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 $x \in \mathbb{Z}$.

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

ARITHMÉTIQUE (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.

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

❧ 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 $x = 7 + 20k$.