la relation de similitude sur les matrices carrées

$$M \mapsto P^{-1}MP.$$

Il est en particulier intéressant de comparer les points fixes par τ et les points fixes par $\sigma^{-1} \circ \tau \circ \sigma$ — de même qu'il est intéressant de relier les vecteurs propres de M aux vecteurs propres de $P^{-1}MP$.

Tout d'abord,

$$\begin{array}{ccccccc} k & \overset{\sigma}{\mapsto} & i & \overset{\tau_1}{\mapsto} & j & \overset{\sigma^{-1}}{\mapsto} & \ell \\ \ell & \overset{\sigma}{\mapsto} & j & \overset{\tau_1}{\mapsto} & i & \overset{\sigma^{-1}}{\mapsto} & k \end{array}$$

et d'autre part, pour tout $x \notin \{k, \ell\}$, comme σ est injective,

$$x \mapsto \sigma(x) \notin \{i, j\}$$

puis

$$\tau_1 \circ \sigma(x) = \sigma(x)$$

car $\sigma(x) \notin \{i, j\}$ et donc finalement

$$\sigma^{-1} \circ \tau_1 \circ \sigma(x) = \sigma^{-1} \circ \sigma(x) = x.$$

Tout cela montre bien que $\tau_2 = \sigma^{-1} \circ \tau_1 \circ \sigma$.

❧ Revenons au morphisme φ : puisque c'est un morphisme,

$$\varphi(\tau_2) = \big[\varphi(\sigma)\big]^{-1} \times \varphi(\tau_1) \times \big[\varphi(\sigma)\big] = \varphi(\tau_1).$$

Ainsi, il n'y a que deux possibilités :
— ou bien $\varphi(\tau) = 1$ pour *toute* transposition τ ;
— ou bien $\varphi(\tau) = -1$ pour *toute* transposition τ.

❧ Or le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions : pour toute permutation $\sigma \in \mathfrak{S}_n$, il existe un certain nombre p de transpositions $\tau_1, \dots, \tau_p$ telles que

$$\sigma = \tau_p \circ \cdots \circ \tau_1.$$

Comme φ est un morphisme, on en déduit que

$$\varphi(\sigma) = \prod_{k=1}^{p} \varphi(\tau_k).$$

Par conséquent,
— si $\varphi(\tau) = 1$ pour toute transposition τ, alors $\varphi = \mathrm{Id}$;
— si $\varphi(\tau) = -1$ pour toute transposition τ, alors φ est la signature.

Solution 51 rms130-471

L'application $\det : \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^*$ est un morphisme de groupes (multiplicatifs) et son noyau est, par définition, le sous-groupe $\mathrm{SL}_2(\mathbb{C})$:

$$\mathrm{SL}_2(\mathbb{C}) = \big\{M \in \mathrm{GL}_2(\mathbb{C}) \ : \ \det M = 1\big\}.$$

❧ Par conséquent, l'image par det du sous-groupe fini G :

$$D = \big\{\det g, \ g \in G\big\}$$

est un sous-groupe fini de $(\mathbb{C}^*, \times)$.

Comme $G \cap \mathrm{SL}_2(\mathbb{C}) = \{I_2\}$, la restriction du morphisme det à G est injective :

$$\begin{cases} \det g = 1 \\ g \in G \end{cases} \iff g \in G \cap \mathrm{SL}_2(\mathbb{C})$$

donc $\#(D) = \#(G)$.

❧ Soit $n \in \mathbb{N}^*$, l'ordre de G (et donc celui de D). Comme l'ordre d'un élément divise l'ordre du groupe,

$$\forall\, g \in G, \quad (\det g)^n = 1$$

ce qui prouve que $\det g$ est une racine n-ième de l'unité.

On a donc

$$D \subset \mathbb{U}_n \qquad \text{et} \qquad \#(D) = \#(\mathbb{U}_n) = n$$

ce qui prouve que $D = \mathbb{U}_n$.

❧ En particulier, il existe $g_0 \in G$ tel que

$$\det g_0 = \zeta_n = e^{2i\pi/n}$$

et par conséquent

$$\mathbb{U}_n = \left\{\det(g_0^k),\ 0 \leqslant k < n\right\}.$$

On a justifié que le morphisme det : $G \to D = \mathbb{U}_n$ était injectif et comme il est surjectif par construction, on en déduit que

$$G = \{g_0^k, 0 \leqslant k < n\} = \langle g_0 \rangle.$$

✍ *On aurait pu conclure plus vite : ayant établi que* det *était un isomorphisme de groupes de* $(G, \times)$ *sur* $(\mathbb{U}_n, \times)$*, on savait que* G *était cyclique (tout groupe isomorphe à un groupe cyclique est lui-même cyclique).*

On aurait également pu invoquer le premier résultat du ***[468]*** *: comme* det *est un isomorphisme de* G *sur* $\mathbb{U}_n$*, alors* g_0 *est un générateur de* G *si, et seulement si,* $\det g_0$ *est un générateur de* $\mathbb{U}_n$.

Solution 52 rms130-1127

1. Comme l'application

$$[P \mapsto P(\alpha)]$$

est un morphisme d'anneaux de $\mathbb{Q}[X]$ dans $\mathbb{C}$, le noyau

$$I_\alpha = \left\{P \in \mathbb{Q}[X] \ :\ P(\alpha) = 0\right\}$$

de cette application est bien un idéal de $\mathbb{Q}[X]$, dit **idéal annulateur** de α.

Comme le nombre α est supposé algébrique, alors l'idéal I_α n'est pas réduit au polynôme nul et il existe alors un unique polynôme unitaire Π qui engendre cet idéal et en particulier tel que $\Pi(\alpha) = 0$: le **polynôme minimal** de α.

❧ Vérifions maintenant que le polynôme minimal est irréductible.

Si le polynôme minimal Π admet une factorisation $\Pi = P.Q$ où P et Q sont des polynômes à coefficients rationnels, alors

$$\Pi(\alpha) = P(\alpha).Q(\alpha) = 0$$

et comme $\mathbb{C}$ est un corps, alors $P(\alpha) = 0$ ou $Q(\alpha) = 0$.

Supposons (par exemple) que $P(\alpha) = 0$. Dans ce cas, $P \in I_\alpha$ et en particulier Π divise P. Mais P divise Π par définition, donc P et Π sont associés et le cofacteur Q est inversible.

Cela prouve que Π est irréductible dans $\mathbb{Q}[X]$.

✍ *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1*.*

Les polynômes irréductibles de $\mathbb{R}[X]$ *sont d'une part les polynômes de degré* 1 *et d'autre part les polynômes de degré* 2 *dont le discriminant est strictement négatif.*

En revanche, il existe dans $\mathbb{Q}[X]$ *des polynômes irréductibles de degré arbitrairement grand...*

❧ Supposons pour finir qu'il existe un polynôme irréductible et unitaire P tel que $P(\alpha) = 0$. Ce polynôme appartient à I_α, donc il est divisible par le polynôme minimal Π, qui est irréductible et unitaire. Par conséquent, $P = \Pi$.

✍ *Un polynôme irréductible* P *n'est divisible que par deux types de polynômes : les polynômes inversibles (= les polynômes constants non nuls) et les polynômes qui lui sont associés.*

Deux polynômes associés qui ont même coefficient dominant sont égaux.

Il existe donc un, et un seul, polynôme irréductible et unitaire Π tel que $\Pi(\alpha) = 0$ et c'est le polynôme minimal de α.

2. Il est clair que

$$\mathbb{Q}_{d-1}[\alpha] \subset \mathbb{Q}[\alpha].$$

Réciproquement, soit $x \in \mathbb{Q}[\alpha]$: il existe donc un polynôme $P \in \mathbb{Q}[X]$ tel que $x = P(\alpha)$. Effectuons la division euclidienne de P par Π (polynôme unitaire et donc non nul) :

$$P = Q.\Pi + R$$

avec $\deg R < \deg \Pi = d$ et donc $R \in \mathbb{Q}_{d-1}[X]$.

En substituant α à X, on en déduit que

$$x = P(\alpha) = Q(\alpha).\Pi(\alpha) + R(\alpha) = R(\alpha) \in \mathbb{Q}_{d-1}[\alpha].$$

Par double inclusion, on a démontré que

$$\mathbb{Q}_{d-1}[\alpha] = \mathbb{Q}[\alpha].$$

✍ *On en déduit que, en tant que sous-espace vectoriel de $\mathbb{C}$ (considéré comme un espace vectoriel sur le corps $\mathbb{Q}$), le sous-espace $\mathbb{Q}[\alpha]$ est engendré par la famille finie*

$$(1, \alpha, \dots, \alpha^{d-1})$$

et que sa dimension est par conséquent finie, inférieure à d.

Plus précisément, si la famille

$$(1, \alpha, \dots, \alpha^{d-1})$$

était liée dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\alpha]$, alors il existerait une famille

$$(q_0, \dots, q_{d-1}) \neq (0, \dots, 0)$$

dans $\mathbb{Q}^d$ telle que

$$\sum_{k=0}^{d-1} q_k \alpha^k = 0$$

et le polynôme

$$\sum_{k=0}^{d-1} q_k X^k \in \mathbb{Q}[X]$$

serait un polynôme annulateur non nul de α dont le degré serait inférieur à $(d-1)$ et donc strictement inférieur au degré du polynôme minimal de α : impossible !

Donc $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = d = \deg \Pi$.

❧ *De même, si f est un endomorphisme de l'espace vectoriel E qui admet un polynôme minimal de degré d, alors la dimension de la sous-algèbre $\mathbb{K}[f]$ des polynômes en f est égale à d et, plus précisément, $\mathbb{K}[f] = \mathbb{K}_{d-1}[f]$.*

3. On sait que $\mathbb{Q}[\alpha]$ est la sous-algèbre de $\mathbb{C}$ engendrée par α, donc c'est en particulier un sous-anneau de $(\mathbb{C}, +, \times)$.
Soit $x_0 \in \mathbb{Q}[\alpha]$, non nul.

✍ *En tant que nombre complexe non nul, x_0 est inversible : il existe un nombre complexe x_1 tel que $x_0.x_1 = 1$. Mais pour le moment, on ne sait pas si x_1 appartient, ou pas, à $\mathbb{Q}[\alpha]$.*

L'application

$$[x \mapsto x_0.x]$$

est clairement un endomorphisme de $\mathbb{Q}[\alpha]$. Comme $x_0 \neq 0$ et que $\mathbb{Q}[\alpha] \subset \mathbb{C}$, le noyau de cet endomorphisme est réduit à $\{0\}$. Comme $\mathbb{Q}[\alpha]$ est un espace vectoriel de dimension finie, cet endomorphisme est donc un automorphisme et il existe en particulier un élément $x_1 \in \mathbb{Q}[\alpha]$ tel que

$$x_0.x_1 = 1.$$

Donc x_0 est bien inversible en tant qu'élément de l'anneau $\mathbb{Q}[\alpha]$.

Ainsi $\mathbb{Q}[\alpha]$ est un sous-anneau de $\mathbb{C}$ dans lequel tout élément distinct de 0 admet un inverse : c'est bien un sous-corps de $\mathbb{C}$.

✍ *Si on* admet *que tous les éléments de $\mathbb{Q}[\alpha]$ sont également des nombres algébriques, alors tout élément non nul de $\mathbb{Q}[\alpha]$ admet un polynôme minimal unitaire et irréductible (comme on l'a démontré pour α).*

Le seul polynôme unitaire et irréductible divisible par X est X lui-même, c'est-à-dire le polynôme minimal de 0.

Si $x_0 \neq 0$ est algébrique, alors son polynôme minimal est irréductible et non divisible par X, donc son coefficient constant est différent de 0 :

$$\exists\, (q_0, q_1, \dots, q_r) \in \mathbb{Q}^{r+1}, \quad q_r x_0^r + \cdots + q_1 x_0 + \underbrace{q_0}_{\neq 0} = 0$$

et par conséquent

$$x_0 \underbrace{\left(\sum_{k=1}^{r} \frac{-q_k}{q_0} \cdot x_0^{k-1} \right)}_{\in \mathbb{Q}[x_0] \subset \mathbb{Q}[\alpha]} = 1$$

ce qui prouve que x_0 est inversible dans $\mathbb{Q}[\alpha]$.

Solution 53 rms130-1128

1. Si m divise n, alors il existe un entier $q \in \mathbb{N}^*$ tel que

$$n = q.m$$

et par conséquent

$$X^n - 1 = X^{qm} - 1 = (X^m - 1)(X^{(q-1)m} + \cdots + X^m + 1)$$

donc $(X^m - 1)$ divise $(X^n - 1)$.

✍ *Une expresion de la forme*

$$X^n - 1 = X^n - 1^n$$

doit impérativement faire penser à la formule de la somme géométrique :

$$a^n - b^n = (a - b) \cdot \left(\sum_{k=0}^{n-1} a^k b^{n-k} \right)$$

qui est vraie dans tout anneau pourvu que a et b commutent.

2. Réciproquement, si $(X^m - 1)$ divise $(X^n - 1)$, alors toute racine m-ième de l'unité est aussi une racine n-ième de l'unité et en particulier

$$\left(\exp \frac{2i\pi}{m} \right)^n = 1$$

c'est-à-dire

$$\exp \frac{2im\pi}{n} = 1$$

donc $2im\pi/n$ est un multiple entier de $2i\pi$. Autrement dit, n divise m !

✍ *On doit savoir que l'application*

$$\left[t \mapsto e^{it} \right]$$

est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$ et que le noyau de ce morphisme est le sous-groupe discret $2\pi\mathbb{Z}$.

Solution 54 rms133-984

1. Par définition, $G_d \subset G$.
Puisque $e^d = e$, l'ensemble G_d contient e (et n'est donc pas vide).
Soient x et y, deux éléments de G_d. Par définition, $x^d = y^d = e$ et comme le groupe $(G, \cdot)$ est commutatif,

$$(x \cdot y^{-1})^d = x^d \cdot (y^{-1})^d = e \cdot (y^d)^{-1} = e^{-1} = e,$$

ce qui prouve que $x \cdot y^{-1} \in G_d$.
L'ensemble G_d est donc bien un sous-groupe de $(G, \cdot)$.

2. Comme $(G, \cdot)$ est un groupe fini, d'après le Théorème de Lagrange, l'ordre de tout élément x de G divise l'ordre n de G.
Si $x \in G_d$, alors (par définition) $x^d = e$, donc l'ordre de x est un diviseur de d.
Comme n et d sont ici supposés premiers entre eux, on en déduit que l'ordre de $x \in G_d$ est égal à 1, c'est-à-dire $x = e$.
Ainsi, $G_d = \{e\}$ pour tout entier d premier à n.

3. Soit $x = (x_1, \ldots, x_r) \in \Gamma$. Comme les x_k appartiennent tous à G et que $(G, \cdot)$ est un groupe, le produit $x_1 \cdots x_r$ appartient aussi à G. Par conséquent, l'application f est bien définie de Γ dans G.

❧ Cette application f est bien un morphisme de groupes : quels que soient $x = (x_1, \ldots, x_r)$ et $y = (y_1, \ldots, y_r)$ dans Γ,

$$x \otimes y = (x_1 \cdot y_1, \ldots, x_r \cdot y_r)$$

(par définition de la loi sur le groupe produit) et

$$f(x \otimes y) \overset{\dagger}{=} (x_1 \cdot y_1) \cdot \cdots \cdot (x_r \cdot y_r) \overset{\ddagger}{=} (x_1 \cdot \cdots \cdot x_r) \cdot (y_1 \cdot \cdots \cdot y_r) \overset{\dagger}{=} f(x) \cdot f(y)$$

par définition de f ($\dagger$) et commutativité de la loi $\cdot$ ($\ddagger$).
Donc l'application f est bien un morphisme de groupes du groupe produit $(\Gamma, \otimes)$ dans le groupe $(G, \cdot)$.

❧ Le morphisme de groupes f est injectif si, et seulement si, son noyau est réduit à l'élément neutre du groupe de départ, c'est-à-dire :

$$\operatorname{Ker} f = \{(e, \dots, e)\}.$$

✍ *Comme* $\operatorname{Ker} f$ *est un sous-groupe de* $(\Gamma, \otimes)$*, l'inclusion*

$$\{(e, \dots, e)\} \subset \operatorname{Ker} f$$

est toujours vraie et on n'en parle jamais.

Considérons donc $x = (x_1, \dots, x_r) \in \Gamma$ tel que

$$f(x) = x_1 \cdot \dots \cdot x_r = e.$$

Par définition des sous-groupes G_{π_i}, on sait que

$$x_1^{\pi_1} = x_2^{\pi_2} = \dots = x_r^{\pi_r} = e.$$

Comme les entiers $\pi_1 = p_1^{\alpha_1}$, $\pi_2 = p_2^{\alpha_2}$, …, $\pi_r = p_r^{\alpha_r}$ sont deux à deux premiers entre eux (puisque les entiers $p_1, \dots, p_r$ sont des nombres premiers deux à deux distincts), on déduit du Lemme chinois que, pour tout entier $1 \leqslant i \leqslant r$, il existe un entier n_i tel que

$$n_i \equiv 1 \pmod{\pi_i} \qquad \text{et} \qquad \forall\, j \neq i, \quad n_i \equiv 0 \pmod{\pi_j}.$$

Autrement dit, il existe des entiers $k_{i,1}, \dots, k_{i,r}$ tels que

$$n_i = 1 + k_{i,i}\pi_i \qquad \text{et} \qquad \forall\, j \neq i, \quad n_i = k_{i,j}\pi_j.$$

On déduit alors de $x_1 \cdot \dots \cdot x_r = e$ que

$$e = (x_1 \cdot \dots \cdot x_r)^{n_i} = x_1^{n_i} \cdot \dots \cdot x_r^{n_i} = x_i^{1+k_{i,i}\pi_i} \cdot \prod_{\substack{1 \leqslant j \leqslant r \\ j \neq i}} x_j^{k_{i,j}\pi_j} = x_i$$

pour tout $1 \leqslant i \leqslant r$. On a ainsi démontré l'injectivité de f.

❧ Nous allons maintenant démontrer la surjectivité du morphisme f. Pour cela, nous considérons un élément $y \in G$ et nous cherchons un antécédent $x = (x_1, \dots, x_r) \in \Gamma$ de y par f.

Comme les entiers $\pi_1, \dots, \pi_r$ sont deux à deux premiers entre eux, on en déduit que les entiers

$$q_1 = \prod_{j \neq 1} \pi_j, \quad q_2 = \prod_{j \neq 2} \pi_j, \quad \dots, \quad q_r = \prod_{j \neq r} \pi_j$$

sont premiers dans leur ensemble. Il existe donc des entiers relatifs $a_1, \dots, a_r$ tels que

$$\sum_{i=1}^{r} a_i q_i = 1.$$

Par conséquent,

$$y = y^1 = \prod_{i=1}^{r} y^{a_i q_i} = \prod_{i=1}^{r} (y^{q_i})^{a_i}.$$

Par définition des entiers q_i, on sait que $q_i \pi_i = n$ pour tout $1 \leqslant i \leqslant r$, donc

$$\forall\, 1 \leqslant i \leqslant r, \qquad (y^{q_i})^{\pi_i} = y^{q_i \pi_i} = y^n = e$$

puisque l'ordre de l'élément y divise l'ordre n du groupe $(G, \cdot)$. Cela prouve que

$$\forall\, 1 \leqslant i \leqslant r, \qquad y^{q_i} \in G_{\pi_i}$$

et comme G_{π_i} est un sous-groupe de $(G, \cdot)$, on en déduit que

$$\forall\, 1 \leqslant i \leqslant r, \qquad (y^{q_i})^{a_i} \in G_{\pi_i}$$

(les a_i sont des entiers relatifs). On a ainsi démontré que

$$\forall\, y \in G, \qquad x = \big((y^{q_1})^{a_1}, (y^{q_2})^{a_2}, \dots, (y^{q_r})^{a_r}\big) \in \Gamma$$

et que $y = f(x)$.

❧ En conclusion, l'application f est bien un isomorphisme de groupes du groupe produit $(\Gamma, \otimes)$ sur le groupe $(G, \cdot)$.

4. a. En particulier, le morphisme f réalise une bijection entre deux ensembles finis, donc les cardinaux de ces deux ensembles sont égaux. Ainsi,

$$n = \#(G) = \prod_{i=1}^{r} \#(G_{\pi_i}).$$

On suppose ici que

$$\forall\, 1 \leqslant i \leqslant r, \qquad \#(G_{\pi_i}) \leqslant \pi_i$$

donc

$$\prod_{i=1}^{r} \#(G_{\pi_i}) \leqslant \prod_{i=1}^{r} \pi_i = n.$$

On en déduit que

$$\forall\, 1 \leqslant i \leqslant r, \qquad \#(G_{\pi_i}) = \pi_i.$$

❧ Le Théorème de Lagrange nous assure que l'ordre de tout élément du sous-groupe G_{π_i} divise l'ordre de ce sous-groupe. Comme π_i est un puissance de p_i, on en déduit que l'ordre de tout élément de G_{π_i} est une puissance de p_i.

Par conséquent, s'il n'existe aucun élément de G_{π_i} dont l'ordre soit égal à π_i, alors l'ordre de chaque élément de G_{π_i} est un diviseur strict de π_i :

$$\forall\, x \in G_{\pi_i}, \qquad x^{p_i^{\alpha_i - 1}} = e.$$

Autrement dit,

$$G_{\pi_i} \subset G_{p_i^{\alpha_i - 1}}$$

et donc, en considérant les cardinaux,

$$\pi_i = \#(G_{\pi_i}) \leqslant \#(G_{p_i^{\alpha_i - 1}}) \leqslant p_i^{\alpha_i - 1} < \pi_i,$$

ce qui est absurde.

❧ On a ainsi démontré que chaque sous-groupe G_{π_i} contient un élément g_i dont l'ordre est égal à π_i.

Puisque l'ordre du sous-groupe G_{π_i} est égal à l'ordre de $g_i \in G_{\pi_i}$, le sous-groupe G_{π_i} est en fait cyclique et engendré par g_i :

$$\forall\, 1 \leqslant i \leqslant r, \qquad G_{\pi_i} = \langle g_i \rangle.$$

✍ *Le groupe produit $H = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$ est un groupe commutatif d'ordre 12.*

Le groupe $H_8 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ n'est pas cyclique (l'ordre de chacun de ses éléments est au plus égal à 4, aucun n'est d'ordre 8), alors que le groupe $H_3 = \mathbb{Z}/3\mathbb{Z}$ est cyclique. Par conséquent, le groupe produit $H = H_8 \times H_3$ n'est pas cyclique et, par isomorphisme le groupe $(G, \cdot)$ n'est pas cyclique non plus.

❧ *Non, ce groupe $(G, \cdot)$ n'est pas défini, mais c'est sans importance : quel qu'il soit, il est isomorphe à un groupe (bien défini !) qui n'est pas cyclique, donc il n'est pas cyclique.*

❧ *Oui, on peut expliciter un groupe $(G, \cdot)$ qui vérifie ces propriétés : il suffit de fureter dans le groupe symétrique $(\mathfrak{S}_9, \circ)$.*

4. b. Comme les entiers π_i sont deux à deux premiers entre eux, l'ordre de l'élément

$$g = g_1 \cdot g_2 \cdot \cdots \cdot g_r$$

est égal au produit des entiers π_i, c'est-à-dire à n.

✍ *Voir l'exercice corrigé* `rms135-492` *pour le cas de deux éléments et conclure par récurrence sur r.*

On a donc un élément g de G dont l'ordre est égal à l'ordre du groupe $(G, \cdot)$, ce qui prouve que $G = \langle g \rangle$ et en particulier que le groupe $(G, \cdot)$ est cyclique.

Solution 55 — rms135-489

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique, donc tout sous-groupe est lui même cyclique.

❧ Pour tout entier $0 \leqslant k < n$, il s'agit donc d'identifier le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe $\mathscr{C}(k)$.

Soit d, le pgcd de k et n. D'après le Théorème de Bézout, il existe deux entiers a et b tels que

$$d = ak + bn$$

et donc tels que

$$\mathscr{C}(d) = a \cdot \mathscr{C}(k) + b \cdot \mathscr{C}(n) = a \cdot \mathscr{C}(k).$$

La classe $\mathscr{C}(d)$ appartient donc au sous-groupe engendré par la classe $\mathscr{C}(k)$.

De plus, pour tout élément x du sous-groupe engendré par $\mathscr{C}(k)$, il existe un exposant $m \in \mathbb{N}$ tel que $x = m \cdot \mathscr{C}(k)$ et comme d est un diviseur de k, il existe un entier $q \in \mathbb{N}$ tel que $k = qd$. Donc

$$x = m \cdot \mathscr{C}(k) = mq \cdot \mathscr{C}(d),$$

donc $\mathscr{C}(d)$ est même un générateur de ce sous-groupe.

On a ainsi démontré que le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\mathscr{C}(k)$ est aussi le sous-groupe engendré par $\mathscr{C}(d)$ où $d = k \wedge n$.

❧ Le pgcd $d = k \wedge n$ est un diviseur de n.

Réciproquement, tout diviseur strict d de n est le pgcd de n et de l'entier $0 \leqslant d < n$. D'autre part, $d = n$ est un diviseur de n et $n = 0 \wedge n$.

Par conséquent, les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les diviseurs de n.

✍ *Voir aussi* ***104-146***.

Solution 56 rms135-490

1. Soient g et h, deux éléments de G. Dans tout groupe, on sait que

$$(g * h)^{-1} = h^{-1} * g^{-1}.$$

Or, par hypothèse, $x^{-1} = x$ pour tout $x \in G$. En appliquant cette propriété à g, à h ainsi qu'à $(g * h)$, on obtient

$$g * h = (g * h)^{-1} = h * g.$$

Le groupe $(G, *)$ est donc commutatif.

2. a. Comme a admet un symétrique dans G, l'application $\varphi_a = [x \mapsto a * x]$ est une bijection de G dans G et cette bijection est même une involution :

$$\forall\, x \in G, \qquad \varphi_a\big(\varphi_a(x)\big) = a * (a * x) = a^2 * x = x.$$

✍ *Une* ***involution*** *est une bijection $f : G \to G$ qui est sa propre réciproque :*

$$\forall\, x \in G, \quad f^{-1}(x) = f(x) \quad \textit{c'est-à-dire} \quad \forall\, x \in G, \quad f\big(f(x)\big) = x.$$

Par exemple, toute symétrie centrale ou axiale est une involution.

L'application φ_a est donc injective.

❧ Par définition de aH, l'application φ_a induit une application surjective de H sur aH et comme φ_a est injective, l'application induite est une bijection de H sur aH.

❧ En particulier, les ensembles H et aH ont même cardinal.

2. b. Si $x \in H \cap aH$, alors il existe deux éléments h_1 et h_2 de H tels que

$$x = h_1 = a * h_2.$$

On en déduit en multipliant à droite par h_2^{-1} que

$$H \ni h_1 * h_2^{-1} = a \notin H$$

puisque H est un sous-groupe de $(G, *)$. C'est absurde, donc l'intersection $H \cap aH$ est vide.

✍ *En particulier, l'ensemble aH ne contient pas l'élément neutre e (qui appartient au sous-groupe H), donc aH n'est pas un sous-groupe de $(G, *)$.*

2. c. Il est clair que l'union $H \cup aH$ est contenue dans G.

❧ Comme H est un sous-groupe de $(G, *)$, on sait que

$$e \in H \subset H \cup aH.$$

❧ Soient x et y dans $H \cup aH$. Il faut démontrer que $x * y^{-1} \in H \cup aH$ et quatre cas se présentent. Il existe deux éléments h_1 et h_2 de H tels que :

— $x = h_1$ et $y = h_2$, donc $x * y^{-1} = h_1 * h_2^{-1} \in H$ puisque H est un sous-groupe ;

— $x = a * h_1$ et $y = h_2$, donc $x * y^{-1} = a * (h_1 * h_2^{-1}) \in aH$ puisque H est un sous-groupe ;

— $x = h_1$ et $y = ah_2$, donc $x * y^{-1} = h_1 * (h_2^{-1} * a^{-1}) = a * (h_1 * h_2)$ puisque $(G, *)$ est un groupe commutatif où tout élément est son propre symétrique et comme H est un sous-groupe, le produit $h_1 * h_2$ appartient à H et $x * y^{-1} \in aH$;
— $x = a * h_1$ et $y = a * h_2$, donc

$$x * y^{-1} = a * h_1 * h_2^{-1} * a^{-1} = a^2 * h_1 * h_2 = h_1 * h_2 \in H$$

pour les mêmes raisons.
Dans tous les cas, on a démontré que $x * y^{-1} \in H \cup aH$.

On a ainsi démontré que $H \cup aH$ était un sous-groupe de $(G, *)$.

3. On procède par récurrence.

❧ L'ensemble $H_0 = \{e\}$ est un sous-groupe de $(G, *)$ de cardinal $1 = 2^0$.
❧ HR : On suppose connu un sous-groupe H_n de $(G, *)$ de cardinal 2^n.
❧ Deux cas se présentent.
— Si $H_n = G$, alors le cardinal de G est une puissance de 2.
— Sinon, H_n est un sous-groupe strict de G et il existe donc $a_{n+1} \in G \setminus H_n$. D'après la question précédente, l'ensemble

$$H_{n+1} = H_n \cup a_{n+1} H_n$$

est un sous-groupe de $(G, *)$ et

$$\#(H_{n+1}) = \#(H_n) + \#(a_{n+1} H_n) = 2\#(H_n) = 2^{n+1}.$$

❧ Comme G est un ensemble fini, que $\#(H_n) = 2^n$ pour tout entier n tel que H_n soit défini et que la suite $(2^n)_{n\in\mathbb{N}}$ tend vers $+\infty$, il existe un rang N tel que H_N soit défini mais que H_{N+1} ne soit pas défini.

On en déduit alors que $G = H_N$ et donc que $\#(G) = 2^N$.

✍ *Exemples avec $\#(G) = 2$: $\{\pm 1\}$ en tant que sous-groupe de $(\mathbb{R}^*, \times)$ ou $\{\pm I_2\}$ en tant que sous-groupe du groupe $(SO_2(\mathbb{R}), \times)$ des rotations plances.*

Exemples avec $\#(G) = 4$:

$$\left\{ I_3, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

en tant que sous-groupe du groupe $(SO_3(\mathbb{R}), \times)$ des rotations de $\mathbb{R}^3$ ou le sous-groupe

$$V_4 = \{I, (\ 1\ \ 2\ ), (\ 3\ \ 4\ ), (\ 1\ \ 2\ )(\ 3\ \ 4\ )\}$$

en tant que sous-groupe du groupe symétrique $(\mathfrak{S}_4, \circ)$.

4. Comme l'opération $*$ est associative et commutative, on peut définir le produit des éléments de G sans qu'il soit nécessaire de préciser la position des différents facteurs (commutativité), ni la position des parenthèses qui détermine l'ordre chronologique des opérations (associativité).

❧ Puisque $H_{n+1} = H_n \cup a_n H_n$ et que H_n et $a_n H_n$ sont disjoints,

$$\prod_{x\in H_{n+1}} x = \left(\prod_{y\in H_n} y \right) * \left(\prod_{z\in a_n H_n} z \right) = \left(\prod_{y\in H_n} y \right) * \left(\prod_{y\in H_n} (a_n * y) \right).$$

Comme le groupe $(G, *)$ est abélien et que $y^2 = e$ pour tout $y \in G$,

$$\prod_{x\in H_{n+1}} x = a_n^{\#(H_n)} * \left(\prod_{y\in H_n} y^2 \right) = a_n^{\#(H_n)} = a_n^{2^n}.$$

❧ Si $G = H_0 = \{e\}$, alors le produit des éléments de G est égal à e !
Si $G = H_1$, alors $G = \{e, a_1\}$ avec $a_1 \neq e$ et le produit des éléments de G est égal à a_1.
Si $G = H_{n+1}$ avec $n \geqslant 1$, alors 2^n est un entier *pair*, donc $a_n^{2^n} = e$ et le produit des éléments de G est égal à e.

Solution 57 rms135-492

1. Comme le groupe est commutatif,

$$(xy)^{ab} = x^{ab} \cdot y^{ab} = (x^a)^b \cdot (y^b)^a = e^b \cdot e^a = e.$$

Par conséquent, l'ordre de xy divise l'entier $ab \in \mathbb{N}^*$.

❧ Réciproquement, supposons qu'un entier $m \in \mathbb{N}^*$ vérifie $(xy)^m = e$. On en déduit que $x^m \cdot y^m = e$ (puisque le groupe est commutatif) et donc que $x^m = y^{-m}$ ou, ce qui revient au même $x^{-m} = y^m$.

On a donc

$$y^{am} = (y^m)^a = (x^{-m})^a = (x^a)^{-m} = e^{-m} = e,$$

ce qui prouve que l'ordre b de y divise l'exposant am.

✍ *L'ensemble des exposants $k \in \mathbb{Z}$ tels que $y^k = e$ est un sous-groupe de $(\mathbb{Z}, +)$ et, par définition, l'ordre b de y est l'unique générateur positif de ce sous-groupe.*

Par conséquent,

— *$y^k = e$ si, et seulement si, l'ordre b divise l'exposant k;*

— *l'ordre b de y est le plus petit entier strictement positif k tel que $y^k = e$.*

Par hypothèse, a et b sont premiers entre eux, donc b divise m (Théorème de Gauss) et donc $y^m = e$.

Par symétrie, a divise m et $x^m = e$.

On a ainsi démontré que m était divisible par a et par b, donc divisible par ab (puisque a et b sont premiers entre eux).

2. D'après la question précédente,

$$H = \{(xy)^k,\ 0 \leqslant k < ab\}.$$

✍ *D'après le cours sur l'ordre d'un élément, les puissances $(xy)^k$ sont deux à deux distinctes lorsque l'exposant k parcourt $[\![0, ab[\![$.*

On a démontré plus haut que : si $(xy)^m = e$, alors $x^m = y^m = e$ et m est un multiple de a et de b. On pourrait démontrer de la même manière que : si $x^m \cdot y^n = e$, alors $x^m = y^n = e$, m est un multiple de a et n est un multiple de b.

On en déduit facilement que les produits $x^m \cdot y^n$ sont deux à deux distincts lorsque le couple (m, n) parcourt $[\![0, a[\![\times [\![0, b[\![$.

❧ Soit $0 \leqslant k < ab$. Comme $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, on peut effectuer les divisions euclidiennes de k par a et par b. Il existe donc des entiers q_a, q_b, r_a et r_b tels que

$$k = aq_a + r_a = bq_b + r_b \qquad \text{avec} \qquad 0 \leqslant r_a < a \quad \text{et} \quad 0 \leqslant r_b < b.$$

Alors, comme le groupe est commutatif et que $x^a = y^b = e$,

$$(xy)^k = x^k y^k = (x^a)^{q_a} \cdot x^{r_a} \cdot (y^b)^{r_b} \cdot y^{r_b} = x^{r_a} \cdot y^{r_b}.$$

❧ Réciproquement, soient deux entiers $0 \leqslant m < a$ et $0 \leqslant n < b$. Comme a et b sont premiers entre eux, on déduit du Lemme chinois qu'il existe un (unique) entier $0 \leqslant p < ab$ tel que

$$p \equiv m \pmod{a} \qquad \text{et} \qquad p \equiv n \pmod{b}.$$

Il existe donc deux entiers relatifs k_a et k_b tels que

$$p = ak_a + m = bk_b + n$$

et on en déduit que

$$x^m \cdot y^n = e \cdot x^m \cdot e \cdot y^n = (x^a)^{k_a} \cdot x^m \cdot (y^b)^{k_b} \cdot y^n = x^{ak_a+m} \cdot y^{bk_b+n} = (xy)^p \in H.$$

❧ On a ainsi démontré l'égalité des deux ensembles par double inclusion.

Solution 58 rms135-493

✍ *Il faut bien connaître les axiomes des groupes pour savoir ce qu'il convient de démontrer ! Il suffit de vérifier que l'élément e donné par l'énoncé vérifie en fait les propriétés suivantes.*

$$\forall\, x \in G, \quad x * e = e * x = x \qquad \textit{et} \qquad \forall\, x \in G,\ \exists\, x' \in G, \quad x' * x = x * x' = e.$$

Considérons l'élément e donné par l'énoncé et choisissons un élément $x \in G$. D'après l'énoncé, il existe un élément $x' \in G$ tel que $x * x' = e$ et $x * e = x$. Toujours d'après l'énoncé, $x' * e = x'$.

❧ Considérons alors l'élément $x' * x \in G$. Par hypothèse, il existe un élément de G, que nous noterons $(x' * x)'$, tel que $(x' * x) * (x' * x)' = e$.

❧ Par associativité de $*$, on déduit des relations précédentes que

$$x' = x' * e = x' * (x * x') = (x' * x) * x'$$

et donc (en multipliant à droite par x) que

$$x' * x = [(x' * x) * x'] * x = (x' * x) * (x' * x).$$

En multipliant à droite par l'élément $(x' * x)'$ introduit ci-dessus, on en déduit que

$$\begin{aligned} e &= (x' * x) * (x' * x)' \\ &= [(x' * x) * (x' * x)] * (x' * x)' = (x' * x) * [(x' * x) * (x' * x)'] = (x' * x) * e \\ &= (x' * x). \end{aligned}$$

Nous avons ainsi démontré que

$$\forall\, x \in G,\ \exists\, x' \in G, \qquad x' * x = x * x' = e.$$

❧ Par conséquent, pour tout $x \in G$, il existe un élément $x' \in G$ tel que

$$e * x = (x * x') * x = x * (x' * x) = x * e = x$$

et nous avons enfin démontré que $(G, *)$ était bien un groupe.