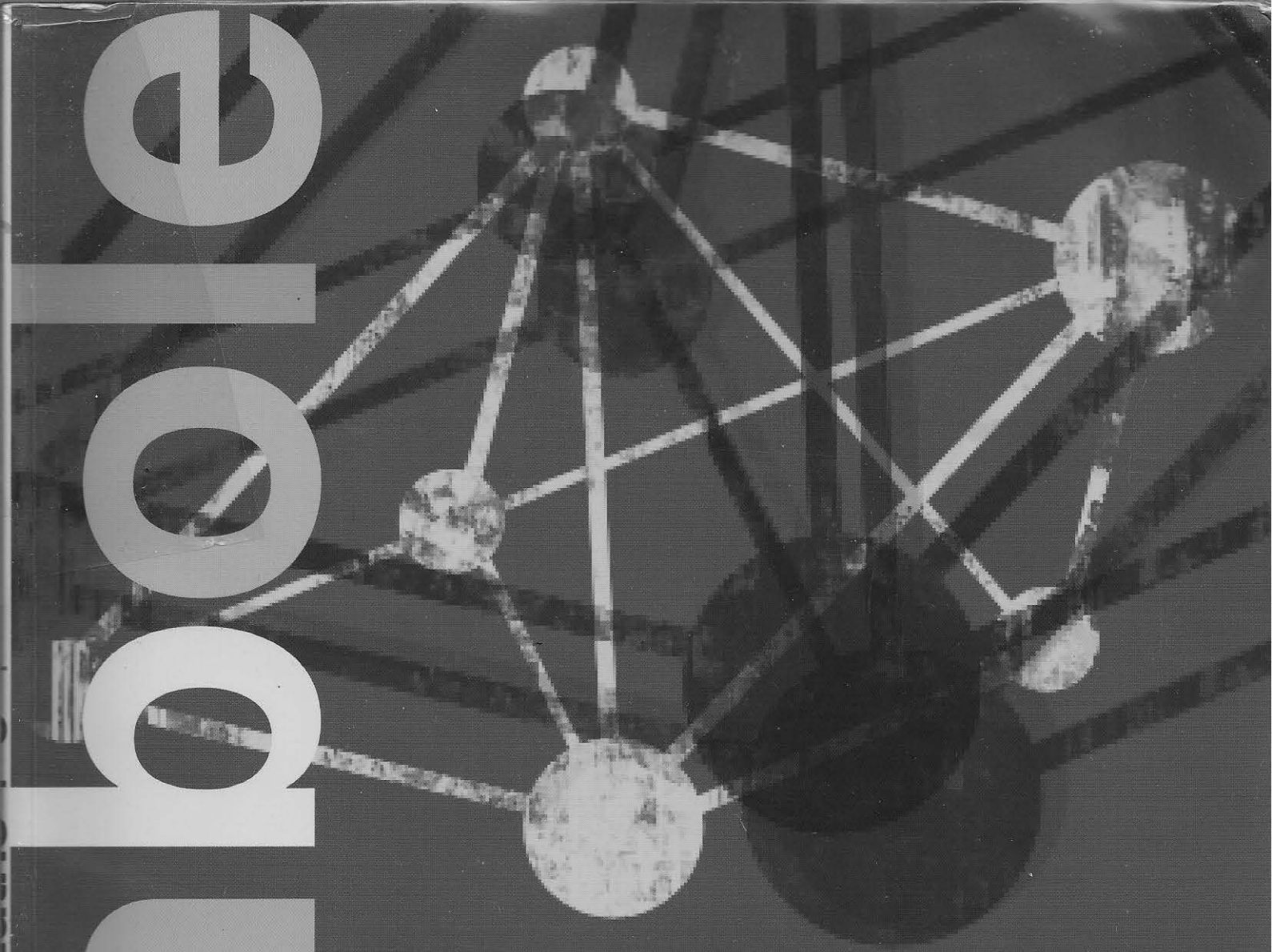


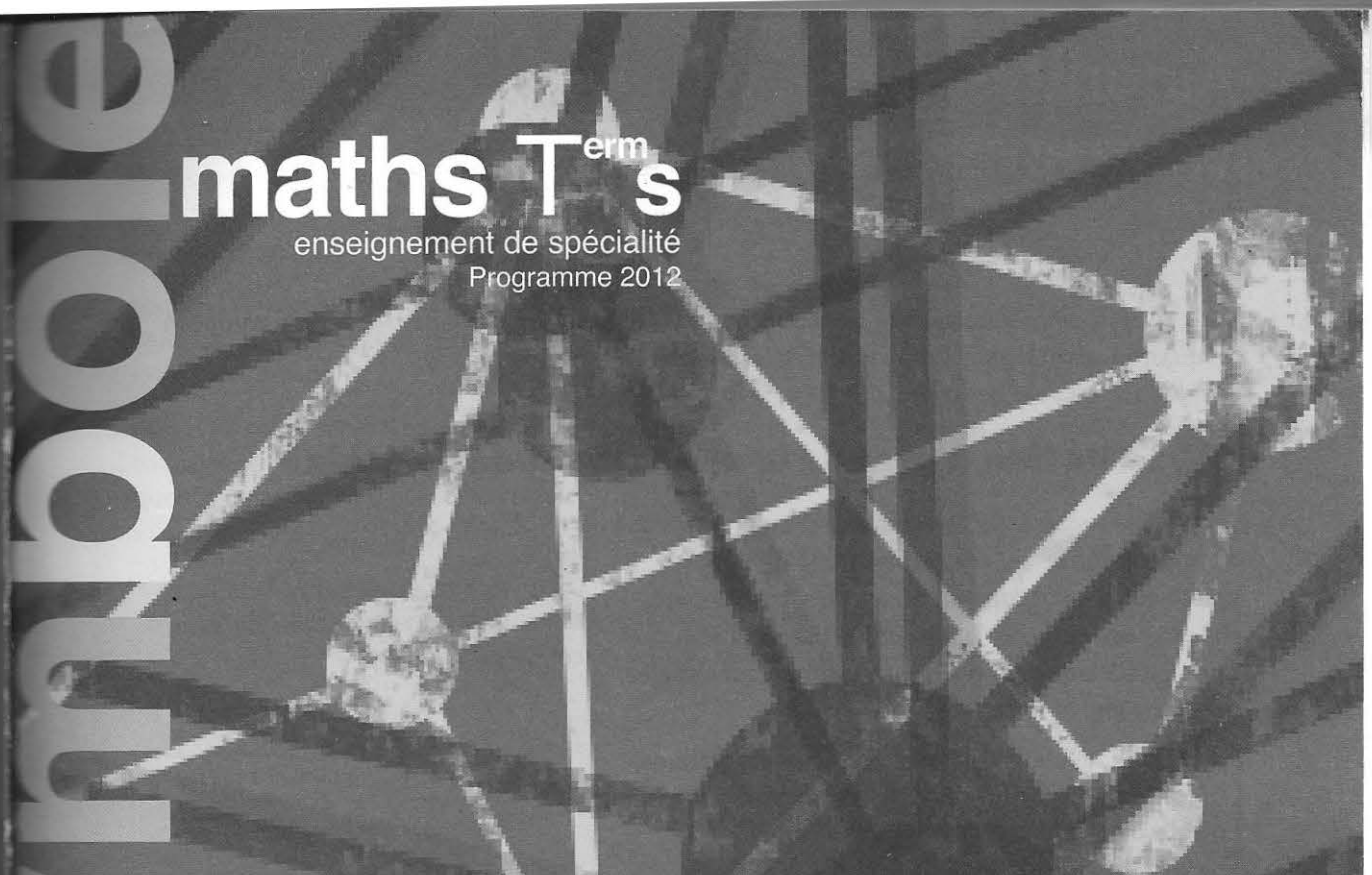
sympole

maths Term s

enseignement de spécialité

programme 2012

Belin:
ÉDITEUR INDÉPENDANT
DEPUIS 1777



Symbole

maths Term S

enseignement de spécialité
Programme 2012

Guide pratique
Algorithmique et TICE

Algorithmique : l'essentiel à connaître

1. La notion d'état de la mémoire et de variable II
2. Les quatre instructions II
3. Les principaux types de données V
4. Écrire un programme V

Les fiches TICE

Fiche 1. Calculs formels avec Xcas et Maxima VI
Fiche 2. Les tableurs Excel et Open Office Calc XI
Fiche 3. Géométrie dynamique avec GeoGebra et CaRMetal XIV

Belin
ÉDITEUR INDÉPENDANT
DEPUIS 1777

Algorithmique
L'essentiel à connaître

Dans ce livre, nous allons écrire les algorithmes en utilisant un langage très simple composé de quatre **instructions** : l'*affectation*, la *séquence*, le *test* et la *boucle*.

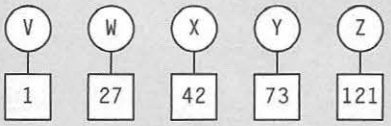
1 La notion d'état de la mémoire et de variable

On peut se représenter **la mémoire** d'un ordinateur comme étant formée d'une multitude de petites boîtes qui ont chacune un nom et qui contiennent chacune une donnée (par exemple un nombre). Une boîte à laquelle on a donné un nom est appelée une **variable**.

ATTENTION: Au cours de l'exécution d'un programme, le **contenu** des boîtes peut être **modifié**, on dira que l'on « modifie le contenu de la variable ».

EXEMPLES

Dans l'exemple ci-dessous, la boîte nommée v contient 1, celle nommée w contient 27, etc.



État de mémoire n° 1

2 Les quatre instructions

a. L'affectation

Définition 1

Une **affectation** est une instruction qui sert à modifier le contenu de l'une des variables de la mémoire.

Une **affectation** s'écrit :

`x = expression ;`

- `x` est le nom d'une variable.
- `expression` est une expression algébrique formée avec les noms des variables (x, y, z, ...) et les quatre opérations : l'addition (+), la multiplication (*), la soustraction (–) et la division (/).

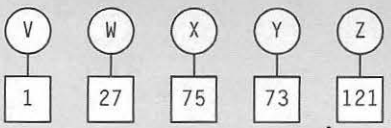
REMARQUE: La plupart des langages donnent accès à des fonctions toutes faites comme la racine carrée ou la fonction puissance.

EXEMPLES

Voici deux exemples d'affectations :

```
x = y + 2 ;
w = 3*x - 2*v/3 ;
```

Quand l'affectation `x = y + 2 ;` est exécutée dans l'état de mémoire n° 1 :
(1) La valeur de l'expression y + 2 est calculée : 73 + 2 = 75.
(2) Le contenu de la variable de nom x est modifié en y mettant la valeur 75.
Cela donne un état de la mémoire n° 2, qui est l'état de la mémoire produit par l'exécution de cette instruction.



État de mémoire n° 2

b. La séquence

Définition 2

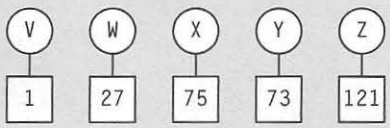
Une **séquence** est une instruction qui sert à enchaîner deux instructions.

Une **séquence** s'écrit :

```
instruction1 ;
instruction2 ;
```

EXEMPLES

La séquence : `x = y + 2 ;`
`y = x + y ;`
est exécutée dans l'état de mémoire n° 1.



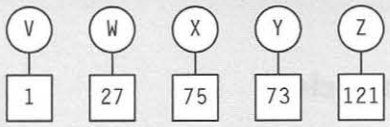
`instruction1` et `instruction2` sont deux instructions (par exemple, deux affectations).

Remarque : À l'aide de l'instruction **séquence**, on peut enchaîner un grand nombre d'instructions.

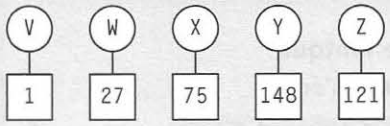
Exemple : La séquence suivante permet d'enchaîner trois instructions. C'est une séquence qui contient une séquence et une instruction.

Séquence
- Séquence
  - `a = a + b ;`
  - `b = a - b ;`
- `a = a - b ;`

(1) L'instruction `x = y + 2 ;` est exécutée, on obtient un nouvel état de mémoire, l'état n° 2 :



(2) L'instruction `y = x + y ;` est ensuite exécutée, et on obtient un nouvel état de mémoire, l'état n° 3, qui est l'état de la mémoire produit par l'exécution de la séquence :



c. Le test

Définition 3

Un **test** est une instruction qui sert à exécuter une instruction si une **condition** est vraie et éventuellement une autre instruction si la condition est fausse.

Une test s'écrit :

```
Si condition alors
   Instruction1 ;
Sinon
   Instruction2 ;
FinSi
```

`condition` est une expression qui est soit vraie, soit fausse. Elle est formée d'expressions algébriques et des symboles =, <, ⩽, >, ⩾, ≠, que l'on note en programmation respectivement ==, <, <=, >=, !=.

Vocabulaire : Ce type d'expression est appelée *expression booléenne*.

Remarque : Un test peut contenir la partie `Si ... alors` sans la partie `Sinon`.

EXEMPLES

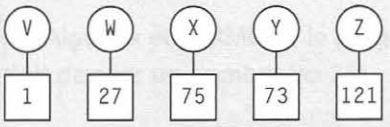
- Le test suivant :

```
Si 2 * x < z alors
   x = y + 2 ;
Sinon
   y = x + y ;
   v = y - w ;
FinSi
```

est exécuté dans l'état de mémoire n° 1.

(1) Dans cet état, 2 × x = 84, et z = 121.
La condition `2 * x < z` a la valeur vrai.

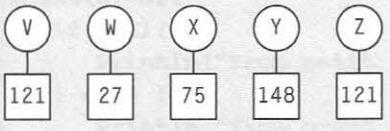
(2) L'instruction `x = y + 2 ;` est donc exécutée et on obtient l'état de mémoire n° 2 :



- Le même test est à nouveau exécuté dans l'état de mémoire n° 2.

(1) Dans cet état, 2 × x = 150, et z = 121.
La condition `2 * x < z` a la valeur faux.

(2) L'instruction `y = x + y ;` est exécutée donnant lieu à un nouvel état de mémoire, puis `v = y - w ;` est exécutée et l'état de mémoire final suivant est obtenu :



d. Les boucles

Définition 4

Une **boucle** est une instruction qui sert à **répéter** une instruction plusieurs fois.

La boucle Tantque

Cette **boucle** s'écrit :

```
TantQue condition faire
    Instruction ;
FinTantQue
```

Il existe deux types de boucles :

- la boucle `TantQue`, que l'on utilise lorsqu'on ne connaît pas a priori le nombre d'exécutions de la boucle ;
- La boucle `Pour`, version condensée de la boucle `TantQue`, que l'on utilise lorsqu'on connaît à l'avance le nombre d'exécutions de la boucle.

EXEMPLES

On exécute la boucle suivante :

```
x = 1 ;
TantQue x < 100 faire
    x = x * 2;
FinTantque
```

(1) Dans l'état de mémoire initial, la condition `x < 100` a la valeur vrai, puisque le contenu de la variable `x` est égal à 1.

(2) L'instruction `x = x * 2 ;` est alors exécutée, ce qui a pour effet de produire un nouvel état de mémoire dans lequel le contenu de la variable `x` est 2.

(3) Les étapes **(1)** et **(2)** se répètent tant que la condition est vraie, et le contenu de la variable `x` prend successivement les valeurs 4 ; 8 ; 16 ; 32 ; 64 ; 128.

(4) À ce moment-là, la condition `x < 100` a la valeur faux et l'exécution de la boucle se termine.

On obtient au final un état de mémoire dans lequel le contenu de la variable `x` est égal à 128.

Remarques : • Cette instruction calcule la plus petite puissance de 2 supérieure à 100.

• Si la variable `x` avait contenu dès le départ la valeur 120, alors la boucle n'aurait pas été exécutée.

Considérons la boucle `TantQue` suivante :

```
x = 1 ;
i = i ;
TantQue i <= 7 faire
| x = x * 2 ;
| i = i + 1 ;
FinTantque
```

On peut l'exprimer de manière plus condensée à l'aide de la boucle `Pour` :

```
x = 1 ;
Pour i allant de 1 à 7 faire
    x = x * 2 ;
FinPour
```

L'instruction `x = x * 2 ;` est exécutée 7 fois, si bien que la variable `x` contient successivement les nombres 1, 2, 4, 8, ..., 128.

Remarque : Le nombre d'exécutions est contrôlé par la variable `i` qui joue un rôle de compteur (allant de 1 à 7).

3 Les principaux types de données

• Nombre (entiers, décimaux, réels).

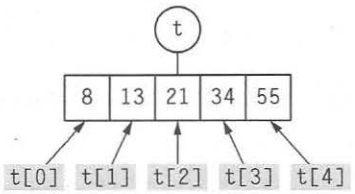
EXEMPLES : 23 ; –256 ; 1,2012.

• Caractère et chaîne de caractères.

EXEMPLES : « c » ; « o » ; « Bonjour » ; « <&@&#* ».

• Tableau (contenant des nombres, des caractères ou des chaînes) :
un tableau est une boîte contenant plusieurs cases numérotées.

EXEMPLE :



ATTENTION : Selon le langage utilisé, la numérotation ne commence pas à 0 mais à 1. Ainsi pour initialiser à 0 un tableau de *n* valeurs, on écrira quand la numérotation commence à 0 :

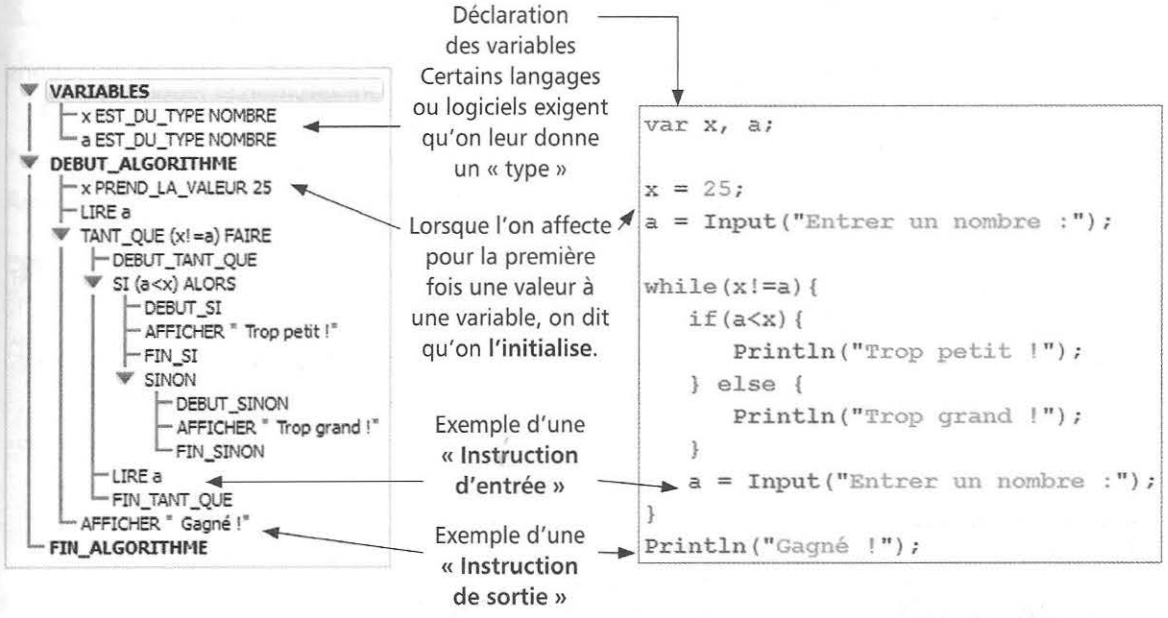
```
Pour i allant de 0 à n-1 faire
   t[i] = 0 ;
FinPour
```

et quand la numérotation commence à 1

```
Pour i allant de 1 à n faire
   t[i] = 0 ;
FinPour
```

4 Écrire un programme

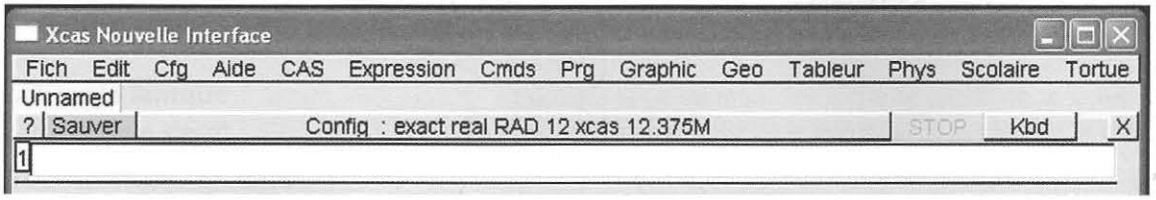
On a écrit ici dans le langage de deux logiciels différents (Algobox et CaRMetal) le programme du jeu « plus grand/plus petit » dans lequel un joueur doit deviner un nombre (ici 25).



Calculs formels avec Xcas et Maxima

L'interface

Xcas



La saisie s'effectue dans la ligne numérotée (1 puis 2 ...) et on exécute avec la touche « Entrée ». Le bouton « Kdb » permet de faire apparaître un clavier virtuel facilitant les saisies.

Maxima



La saisie s'effectue directement dans la fenêtre sous les menus et on exécute avec la combinaison de touche « Schift + Entrée ».

Remarque: Nous présentons ici l'interface wxMaxima, mais il en existe d'autres.

Pour utiliser les commandes présentées par la suite, on pourra soit directement les saisir, soit y accéder par l'un ou l'autre des menus déroulants de l'interface du logiciel utilisé.

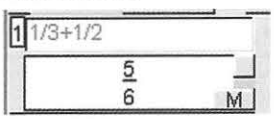
Faire des calculs

Il existe deux modes « Exact » et « Approché ». On utilise les symboles +, –, *, /, ^ pour les opérations élémentaires, d'autres instructions permettent de calculer les valeurs de fonctions particulières.

Remarques: • Le choix du mode peut être modifié :
Avec Xcas dans le menu **Cfg/Configuration CAS** en cochant ou décochant la case « approx » ;
Avec Maxima, dans le menu **Numérique/Basculer l'affichage numérique**.
• On peut aussi passer d'une valeur exacte à une valeur approchée en utilisant la commande **evalf** sous Xcas et **float** sous Maxima.

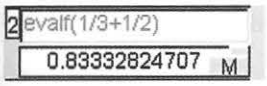
Exemples: **sqrt** pour la racine carrée ; **cos**, **sin**, **tan** pour les fonctions trigonométriques, **floor** pour la partie entière, **rand(0,1)** (sous Xcas), **random(1.0)** (sous Maxima) pour produire un nombre aléatoire de l'intervalle [0 ; 1 [.

Avec Xcas

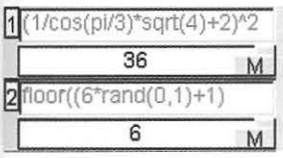


Avec Maxima

```
(%i1) 1/2+1/3;
(%o1) 5/6
```




```
(%i2) float(1/2+1/3);
(%o2) 0.83333333333333
```



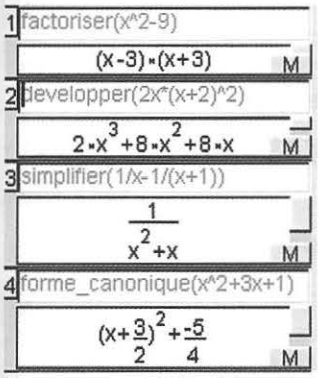

```
(%i1) (1/cos(%pi/3)*sqrt(4)+2)^2;
(%o1) 36
```

```
(%i2) floor(6*random(1.0)+1);
(%o2) 6
```

Commandes de calculs formels

• Transformer une expression.

Avec Xcas



Avec Maxima

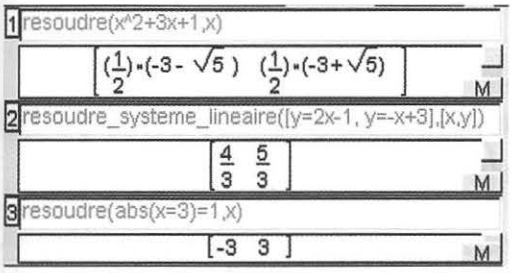
```
(%i1) factor(x^2-9);
(%o1) (x-3)(x+3)
```

```
(%i2) expand(2*x*(x+2)^2);
(%o2) 2 x^3+8 x^2+8 x
```

```
(%i3) ratsimp(1/x-1/(x+1));
(%o3) 1/(x^2+x)
```

• Résoudre une équation, une inéquation ou un système.

Avec Xcas



Avec Maxima

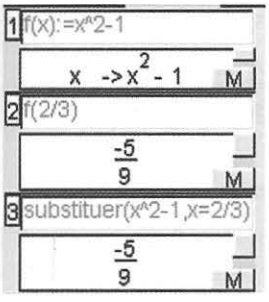
```
(%i1) solve(x^2+3*x+1);
(%o1) [x=-(sqrt(5)+3)/2, x=(sqrt(5)-3)/2]
```

```
(%i2) solve([y=2*x-1,y=-x+3], [x,y]);
(%o2) [[x=4/3, y=5/3]]
```

Remarques : • Le membre de droite de l'équation est supposé nul s'il n'est pas précisé ;
• Il faut indiquer le nom des inconnues *x*, *y*,...

• Calculer des images d'une fonction.

Avec Xcas



Avec Maxima

```
(%i1) f(x):=x^2-1;
(%o1) f(x):=x^2-1
```

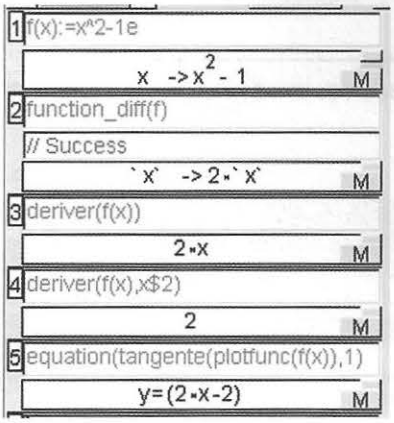
```
(%i2) f(2/3);
(%o2) -5/9
```

```
(%i3) subst(2/3, x, x^2-1);
(%o3) -5/9
```

Remarque : Soit on définit la fonction, soit on peut utiliser directement la commande **substituer**.

• **Déterminer une dérivée.**

Avec Xcas



Avec Maxima

```
(%i1) f(x):=x^2-1;
(%o1) f(x):=x^2-1

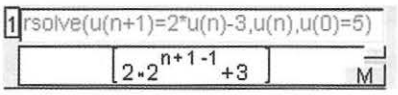
(%i2) diff(x^2-1,x,1);
(%o2) 2 x

(%i3) diff(f(x),x,2);
(%o3) 2
```

Remarque : On peut calculer des dérivées à différents ordres. Dans les exemples précédents, on a calculé la dérivée et la dérivée seconde (ligne 4 sous Xcas et 3 sous Maxima).
Xcas permet aussi d'obtenir des équations de tangentes (voir ligne 5).

• **Déterminer, si elle existe, la formule explicite d'une suite définie par récurrence.**

Avec Xcas

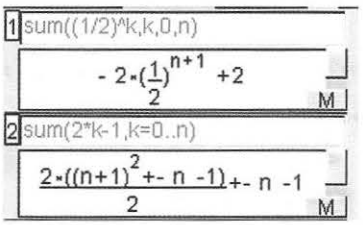



```
(%i1) load(solve_rec);
(%o1) C:/PROGRA~2/Maxima/share/maxima/5.26.0/s

(%i2) solve_rec(u(n+1)=2*u(n)-3,u(n),u(0)=5);
(%o2) u(n)=2^(n+1)+3
```

• **Calculer une somme.**

Avec Xcas



Avec Maxima

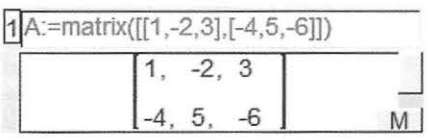
```
(%i1) sum((1/2)^k, k, 1, n), simpsum;
(%o1) -2(2^(-n-1)-1/2)

(%i2) sum(2*k-1, k, 0, n), simpsum;
(%o2) n^2-1
```

Manipuler une matrice

• **Entrer une matrice.**

Avec Xcas



Avec Maxima

Menu Algèbre / Entrer une matrice et saisir les coefficients.

```
(%i1) A: matrix(
        [1,-2,3],
        [-4,5,-6]
      );
(%o1) [ 1  -2  3 ]
      [          ]
      [-4  5  -6 ]
```

• **Renvoie la *n*-ième ligne d'une matrice.**

Avec Xcas

```
2 A[1]
        [-4, 5, -6 ]   M
```

Avec Maxima

```
(%i2) A[1];
(%o2) [1,-2,3]
```

Remarque : Dans Xcas, la numérotation commence à 0.

• **Renvoie le coefficient a_{ij} d'une matrice.**

Avec Xcas

```
3 A[1,2]
        -6   M
4 A[1][2]
        -6   M
```

Avec Maxima

```
(%i3) A[1,2];
(%o3) -2
```

```
(%i4) A[1][2];
(%o4) -2
```

• **Générer une matrice à partir d'une formule.**

Avec Xcas

```
1 A:=matrix(2,5,(i,j)->2*(i+1)^2-3*(j+1))
        [-1, -4, -7, -10, -13]
        [5,  2,  -1, -4,  -7 ]   M
```

Avec Maxima

```
(%i1) f[i,j]:=2*i^2-3*j;
(%o1) f_{i,j}:=2 i^2-3 j
```

```
(%i2) A:genmatrix(f,2,5);
(%o2) [-1  -4  -7  -10  -13]
      [ 5   2  -1   -4   -7]
```

Opérations avec les matrices

• **Additionner deux matrices.**

Avec Xcas

```
2 B:=matrix([7,-8,9],[-10,11,-12])
        [7,   -8,  9  ]
        [-10, 11,  -12]   M
3 C:=matrix([1,0],[0,-1])
        [1,  0 ]
        [0,  -1]   M
4 A+B
        [8,   -10, 12 ]
        [-14, 16,  -18]   M
5 A+C
        [2,  -2, 3 ]
        [-4, 4,  -6]   M
```

Avec Maxima

```
(%i2) B: matrix(
        [7,-8,9],
        [-10,11,-12]
      )$
```

```
(%i3) C: matrix(
        [1,0],
        [0,-1]
      )$
```

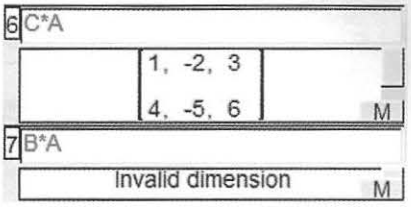
```
(%i4) A+B;
(%o4) [ 8   -10  12 ]
      [-14  16   -18]
```

```
(%i5) A+C;
fullmap: arguments must have same formal structure.
 -- an error. To debug this try: debugmode(true);
```

Remarques : • Pas d'erreur lorsque les matrices n'ont pas la même taille.
• Une erreur apparait lorsque les matrices n'ont pas la même taille.

• **Multiplier deux matrices.**

Avec Xcas



Avec Maxima

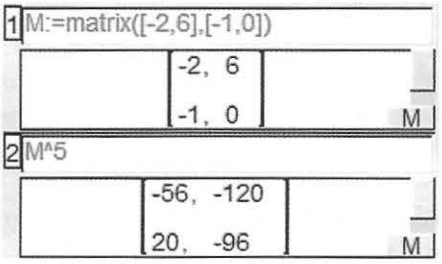
```
(%i6) C.A;
(%o6) [ 1  -2  3 ]
      [ 4  -5  6 ]

(%i7) B.A;
MULTIPLYMATRICES: attempt to multiply nonconformable matrices.
 -- an error. To debug this try: debugmode(true);
```

Remarque : Une erreur apparait lorsque les matrices n'ont pas la même taille.

• **Puissance d'une matrice carrée.**

Avec Xcas



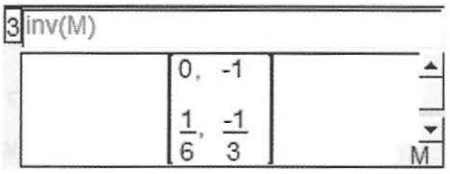
Avec Maxima

```
(%i1) M: matrix(
        [-2,6],
        [-1,0]
      )$

(%i2) M^^5;
(%o2) [ -56  -120 ]
      [  20   -96 ]
```

• **Inverse d'une matrice carrée.**

Avec Xcas



Avec Maxima

```
(%i3) invert(M);
(%o3) [  0   -1 ]
      [ 1/6  -1/3 ]
```

Autres fonctionnalités

Ces deux logiciels permettent aussi de tracer des courbes, d'utiliser un tableur (pour Xcas), de faire de la programmation, de la géométrie dynamique…

Xcas est un logiciel libre, téléchargeable gratuitement à l'adresse suivante :
http://www-fourier.ujf-grenoble.fr/~parisse/install_fr.html.

Maxima et son interface **wxMaxima** sont des logiciels libres, téléchargeable gratuitement à l'adresse suivante :
http://wxmaxima.sourceforge.net/wiki/index.php/Main_Page

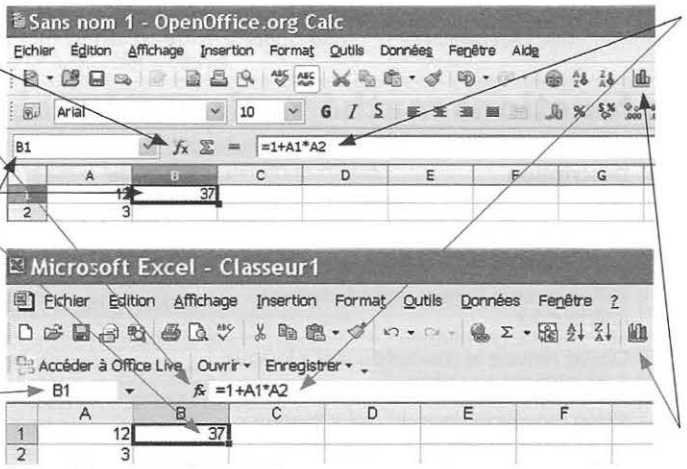
Fiche 2

Les tableurs Excel et Open Office Calc

Qu'est ce qu'un tableur ?

Un tableur est un programme informatique permettant de manipuler des données contenues dans les « cellules » d'un tableau. Il permet de réaliser des calculs sur un grand nombre de données et de les représenter graphiquement.

Présentation de l'interface



Utiliser le tableur

• **Repérer une cellule**

Les cellules sont référencées par leur numéro de colonne, suivi de leur numéro de ligne.

Remarque: On peut directement faire référence à un groupe rectangulaire de cellules.

Exemples: C5 désigne la cellule située sur la colonne C à la 5e ligne ; B1 : E4 désigne toutes les cellules situées entre les colonnes B et E d'une part, et entre les lignes 1 et 4 d'autre part.

• **Sélectionner une ou plusieurs cellules**

– Pour sélectionner une cellule, cliquer sur cette dernière.
– Pour sélectionner un groupe de cellules contiguës, cliquer sur la première cellule, puis bouger la souris jusqu'à la dernière cellule en maintenant le bouton gauche de la souris enfoncé.

• **Saisir des données dans une cellule**

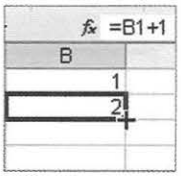
Une fois une cellule sélectionnée avec le pointeur de la souris, on peut :
– saisir un nombre ou un texte ;
– saisir une formule, en commençant par le signe « = ».

Remarque: On utilise les symboles +, –, *, /, ^ pour les opérations élémentaires ; une formule peut contenir des références à d'autres cellules.

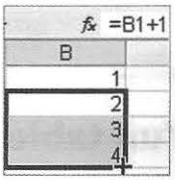
Exemples: « =11+3^2 » ou « =A1+A2*B5 ».

• **Recopier une formule**

1. Sélectionner la cellule contenant la formule à recopier (ici B2).



2. Placer le pointeur de la souris dans le coin inférieur-droit jusqu'à ce qu'il devienne une croix +.



3. Tout en appuyant sur le bouton gauche de la souris, déplacer le pointeur pour sélectionner les cellules où sera recopiée la formule (ici B3 puis B4).

Remarque : Si on recopie une formule *n* lignes en dessous et *p* colonnes à droite, alors toute référence contenue dans cette formule est elle aussi décalée de *n* lignes et *p* colonnes.

Exemple : La formule de la cellule B2, « =B1+1 », est recopiée deux lignes en dessous en B4 et devient « =B3+1 ».

Utiliser des fonctions mathématiques du tableur

Fonction	Description	Exemple	Résultat
Racine carrée		=RACINE(10)	3,162277660
Valeur absolue		=ABS(-7,2)	7,2
Partie entière	ENT(*x*) renvoie l'entier immédiatement inférieur à *x*	=ENT(18,96)	18
Cos	COS(*x*) renvoie le cosinus du réel *x* lorsque *x* est exprimé en radian	=COS(0)	1
Sin	SIN(*x*) renvoie le sinus du réel *x* lorsque *x* est exprimé en radian	=SIN(PI()/2)	1
Nombre aléatoire	ALEA() renvoie un nombre au hasard appartenant à l'intervalle [0 ; 1]	=ALEA()	0,376410967
Nombre aléatoire entre deux bornes	ALEA.ENTRE.BORNES(*a* ; *b*) renvoie un nombre entier au hasard entre les entiers *a* et *b*.	=ALEA.ENTRE.BORNES(0;100)	47

Utiliser des fonctions logiques du tableur

	A
1	2
2	3
3	8
4	10

Remarque : Les résultats des exemples sont obtenus en utilisant les cellules ci-contre.

Fonction	Description	Exemple	Résultat
Test	SI(Condition ; X ; Y) vérifie si la condition est vérifiée ; si elle l'est, renvoie la valeur X, sinon, renvoie la valeur Y.	=SI(A4>6;0 ;1)	1
Test Si	NB.SI(Cellules sélectionnées ; Critère) renvoie le nombre de cellules, parmi celles sélectionnées, répondant au critère proposé.	=NB.SI(A1:A4 ;">2")	3
NB	NB(Cellules sélectionnées) renvoie le nombre de cellules contenant un nombre parmi celles sélectionnées.	=NB(A1:A4)	4
ET	ET(Test1 ; Test2) renvoie VRAI si Test1 et Test2 sont vrais, et faux dans le cas contraire.	=ET(A2>1;A3<7)	FAUX
OU	OU(Test1 ; Test2) renvoie VRAI si Test1 ou Test2 est vrai, et faux dans le cas contraire.	=OU(A3>9;A4<20)	VRAI

Utiliser des fonctions statistiques du tableur

Remarque : Les résultats des exemples sont obtenus en utilisant les cellules ci-contre.

	A	B
1	2	2
2	3	3
3	8	1
4	10	5

Fonction	Description	Exemple	Résultat
Maximum	MAX(Cellules sélectionnées) calcule la plus grande valeur parmi les nombres présents dans les cellules sélectionnées.	=MAX(A1:A4)	10
Minimum	MIN(Cellules sélectionnées) calcule la plus petite valeur parmi les nombres présents dans les cellules sélectionnées.	=MIN(A1:A4)	2
Somme	SOMME(Cellules sélectionnées) calcule la somme des nombres présents dans les cellules sélectionnées.	=SOMME(A1:A4)	23
SommeProd	SOMMEPROD(Cellules sélectionnées zone 1; Cellules sélectionnées zone 2) calcule la somme des cellules de la zone 1 pondérées par les nombres de la zone 2.	=SOMMEPROD(A1:A4;B1:B4)	71
Moyenne	MOYENNE(Cellules sélectionnées) calcule la moyenne des nombres présents dans les cellules sélectionnées.	=MOYENNE(A1:A4)	5,75
Variance	VAR.P(Cellule sélectionnnées) renvoie la variance de la série des nombre sélectionnés.	=VAR.P(A1:A4)	11,1875
Écart type	=ECARTYPEP(A1:A4) renvoie l'écart type de la série des nombre sélectionnés.	ECARTYPEP(nombre1;nombre2;...)	3,345
Médiane	MEDIANE(Cellules sélectionnées) renvoie la valeur médiane, ou le nombre qui se trouve au milieu de la liste proposée.	=MEDIANE(A1:A4)	5,5
Premier quartile	QUARTILE(Cellules sélectionnées ; 1) renvoie le premier quartile de la série des nombres sélectionnés.	=QUARTILE(A1:A4;1)	2,75
Troisième quartile	QUARTILE(Cellules sélectionnées ; 3) renvoie le troisième quartile de la série des nombres sélectionnés.	=QUARTILE(A1:A4;3)	8,5
Loi binomiale	LOI.BINOMIALE(*k* ; *n* ; *p* ; Faux()) renvoie la probabilité P(X=*k*) d'obtenir *k* succès lors de *n* épreuves de Bernoulli de paramètre *p*. LOI.BINOMIALE(*k* ; *n* ; *p* ; Vrai()) renvoie la probabilité P(X≤*k*).	=LOI.BINOMIALE(3;5;0,5;Faux())	0,3125
	Remarque : Avec Calc, on écrit 0 plutôt que Faux() et 1 plutôt que Vrai().	=LOI.BINOMIALE(3;5;0,5;Vrai())	0,825

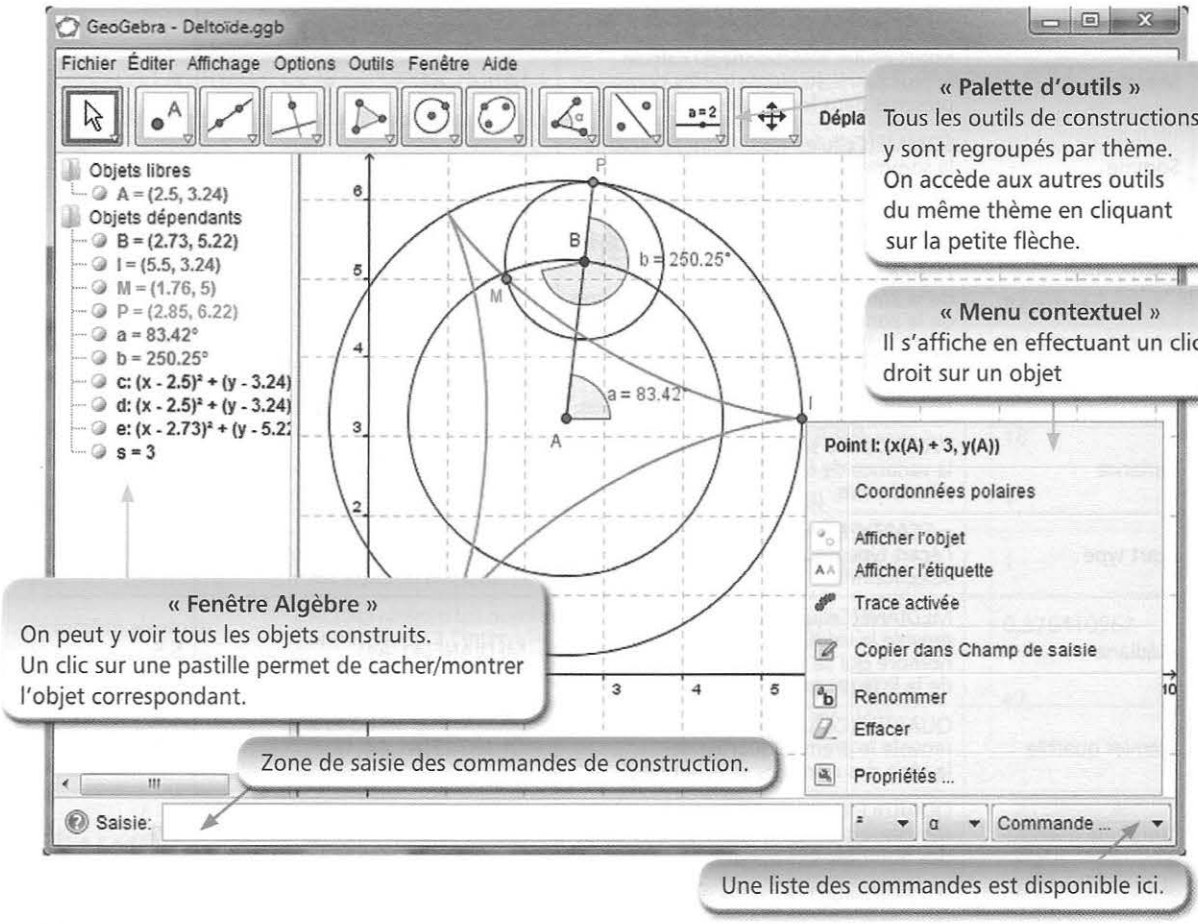
Remarque : Il est possible de calculer une moyenne pondérée en utilisant simultanément la fonction SommeProd et la fonction Somme.

Exemple : SOMMEPROD(A1:A4 ;B1:B4)/SOMME(B1:B4) permet de calculer la moyenne des cellules A1 à A4 respectivement pondérées par les coefficients B1 à B4.

Géométrie dynamique avec GeoGebra et CaRMetal

GeoGebra

L'interface



Quelques outils

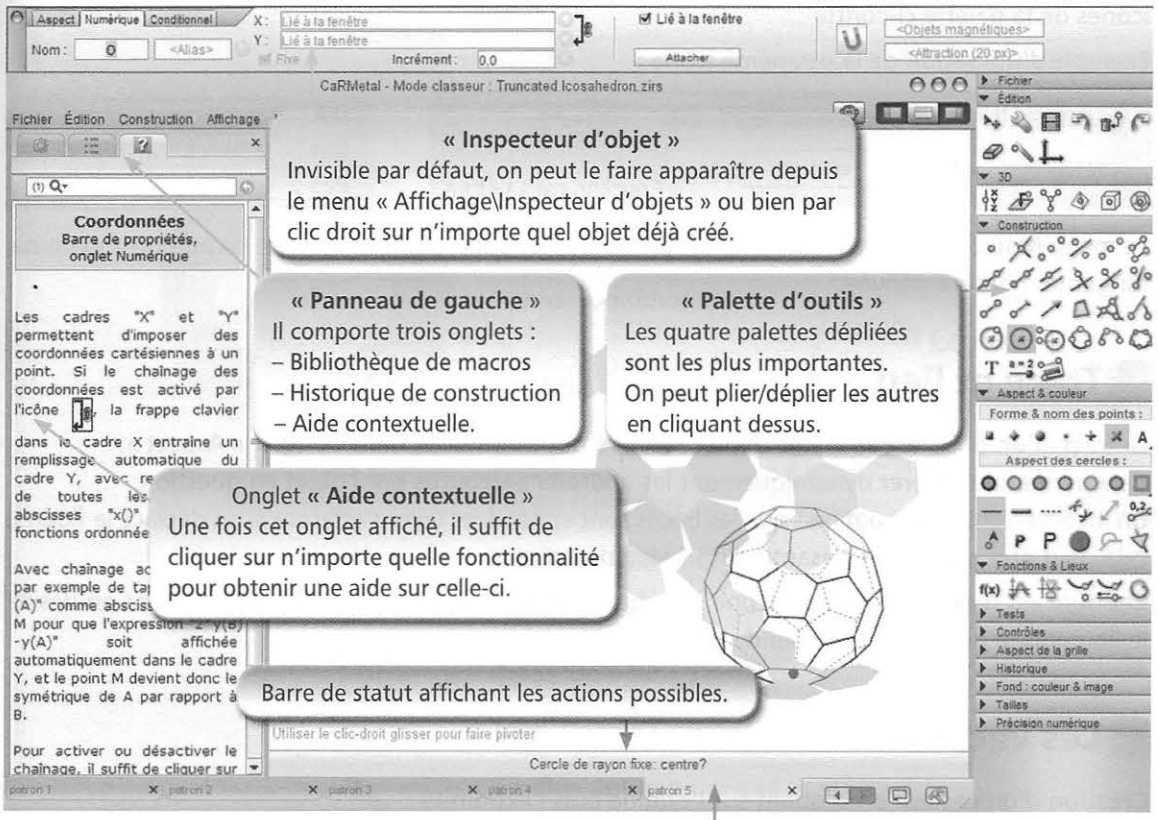
Icône	Description de la fonctionnalité
	Outil permettant de déplacer un objet déjà construit ou de sélectionner plusieurs objets d'une zone.
	Outil permettant de déplacer la totalité de la figure.
	Outils permettant d'annuler ou de refaire une action.

À savoir

- On peut aussi déplacer un objet en maintenant un clic droit sur celui-ci, quel que soit l'outil sélectionné.
- Pour déplacer la totalité de la figure dans la zone de construction, on peut aussi utiliser l'outil permettant de déplacer un objet en maintenant la touche Ctrl.
- Un clic droit sur une zone vierge donne un accès aux propriétés de la zone de construction.
- Pour supprimer un objet, on clique sur « Effacer » depuis le menu contextuel (clic droit).

CaRMetal

L'interface



Palette « Édition »

Icône	Description de la fonctionnalité	
	Outil permettant de déplacer un objet déjà construit ou de copier une zone dans le presse-papier en tant qu'image. Un clic sur cet outil permet de visualiser les objets mobiles en les faisant brièvement clignoter.	
	Outil bascule permettant de cacher ou montrer un objet.	Ces deux outils fonctionnent conjointement.
	Outil bascule permettant d'afficher ou masquer tous les objets cachés.	
	Outil permettant de supprimer l'objet sélectionné, ainsi que tous ceux qui en dépendent.	

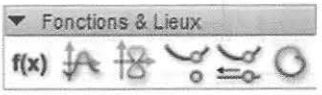
À savoir

- On peut aussi déplacer un objet en maintenant un clic droit sur celui-ci, quel que soit l'outil sélectionné.
- Pour déplacer la totalité de la figure dans la zone de construction, il suffit de maintenir un clic droit sur une zone vierge tout en déplaçant la souris.
- Un clic droit sur une zone vierge donne un accès direct à la bibliothèque de macros.

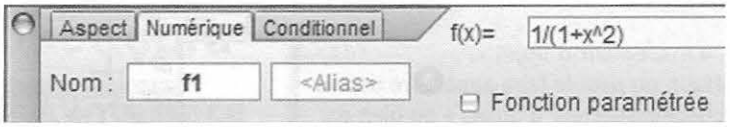
Cette icône correspond à l'outil « Monkey » qui permet de « secouer » la construction : lorsqu'il est maintenu enfoncé à la souris, les points mobiles prennent des positions aléatoires. Cela permet de tester une propriété géométrique, par exemple la concourance de trois droites.

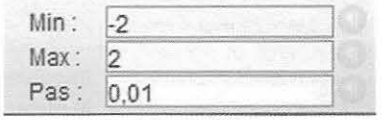
Les fonctions

La création de fonctions s'effectue depuis trois premières icônes de la palette ci-contre :



Exemple d'utilisation de la deuxième icône :





Le menu Macros/Fonctions permet d'accéder à des fonctionnalités telles que recherche d'extrema, tangente, nombre dérivée.

Trace et lieu

La trace d'un objet est activable depuis la barre des propriétés, dans l'onglet « Aspect ».
Cela permet de repérer dynamiquement les endroits parcourus par l'objet en question.
Un inconvénient de cet outil est que les traces sont éphémères (elles s'effacent si on déplace la figure), cela peut être résolu en utilisant l'outil « Lieu de point ».

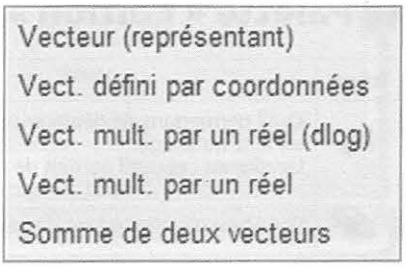
Cet outil est repérable grâce à l'icône suivante . Il suffit de cliquer sur le point dont on désire le lieu puis le point dont il dépend.

Les vecteurs

Création d'un vecteur en cliquant sur l'origine puis l'extrémité :  .

Construction de l'image du point C par la translation de vecteur $\vec{u}$:  .

Toutes les autres constructions sont accessibles depuis le menu Macros\Vecteurs.
Après avoir lancé la macro, il suffit de suivre les instructions dans la barre de status.



GeoGebra est un logiciel libre, téléchargeable gratuitement à l'adresse suivante : http://www.geogebra.org/cms/ .

CaRMetal est un logiciel libre, téléchargeable gratuitement à l'adresse suivante : http://db-maths.nuxit.net/CaRMetal/. On pourra aussi trouver à cette adresse toute une série de vidéo-tutoriels destinés à favoriser une bonne prise en main.

Sous la direction de

Claude Deschamps

RÉGION LANGUEDOC-ROUSSILLON
OPÉRATION GRATUITÉ

Auteurs

Claire Berthelot

Serge Bertrand

Delphine Cheymol

Geneviève Deylon

Gilles Dowek

Jean-Pascal Gaumet

Nicolas Jousse

Didier Krieger

Pierre-Marc Mazat

Anne Redouté-Metrich

maths Term s

enseignement de spécialité

programme 2012

8, RUE FÉROU 75278 PARIS CEDEX 06
WWW.EDITIONS-BELIN.COM

Belin
ÉDITEUR INDÉPENDANT
DEPUIS 1777

lib' Livre Interactif Belin

Vous êtes prescripteurs de nos manuels papier,*

nous vous offrons pendant 4 ans

le Lib' Basic

votre manuel vidéoprojetable

Les Lib' Basic Mathématiques lycée sont accessibles sur www.libtheque.fr/mathslycee
en cliquant sur le bouton



Avec votre Lib' Basic, vous pouvez animer votre cours en classe
grâce à la vidéoprojection et à la boîte à outils :

		Lib' Basic	Lib' Premium
Votre application partout avec vous !	Accès sur internet	✓	✓
	Téléchargement sur un ordinateur	✓	✓
	Exportation sur une clé USB	✓	✓
Animation du cours	Vidéoprojection	✓	✓
	Affichage d'une double page en plein écran	✓	✓
	Boîte à outils (zoom, surligneur, cache, rideau…)	✓	✓
	Accès aux compléments pédagogiques gratuits (livre du prof, exercices complémentaires)	✓	✓
Personnalisation du cours	Fonction Comparateur de documents	✗	✓
	Personnalisation d'une page	✗	✓
	Création d'une page	✗	✓
	Accès à l'intégralité des documents du manuel dans la médiathèque et aux ressources complémentaires	✗	✓
	Import de vos documents personnels (vidéo/image/audio) via la médiathèque	✗	✓

✓ Oui ✗ Non

**offre réservée aux professeurs dont les élèves sont équipés des manuels papier correspondants*

Toutes les références à des sites Internet présentées dans cet ouvrage ont été vérifiées attentivement à la date d'impression. Compte tenu de la volatilité des sites et du détournement possible de leur adresse, les éditions Belin ne peuvent en aucun cas être tenues pour responsables de leur évolution. Nous appelons donc chaque utilisateur à rester vigilant quant à leur utilisation.

Le code de la propriété intellectuelle n'autorise que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » [article L. 122-5] ; il autorise également les courtes citations effectuées dans un but d'exemple ou d'illustration. En revanche « toute représentation ou reproduction intégrale ou partielle, sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » [article L. 122-4]. La loi 95-4 du 3 janvier 1994 a confié au C.F.C. (Centre français de l'exploitation du droit de copie, 20, rue des Grands-Augustins, 75006 Paris), l'exclusivité de la gestion du droit de reprographie. Toute photocopie d'œuvres protégées, exécutée sans son accord préalable, constitue une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal.

DANGER LE PHOTOCOPILLAGE TUE LE LIVRE

© Éditions Belin, 2012

ISBN 978-2-7011-6198-3

Sommaire

Présentation du manuel 4

Programme de l'enseignement de spécialité 6

1 Divisibilité et congruence 8

- Vérifier ses acquis 8
- Activités d'introduction 10
- Le cours et les capacités attendues
  - **A.** Divisibilité dans $\mathbb{Z}$ 14
  - **B.** Division euclidienne 16
  - **C.** Congruences 18
- Travaux pratiques 22
- Exercices 26
- Préparer le BAC 36
- Accompagnement personnalisé 40

2 PGCD, théorème de Bézout et théorème de Gauss 42

- Vérifier ses acquis 42
- Activités d'introduction 44
- Le cours et les capacités attendues
  - **A.** PGCD de deux entiers 48
  - **B.** Entiers premiers entre eux 52
  - **C.** Le théorème de Bézout 52
  - **D.** Le théorème de Gauss 54
- Travaux pratiques 56
- Exercices 60
- Préparer le BAC 70
- Accompagnement personnalisé 74

3 Nombres premiers 76

- Vérifier ses acquis 76
- Activités d'introduction 78
- Le cours et les capacités attendues
  - **A.** Définition et premières propriétés 82
  - **B.** Décomposition en facteurs premiers 84
- Travaux pratiques 86
- Exercices 90
- Préparer le BAC 98
- Accompagnement personnalisé 102

4 Matrices 104

- Vérifier ses acquis 104
- Activités d'introduction 106
- Le cours et les capacités attendues
  - **A.** Notion de matrices 110
  - **B.** Opérations sur les matrices 112
  - **C.** Matrices inversibles 116
- Travaux pratiques 118
- Exercices 122
- Préparer le BAC 134
- Accompagnement personnalisé 138

5 Suites de matrices 140

- Vérifier ses acquis 140
- Activités d'introduction 142
- Le cours et les capacités attendues
  - **A.** Matrices stochastiques 146
  - **B.** Étude asymptotique 148
- Travaux pratiques 150
- Exercices 154
- Préparer le BAC 164
- Accompagnement personnalisé 168

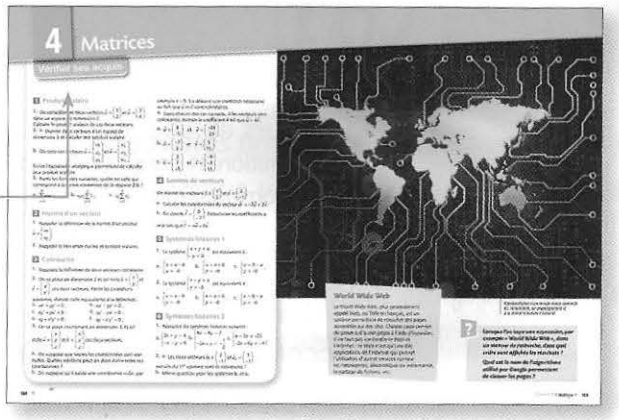
Corrigés des exercices 170

Présentation du manuel

Ouverture

Vérifier ses acquis

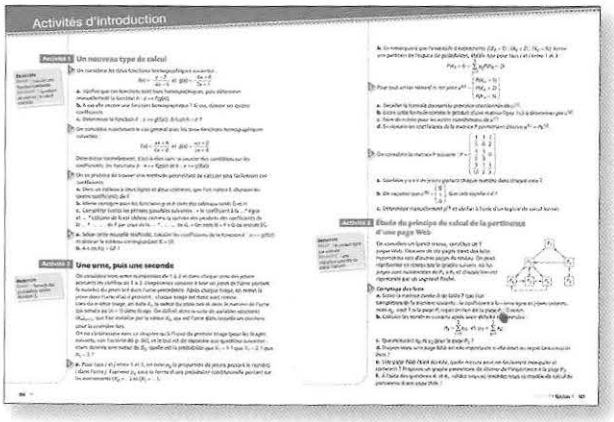
Des exercices pour faire le point sur les connaissances acquises des années précédentes.



Une présentation du chapitre à travers divers éclairages : histoire des sciences, vie quotidienne, etc.

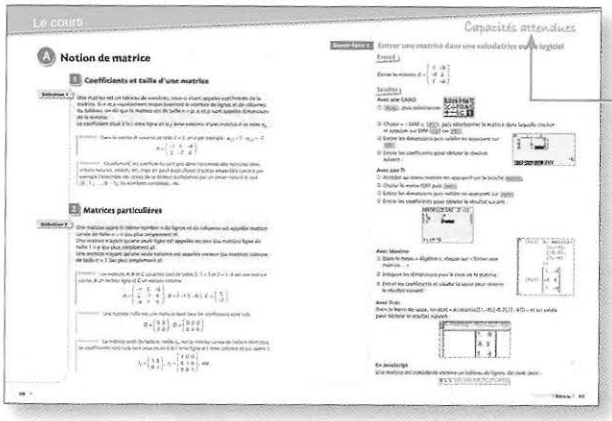
Activités d'introduction

Des activités pour réviser et découvrir les notions du chapitre.



Le cours

Les contenus du programme illustrés par des exemples et des démonstrations.



Les capacités attendues

– Des exercices résolus pour aborder les savoir-faire du programme dont les savoir-faire TICE et algorithmiques.

Logos et indications

Activité faisant appel à l'ordinateur.

Activité faisant appel à la calculatrice.

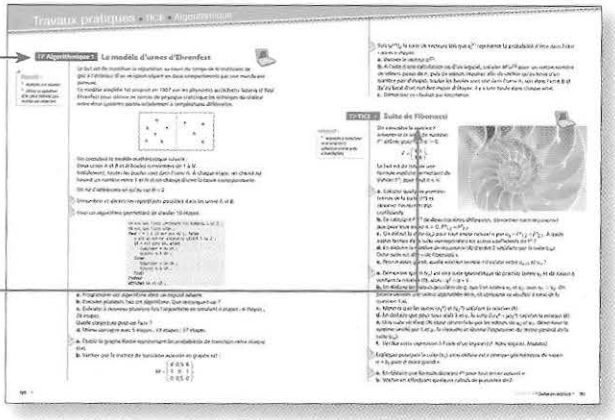
Ressource numérique disponible dans la partie compléments pédagogiques du site www.libtheque.fr/mathslycee.

25 67 Exercices corrigés en fin de manuel.

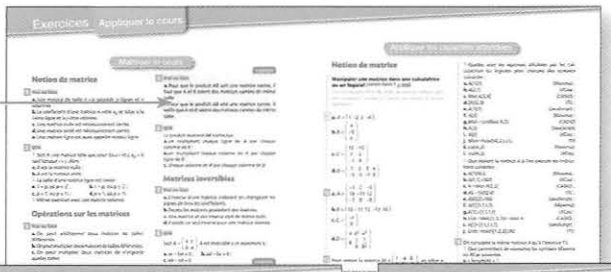
Travaux pratiques

Des **TP Algorithmiques** pour prendre le temps d'expérimenter les notions apprises.

Des **TP TICE** pour expérimenter à l'aide de logiciels.



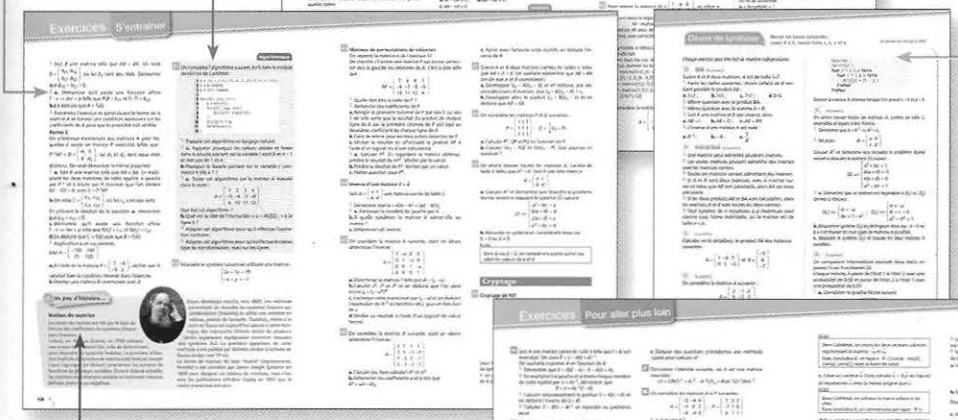
Exercices



Des exercices de difficulté croissante :

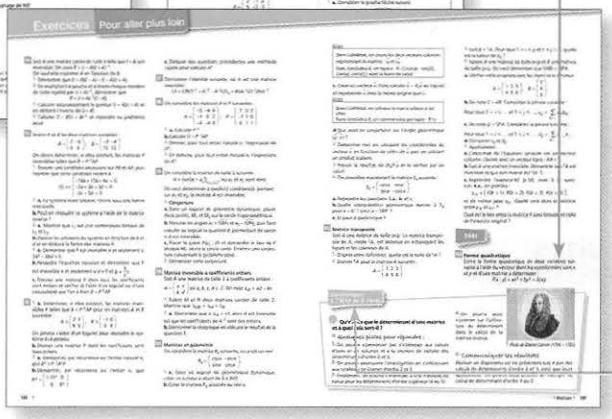
- **Appliquer le cours**
- **S'entraîner**
- **Pour aller plus loin**

Des exercices de **logique** et d'**algorithmique**.



Devoir de synthèse
Une série d'exercices avec indication d'un barème pour réviser avant les devoirs.

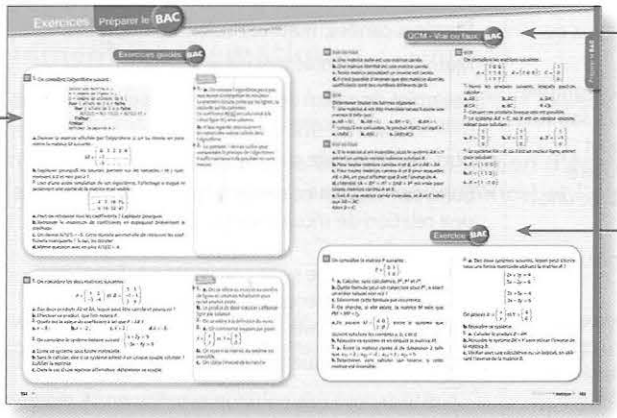
Des défis



Un peu d'histoire
Un exercice pour se familiariser avec quelques mathématiciens célèbres et se donner des repères chronologiques.

Des sujets d'exposés pour s'entraîner à la **communication écrite ou orale**.

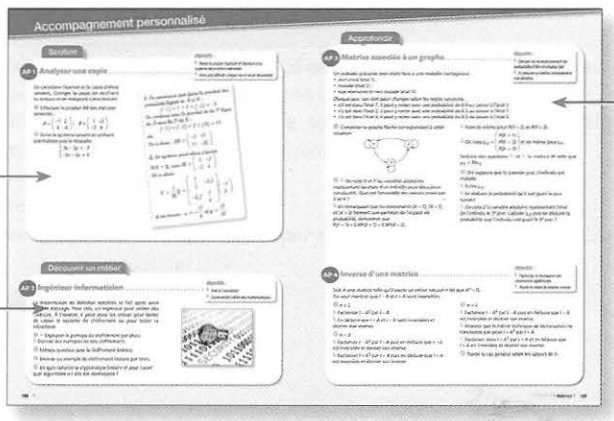
Préparer le BAC



Des **exercices type Bac guidés**

Des **QCM**, des **Vrais** ou **faux** et des **exercices type Bac**

Accompagnement personnalisé



Des exercices de **soutien**

Découverte de métiers
liés aux mathématiques

Des exercices d'**approfondissement**

Programme de Term S

Enseignement de spécialité

Extrait du programme de Terminale S publié au B.O. spécial n° 8 du 13 octobre 2011.

Arithmétique

Les problèmes étudiés peuvent notamment être issus de la cryptographie ou relever directement de questions mathématiques, par exemple à propos des nombres premiers.

Exemples de problèmes	Contenus	Manuel
Problèmes de codage (codes barres, code ISBN, clé du Rib, code Insee). Problèmes de chiffrement (chiffrement affine, chiffrement de Vigenère, chiffrement de Hill). Questionnement sur les nombres premiers : infinitude, répartition, tests de primalité, nombres premiers particuliers (Fermat, Mersenne, Carmichaël). Sensibilisation au système cryptographique RSA.	• Divisibilité dans $\mathbb{Z}$. • Division euclidienne. • Congruences dans $\mathbb{Z}$. • PGCD de deux entiers. • Entiers premiers entre eux. • Théorème de Bézout. • Théorème de Gauss. • Nombres premiers. • Existence et unicité de la décomposition en produit de facteurs premiers.	• Chapitre 1 Divisibilité et congruence • Chapitre 2 PGCD, théorème de Bézout et théorème de Gauss • Chapitre 3 Nombres premiers

Matrices et suites

Il s'agit d'étudier des exemples de processus discrets, déterministes ou stochastiques, à l'aide de suites ou de matrices.
On introduit le calcul matriciel sur des matrices d'ordre 2. Les calculs sur des matrices d'ordre 3 ou plus sont essentiellement effectués à l'aide d'une calculatrice ou d'un logiciel.

Exemples de problèmes	Contenus	Manuel
Marche aléatoire simple sur un graphe à deux ou trois sommets. Marche aléatoire sur un tétraèdre ou sur un graphe à N sommets avec saut direct possible d'un sommet à un autre : à chaque instant, le mobile peut suivre les arêtes du graphe probabiliste ou aller directement sur n'importe quel sommet avec une probabilité constante p. Étude du principe du calcul de la pertinence d'une page web. Modèle de diffusion d'Ehrenfest : N particules sont réparties dans deux récipients ; à chaque instant, une particule choisie au hasard change de récipient. Modèle proie prédateur discrétisé : – évolution couplée de deux suites récurrentes ; – étude du problème linéarisé au voisinage du point d'équilibre.	• Matrices carrées, matrices colonnes : opérations. • Matrice inverse d'une matrice carrée. • Exemples de calcul de la puissance n-ième d'une matrice carrée d'ordre 2 ou 3. • Écriture matricielle d'un système linéaire. • Suite de matrices colonnes (U_n) vérifiant une relation de récurrence du type $U_{n+1} = AU_n + C$: – recherche d'une suite constante vérifiant la relation de récurrence ; – étude de la convergence. • Étude asymptotique d'une marche aléatoire.	• Chapitre 4 Matrices • Chapitre 5 Suites de matrice

Algorithmique

En seconde, les élèves ont conçu et mis en œuvre quelques algorithmes. Cette formation se poursuit tout au long du cycle terminal.

Dans le cadre de cette activité algorithmique, les élèves sont entraînés à :

- décrire certains algorithmes en langage naturel ou dans un langage symbolique ;
- en réaliser quelques-uns à l'aide d'un tableur ou d'un programme sur calculatrice ou avec un logiciel adapté ;
- interpréter des algorithmes plus complexes.

Aucun langage, aucun logiciel n'est imposé.

L'algorithmique a une place naturelle dans tous les champs des mathématiques et les problèmes posés doivent être en relation avec les autres parties du programme (arithmétique, matrices et suites, logique) mais aussi avec les autres disciplines ou le traitement de problèmes concrets.

À l'occasion de l'écriture d'algorithmes et de programmes, il convient de donner aux élèves de bonnes habitudes de rigueur et de les entraîner aux pratiques systématiques de vérification et de contrôle.

La mise en œuvre de l'algorithmique sera faite dans ce manuel dans les Travaux pratiques **TP Algorithmique** et dans les exercices **Algorithmique**.

Instructions élémentaires (affectation, calcul, entrée, sortie)

Les élèves, dans le cadre d'une résolution de problèmes, doivent être capables :

- d'écrire une formule permettant un calcul ;
- d'écrire un programme calculant et donnant la valeur d'une fonction, ainsi que les instructions d'entrées et sorties nécessaires au traitement.

Boucle et itérateur, instruction conditionnelle

Les élèves, dans le cadre d'une résolution de problèmes, doivent être capables de :

- programmer un calcul itératif, le nombre d'itérations étant donné ;
- programmer une instruction conditionnelle, un calcul itératif, avec une fin de boucle conditionnelle.

Notations et raisonnement mathématiques

Cette rubrique, consacrée à l'apprentissage des notations mathématiques et à la logique, ne doit pas faire l'objet de séances de cours spécifiques, mais doit être répartie sur toute l'année scolaire.

En complément des objectifs rappelés ci-dessous, le travail sur la notion d'équivalence doit naturellement être poursuivi (propriété caractéristique, raisonnement par équivalence) et l'on introduit le raisonnement parrécurrence.

Notations mathématiques

Les élèves doivent connaître les notions d'élément d'un ensemble, de sous-ensemble, d'appartenance et d'inclusion, de réunion, d'intersection et de complémentaire et savoir utiliser les symboles de base correspondants : $\in$, $\subset$, $\cup$, $\cap$ ainsi que la notation des ensembles de nombres et des intervalles.

Pour le complémentaire d'un ensemble A, on utilise la notation des probabilités $\overline{A}$.

Pour ce qui concerne le raisonnement logique, les élèves sont entraînés sur des exemples à :

- utiliser correctement les connecteurs logiques « et », « ou » et à distinguer leur sens des sens courants de « et », « ou » dans le langage usuel ;
- utiliser à bon escient les quantificateurs universel, existentiel (les symboles $\forall$, $\exists$ ne sont pas exigibles) et à repérer les quantifications implicites dans certaines propositions et, particulièrement, dans les propositions conditionnelles ;
- distinguer, dans le cas d'une proposition conditionnelle, la proposition directe, sa réciproque, sa contraposée et sa négation ;
- utiliser à bon escient les expressions « condition nécessaire », « condition suffisante » ;
- formuler la négation d'une proposition ;
- utiliser un contre-exemple pour infirmer une proposition universelle ;
- reconnaître et utiliser des types de raisonnement spécifiques : raisonnement par disjonction des cas, recours à la contraposée, raisonnement par l'absurde.

1 Divisibilité et congruence

Vérifier ses acquis

1 Les ensembles de nombres

1. Pour chaque nombre, dire s'il appartient à $\mathbb{N}$, à $\mathbb{Z}$, à $\mathbb{Q}$ ou à $\mathbb{R}$.

$a = \dfrac{144}{32}$; $b = \sqrt{144}$; $c = \dfrac{144}{27}$;

$d = -\sqrt{3}$; $e = 3 + \pi$; $f = -13{,}0$.

2. Vrai ou faux

a. $a \in \mathbb{N}$ et $b \in \mathbb{N} \Rightarrow a - b \in \mathbb{N}$.

b. $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}$.

c. $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \Rightarrow ab \in \mathbb{Z}$.

d. $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^* \Rightarrow \dfrac{a}{b} \in \mathbb{Z}$.

2 Multiples ou diviseurs

a. $13^4 - 3^4$ est-il multiple de 160 ?

b. 56 879 est-il divisible par 436 ?

c. Déterminer tous les entiers naturels diviseurs de 60.

3 Utiliser les critères de divisibilité

Vrai ou Faux

a. 5 148 est divisible par 3 et 9.

b. 2 634 est divisible par 2 et 3.

c. 46 730 est divisible par 5 et 3.

4 Propositions sur la divisibilité

Vrai ou faux Justifier si possible.

a. Si un entier naturel est divisible par 6, alors il est divisible par 3.

b. Si un entier naturel est divisible par 3, alors il est divisible par 6.

c. Si un entier naturel est divisible par 6 et 5, alors il est divisible par 30.

d. Si un entier naturel est divisible par 6 et 4, alors il est divisible par 24.

e. Si 3 divise les entiers naturels a et b, alors 3 divise $a + b$.

5 Division euclidienne

a. Poser la division euclidienne de 371 par 31.

b. Quel est le dividende ? le diviseur ? le quotient ? le reste ?

c. Traduire cette division euclidienne par une égalité et un encadrement.

6 Effectuer sans calculatrice la division euclidienne

a. de 45 par 2 ; **b.** de 47 par 3 ;

c. de 497 par 23 ; **d.** de 756 par 97 ;

e. de 750 par 27.

7 Fraction irréductible

Écrire les rationnels suivants sous forme d'une fraction irréductible :

$a = \dfrac{43}{57}$; $b = \dfrac{355}{220}$; $c = \dfrac{435}{210}$.

8 Une autre écriture d'un rationnel

Écrire les rationnels suivants sous la forme $a + \dfrac{b}{c}$, où $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $c \in \mathbb{N}^*$ et $0 \leqslant \dfrac{b}{c} < 1$.

a. $\dfrac{35}{23}$; **b.** $-\dfrac{35}{23}$; **c.** $\dfrac{42}{13}$; **d.** $\dfrac{77}{4}$.

9 Pair ou impair

n est un entier naturel. Démontrer les propriétés suivantes :

a. Si l'entier naturel n est pair, alors n^2 est pair.

b. Si l'entier naturel n est impair, alors n^2 est impair.

c. Si l'entier naturel n^2 est pair, alors n est pair.

d. Si l'entier naturel n^2 est impair, alors n est impair.

e. Montrer que $n(n + 1)$ est pair.

10 Une curiosité

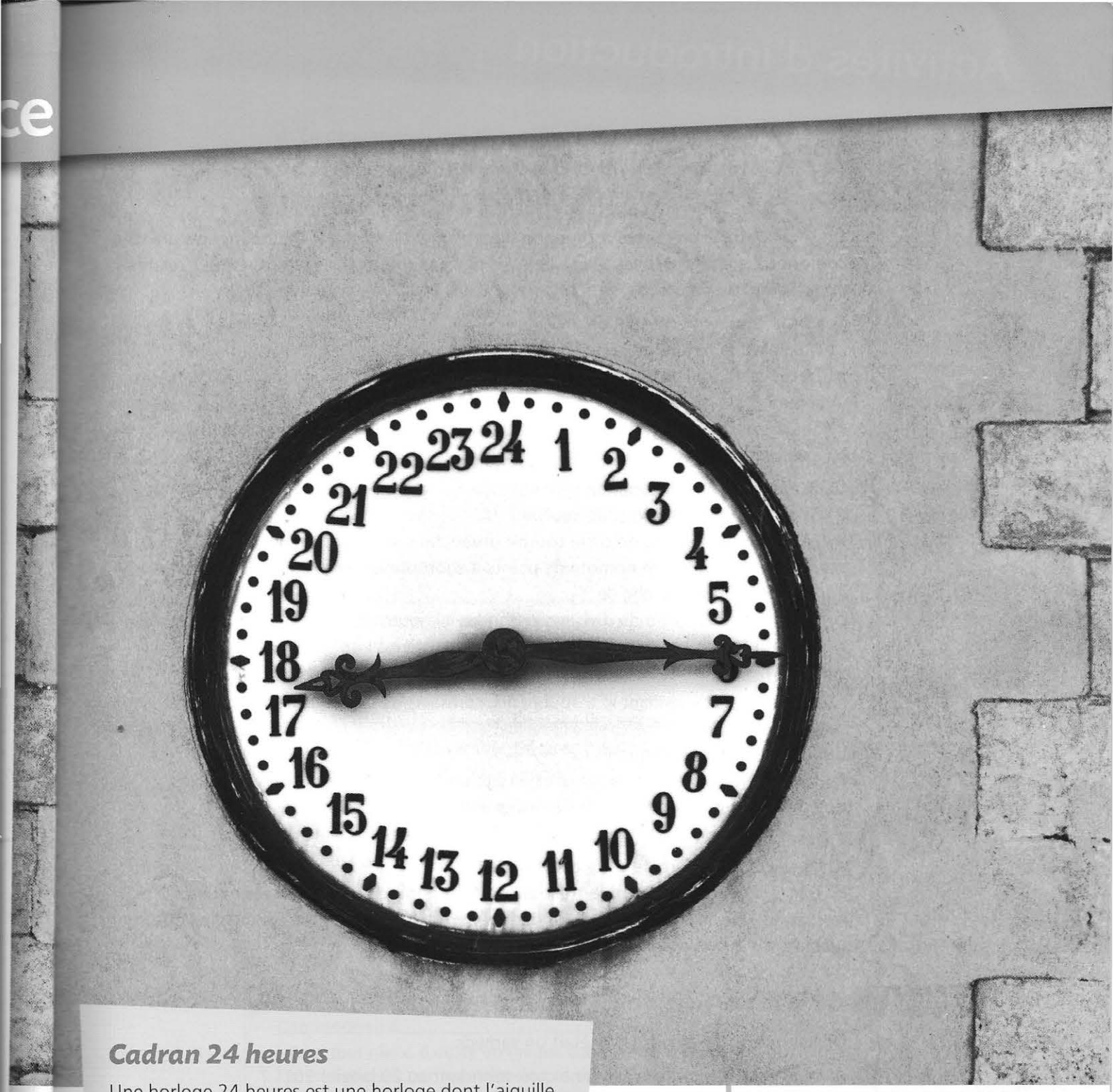
a. Vérifier que $32 + 23$, $94 + 49$ et $57 + 75$ sont des multiples de 11.

b. Démontrer que ce résultat est vrai pour tous les entiers naturels s'écrivant avec deux chiffres dans le système décimal.

11 Une autre curiosité

a. Démontrer que les entiers naturels de trois chiffres identiques sont des multiples de 37.

b. Démontrer que les entiers naturels de 6 chiffres identiques sont des multiples de 37.



Une horloge 24 heures permet d'obtenir une position horaire plus « naturelle ».

Cadran 24 heures

Une horloge 24 heures est une horloge dont l'aiguille des heures effectue un seul tour de cadran dans la journée, au contraire des cadrans de 12 heures pour lesquels les aiguilles font deux tours dans une journée. Elle peut être utile à des personnes se trouvant dans des endroits privés de la vue du soleil (sous-marins, grottes, etc.) ou au contraire pour des personnes qui verraient le soleil se lever et se coucher plusieurs fois dans la journée, comme les astronautes.
Le principal inconvénient de ce type d'horloge est la difficulté pour lire l'heure due, principalement, à la très longue habitude des cadrans conventionnels.

? ***Quelle heure est-il quand les deux aiguilles se superposent sur 22 ?***

Expliquer la différence avec un cadran de 12 heures ?

Activités d'introduction

Activité 1 Points à coordonnées entières sur une courbe

Objectifs
Revoir : la nature de quelques courbes du plan, la divisibilité dans les entiers relatifs.
Découvrir : la recherche de points à coordonnées entières appartenant à une courbe, la notion de diviseurs associés, l'utilité d'une factorisation.

On se place dans un repère orthonormal du plan et on souhaite déterminer les points à coordonnées entières (c'est-à-dire dont les deux coordonnées sont des entiers relatifs) appartenant à une courbe.

1 Cas de la courbe $\mathscr{C}_1$ d'équation $2x + 4y = 5$.
a. Quelle est la nature de cette courbe ?
b. Tracer cette courbe. Cette courbe semble-t-elle contenir des points à coordonnées entières ?
c. En utilisant la notion de diviseur, montrer que $\mathscr{C}_1$ ne contient aucun point à coordonnées entières.

2 Cas de la courbe $\mathscr{C}_2$ d'équation $xy = 10$.
a. Quelle est la nature de cette courbe ?
b. En traçant la branche de cette courbe située dans le quart de plan $x > 0$ et $y > 0$, essayer de déterminer le nombre de points à coordonnées entières qui semblent appartenir à cette branche de $\mathscr{C}_2$.
c. En utilisant la notion de diviseur, répondre à la question **b**.
d. Quel est le nombre de points à coordonnées entières appartenant à $\mathscr{C}_2$?

Commentaire

Deux entiers x et y vérifiant $xy = 10$ sont deux diviseurs de 10 dits associés.

3 Cas de la courbe $\mathscr{C}_3$ d'équation $x^2 - y^2 = 7$.
En factorisant le premier membre et en utilisant la notion de diviseurs associés, déterminer tous les points à coordonnées entières appartenant à $\mathscr{C}_3$.

4 Cas de la courbe $\mathscr{C}_4$ d'équation $x^2 + y^2 = 7$.
a. Quelle est la nature de cette courbe ?
b. Tracer la courbe $\mathscr{C}_4$. Semble-t-elle contenir des points à coordonnées entières ?
c. Justifier que $x^2 < 7$ et $y^2 < 7$. En déduire, en faisant une étude exhaustive, que $\mathscr{C}_4$ ne contient aucun point à coordonnées entières.

Activité 2 Quel jour de la semaine étions-nous le ... ?

Objectifs
Revoir : le calcul du jour de la semaine d'une date, la division euclidienne.
Découvrir : l'importance du reste, la notion de congruence.

On sait que le 1er janvier 2011 était un samedi.

1 **a.** Quel était le jour de la semaine correspondant au 29 janvier 2011 ?
b. Déterminer le nombre de jours écoulés entre le 1er janvier 2011 et le 29 janvier 2011 (c'est-à-dire le nombre de jours écoulés entre le 1er janvier à 0h et le 29 janvier à 0h). On remarque que dans ce calcul on ne compte pas le dernier jour.
c. Déterminer le nombre de jours écoulés entre le 1er janvier 2011 et chaque samedi du mois. Que remarque-t-on ?
d. Déterminer le nombre de jours écoulés entre le 1er janvier 2011 et chaque dimanche du mois. Que remarque-t-on ? Faire de même pour tous les autres jours de la semaine.

2 On veut déterminer le jour de la semaine correspondant au 21 mars 2011.
a. Déterminer le nombre de jours N écoulés entre le 1er janvier 2011 et le 21 mars 2011.
b. Déterminer le nombre q de semaines entières écoulées et le nombre r de jours restant après ces q semaines.
c. Écrire N en fonction de q et r.

d. En déduire quel jour de la semaine était le 21 mars 2011.

3 De la même façon déterminer quel jour de la semaine était le 25 décembre 2011.

4 Déterminer le jour de la semaine correspondant au 25 décembre 2013.

Commentaire

Tout dépend du reste de la division euclidienne de N par 7.
Deux entiers N et N' qui ont le même reste dans la division euclidienne par 7 sont dits congrus modulo 7 et on note $N \equiv N'$ [7].

Activité 3 Partie entière d'un réel



OBJECTIFS

Revoir : les entiers naturels, la notion de plus petit élément et de plus grand élément.

Découvrir : de nouvelles propriétés des entiers naturels et la partie entière.

1 **a.** $\mathbb{N}$ a-t-il un plus petit élément ? $\mathbb{N}$ a-t-il un plus grand élément ?
b. Soit A l'ensemble des entiers naturels dont le carré est inférieur à 15.
A contient-il au moins un élément ? A a-t-il un plus grand élément ? A est-il majoré ?
c. Soit I l'intervalle]2 ; 15[. Cet ensemble a-t-il un plus petit élément ? Un plus grand élément ?
d. Mêmes questions avec $J = I \cap \mathbb{N}$.

Commentaire

L'ensemble des entiers naturels possède les propriétés suivantes :
- Toute partie de $\mathbb{N}$ non vide admet un plus petit élément.
- Toute partie de $\mathbb{N}$ non vide et majorée admet un plus grand élément.

2 Tracer la droite des réels en figurant les entiers relatifs.
Soit un réel x, vous semble-t-il possible de l'encadrer par deux entiers consécutifs ? La solution vous semble-t-elle unique ?

3 Soit x un réel positif ou nul.
a. On considère l'ensemble M des entiers naturels inférieurs ou égaux à x. M est-il non vide ? M est-il majoré ? Que peut-on en conclure ?
b. On appelle q le plus grand élément de M.
Démontrer que $q \leqslant x < q + 1$.
c. Cet entier naturel q est-il unique ?

Aide

Considérer deux entiers relatifs q et q' vérifiant l'encadrement obtenu en **b.**, encadrer la différence q-q' et conclure.

4 Pouvez-vous étendre ce résultat dans le cas d'un réel strictement négatif x ?

Commentaire

Pour tout réel x, il existe un unique entier relatif q vérifiant $q \leqslant x < q + 1$.
q est appelé la partie entière de x et est noté $E(x)$.

5 **a.** Calculer $E(-3)$; $E(-3{,}5)$; $E(-2{,}3)$; $E(-0{,}5)$; $E(0{,}5)$; $E(1{,}5)$.
Tracer la courbe de la fonction partie entière.
b. La fonction partie entière est présente sur les calculatrices TI et Casio (PartEnt ou int sur TI et Int sur Casio). Retrouver les résultats précédents sur la calculatrice.

6 Soit a un entier naturel et b un entier naturel non nul.
a. Comment traduire que q est le quotient et r le reste de la division euclidienne de a par b ?
b. En déduire que $q \leqslant \dfrac{a}{b} < q + 1$. Que peut-on en déduire ?
c. Écrire un algorithme donnant le quotient q et le reste r de la division euclidienne de a par b.
d. Effectuer la division euclidienne de 75 par 9.

Activités d'introduction

Commentaire

Pour tout entier naturel a et pour tout entier naturel non nul b, le quotient de la division euclidienne de a par b est égal à la partie entière de $\frac{a}{b}$ notée $E\left(\frac{a}{b}\right)$.

Activité 4 Ce code est-il exact ?

OBJECTIFS
Revoir : l'importance du reste.
Découvrir : la clé de contrôle d'un code.

Les codes barres



Actuellement tout objet fabriqué a un code formé de 13 chiffres. Les douze premiers chiffres désignent le produit et le treizième est calculé à partir des douze chiffres précédents de la façon suivante :

Pour le code $C = \overline{a_1 a_2 ... a_{12} a_{13}}$, a_{13} est défini par la propriété :

$3 \times \left(\sum_{i=1}^{6} a_{2i}\right) + \sum_{i=0}^{6} a_{2i+1}$ est divisible par 10.

1 Des exemples

a. Vérifier cette formule pour le code $C = 9\ 782701\ 158334$.

b. Que peut-on dire de $C_1 = 9\ 782701\ 157334$ et $C_2 = 9\ 782707\ 158334$?

c. On a interverti deux chiffres consécutifs : $C_3 = 9\ 782701\ 153834$. Ce code vérifie-t-il la formule ? Que peut-on en déduire ?

Commentaire

Le treizième chiffre est appelé la clé de contrôle du code.

2 Calcul de la clé de contrôle

a. Déterminer la clé de contrôle x du code-barres $325\ 1241\ 04176\ x$.

b. Donner un code-barres différent ayant la même clé de contrôle.

c. On pose $N = 3 \times \left(\sum_{i=1}^{6} a_{2i}\right) + \sum_{i=0}^{5} a_{2i+1}$ et on note u le chiffre des unités de N.

Montrer que $a_{13} = 10 - u$.

3 Utilité de la clé de contrôle : détecter certaines erreurs

a. Démontrer que si un seul des chiffres est erroné, l'erreur est détectée.

b. On suppose que deux chiffres consécutifs ont été intervertis. L'erreur sera-t-elle détectée ?

4 Peut-on retrouver un chiffre effacé ?

Déterminer le chiffre manquant du code $325\ 2x37\ 04176\ 7$.

Activité 5 Savez-vous vérifier votre numéro INSEE ?

OBJECTIFS
Revoir : l'importance du reste.
Découvrir : des propriétés du reste et des congruences.

Le code INSEE d'une personne est formé de 15 chiffres : 13 chiffres qui forment le numéro INSEE suivis d'une clé de contrôle de 2 chiffres, calculée de la façon suivante : si N désigne le nombre formé des treize premiers chiffres et r le reste de la division euclidienne de N par 97, alors la clé de contrôle K est le nombre $K = 97 - r$ (ce qui équivaut à la condition $N + K$ est divisible par 97).



1 **Un exemple de calcul de la clé**

Calculer à l'aide de la calculatrice la clé K pour $N = 2\,84\,04\,92\,019\,081$.

2 **Ces nombres sont trop grands pour certaines calculatrices. Voici une autre façon de calculer le reste r de la division euclidienne de N par 97 en se ramenant à des nombres plus petits.**

a. Écrire N sous la forme $N = 10^6 \times A + B$ avec $0 \leqslant B < 10^6$.

b. Vérifier que le reste de la division euclidienne de 10^6 par 97 est 27 et déterminer les restes r_1 et r_2 des divisions euclidiennes de A et B par 97.

c. Soit $N' = 27r_1 + r_2$. Déterminer le reste de la division euclidienne de N' par 97. Que constatez-vous ?

d. Justifier ce résultat. Pour cela, on pourra montrer que si a et b ont pour restes r_1 et r_2 dans la division euclidienne par 97, $a + b$ a le même reste que $r_1 + r_2$ et $a \times b$ le même reste que $r_1 \times r_2$ dans la division euclidienne par 97. Conclure.

Mémo

On dit que N et N' sont **congrus modulo** 97 et on note $N \equiv N'$ [97].

Commentaire

Si $a \equiv a_1$ [n] et $b \equiv b_1$ [n], alors $a + b \equiv a_1 + b_1$ [n] et $a \times b \equiv a_1 \times b_1$ [n].

3 **Utilité de la clé de contrôle**

a. Modifier un chiffre du numéro de la question 1., recalculer la clé et conclure.

b. Échanger deux chiffres consécutifs dans le numéro de la question 1, recalculer la clé et conclure.

c. Conjecturer des erreurs qui semblent décelables.

d. Donner un exemple d'erreur non décelables.

Activité 6 Pour coder vos messages : le chiffrement affine !

Objectifs

Revoir : l'importance du reste.

Découvrir : le chiffrement affine.

Le principe du chiffrement affine est le suivant. On numérote de 0 à 25 et dans l'ordre alphabétique les 26 lettres de l'alphabet français.

On se donne deux nombres a et b, et à chaque n, rang d'une lettre L, correspond le nombre n' qui est le reste de la division euclidienne de $an + b$ par 26. Le nombre n' représente le rang d'une lettre L'. En associant ainsi L' à L, on effectue un chiffrement affine défini par le couple (a ; b). Le couple (a ; b) est la clé secrète du chiffrement affine, elle est connue seulement de l'expéditeur et du destinataire.

1 **Exemple 1** : on choisit $a = 3$ et $b = 5$

a. Coder le mot « Euclide ».

b. Recopier et compléter le tableau ci-contre.

c. En utilisant le tableau, retrouver le mot codé par XFNHH

Lettre en clair	A	B	.	.	.	Z
n	0	1				25
n'	5	8				
Lettre codée	F	I				

d. On remarque que ce chiffrement affine est tel que deux lettres distinctes sont codées par deux lettres distinctes et réciproquement toute lettre code une et une seule lettre.

2 **Exemple 2** : on choisit $a = 13$ et $b = 4$

a. Coder les mots RAGE et PEAU. Que constate-t-on ?

b. Que penser de ce chiffrement ?

3 **Questions ouvertes**

a. La clé d'un chiffrement affine étant connue, comment coder et décoder de façon automatique ?

b. Peut-on retrouver la clé d'un chiffrement affine à partir d'un texte codé ?

c. Comment reconnaître « les bonnes clés » ?

A Divisibilité dans $\mathbb{Z}$

1 Définition

Définition 1

Étant donnés deux entiers relatifs a et b, on dit que a est un diviseur de b ou que b est un multiple de a lorsqu'il existe un entier relatif k tel que $b = ka$.
On dit aussi que a divise b ou que b est divisible par a.

Note : *L'ensemble des multiples de a est noté $a\mathbb{Z}$*

Notation : Si a est un diviseur de b, on note : $a|b$.

Exemple : $210 = 3 \times 70$, donc 70 est un diviseur de 210 ou 210 est un multiple de 70.
$210 = (-14) \times (-15)$, donc -14 et -15 divisent 210.

Remarques :
- Tout entier relatif a est un diviseur de 0 ou 0 est multiple de tout entier relatif.
- Tout entier relatif a admet au moins pour diviseurs : 1, a, -1 et $-a$.
- 1 et -1 ont pour seuls diviseurs 1 et -1.

2 Propriétés de la divisibilité

Propriété 1

Si a divise b et b divise c, alors a divise c.

Démonstration : a divise b et b divise c, donc il existe deux entiers relatifs k et k' tel que $b = ka$ et $c = k'b$. D'où $c = k'ka$ et $kk' \in \mathbb{Z}$, donc a divise c.

Propriété 2

Si a divise b et b divise a, alors $a = b$ ou $a = -b$.

Démonstration : a divise b et b divise a, donc il existe deux entiers relatifs k et k' vérifiant $b = ka$ et $a = k'b$. Ainsi il existe deux entiers relatifs k et k' vérifiant $b = kk'b$.
- si $b \neq 0$, de $b = kk'b$ on déduit $kk' = 1$. k et k' étant des entiers relatifs, $kk' = 1$ implique $k = k' = 1$ ou $k = k' = -1$, donc $a = b$ ou $a = -b$.
- si $b = 0$, alors $a = b = 0$.

Propriété 3

Note : *On dit que $ub + vc$ est une combinaison linéaire à coefficients entiers de b et de c.*

Si a divise b et a divise c, alors a divise $b + c$ et $b - c$ et plus généralement a divise tout entier de la forme $ub + vc$ avec u et v entiers relatifs.

Démonstration : Par hypothèse, il existe deux entiers relatifs k et k' vérifiant $b = ka$ et $c = k'a$.
On en déduit que $ub + vc = uka + vk'a = (uk + vk')a$ et $uk + vk'$ est un entier relatif, donc a divise $ub + vc$.

Propriété 4

Note : *L'ensemble des diviseurs de a est noté D(a).*

Étant donné un entier relatif a et un entier relatif non nul b, si a divise b alors $|a| \leqslant |b|$.

Démonstration : a divise b, donc il existe un entier relatif k vérifiant $b = ka$, d'où $|b| = |k||a|$.
Or b étant un entier relatif non nul, de $b = ka$ on déduit que k est un entier relatif non nul et donc que $|k| \geqslant 1$. De $|k| \geqslant 1$, on déduit $|k||a| \geqslant |a|$, soit $|a| \leqslant |b|$.

Savoir-faire 1 Prouver une divisibilité en utilisant les propriétés

→ Exercice corrigé 19 p. 27
→ Exercices d'application 20 à 25 p. 27

Énoncé

a. Déterminer les entiers relatifs n tels que $n + 4$ divise $n + 17$.
b. Pour $k \in \mathbb{N}$, démontrer que si un entier naturel d divise $10k + 3$ et $6k + 1$ alors il divise 4.

Méthode

- penser à la différence (et à la somme) ;
- choisir des coefficients u et v afin d'éliminer n et k.

Solution

a. • Soit n un entier relatif solution, alors $n + 4$ divise $n + 4$ et $n + 17$ et donc divise $(n + 17) - (n + 4)$, soit 13.
Les diviseurs de 13 étant –13, –1, 1 et 13, on en déduit $n + 4 = -13$ ou $n + 4 = -1$ ou $n + 4 = 1$ ou $n + 4 = 13$, soit $n = -17$ ou $n = -5$ ou $n = -3$ ou $n = 9$.
• Réciproquement, on vérifie que ces quatre entiers sont bien solutions.
• Les solutions sont donc les entiers : –17, –5, –3 et 9.
b. d divise $10k + 3$ et $6k + 1$, donc d divise $3(10k + 3) - 5(6k + 1)$, soit d divise 4.

Savoir-faire 2 Prouver une divisibilité par récurrence

→ Exercice corrigé 26 p. 27
→ Exercices d'application 27 à 30 p. 27

Énoncé

Pour $n \in \mathbb{N}^*$, démontrer que $3^{2n} - 2^n$ est divisible par 7.

Méthode

Utiliser la définition de la divisibilité.

Solution

• Pour $n = 1$, la propriété est vraie.
• On montre que si la propriété est vraie pour $n \geqslant 1$, alors elle est vraie pour $n + 1$.
Par hypothèse de récurrence, il existe $k \in \mathbb{Z}$ tel que $3^{2n} - 2^n = 7k$.
Et $3^{2(n+1)} - 2^{n+1} = 3^2(3^{2n} - 2^n) + 3^2 \times 2^n - 2 \times 2^n = 3^2 \times 7k + 2^n(9 - 2) = 7(2^n + 9k)$ avec $2^n + 9k \in \mathbb{Z}$, donc la propriété est vraie au rang $n + 1$.
• On en déduit que pour tout $n \in \mathbb{N}^*$, $3^{2n} - 2^n$ est divisible par 7.

Savoir-faire 3 Résoudre une équation dans les entiers

→ Exercice corrigé 31 p. 27
→ Exercices d'application 32 à 35 p. 27

Énoncé

Résoudre dans $\mathbb{N}$ l'équation $x^2 - 4y^2 = 20$.

Méthode

- Se ramener à une équation du type $A \times B = C$.
- Faire une étude exhaustive des cas.
- Vérifier et conclure.

Solution

• Soit $(x ; y)$ un couple d'entiers naturels solution.
$x^2 - 4y^2 = 20 \Leftrightarrow (x + 2y)(x - 2y) = 20$
Or $x \in \mathbb{N}$ et $y \in \mathbb{N}$, donc $x + 2y \in \mathbb{N}$ et puisque $(x + 2y)(x - 2y) = 20$, on en déduit donc $x - 2y \in \mathbb{N}$.
Ainsi $x + 2y$ et $x - 2y$ sont deux diviseurs entiers naturels associés de 20 vérifiant $x + 2y \leqslant x - 2y$.
$20 = 1 \times 20 = 2 \times 10 = 4 \times 5$; les diviseurs entiers naturels de 20 sont : 1, 2, 4, 5,10 et 20. Il y a donc trois possibilités : $\begin{cases} x - 2y = 1 \\ x + 2y = 20 \end{cases}$ ou $\begin{cases} x - 2y = 2 \\ x + 2y = 10 \end{cases}$ ou $\begin{cases} x - 2y = 4 \\ x + 2y = 5 \end{cases}$. Seul le second système admet une solution dans $\mathbb{N}$: $(x ; y) = (6 ; 2)$.
• On vérifie que ce couple est solution.
• Le problème a donc un seul couple solution dans $\mathbb{N}$: $(x ; y) = (6 ; 2)$.

B Division euclidienne

1 Division euclidienne dans $\mathbb{Z}$

Propriété 5

Étant donnés un entier relatif a et un entier naturel non nul b, il existe un unique couple d'entiers relatifs $(q ; r)$ tels que $a = bq + r$ et $0 \leqslant r < b$.

Démonstration :

• Existence du couple $(q ; r)$:

On pose $q = E\left(\frac{a}{b}\right)$. L'entier relatif q est défini par l'encadrement : $q \leqslant \frac{a}{b} < q + 1$.

On en déduit, puisque $b > 0$, $bq \leqslant a < b(q + 1)$.

On pose alors $r = a - bq$.

Les entiers relatifs q et r vérifient $a = bq + r$ et $bq \leqslant a < b(q + 1)$, soit $0 \leqslant a - bq < b$, soit $0 \leqslant r < b$.

On a ainsi montré, pour tout entier relatif a et pour tout entier naturel non nul b, l'existence de deux entiers relatifs q et r tels que $a = bq + r$ et $0 \leqslant r < b$.

• Unicité du couple $(q ; r)$:

On suppose qu'il existe deux couples d'entiers relatifs $(q ; r)$ et $(q' ; r')$ vérifiant simultanément :

$a = bq + r = bq' + r'$ et $0 \leqslant r < b < b$ et $0 \leqslant r' < b$.

On en déduit : $r' - r = b(q - q')$, donc $r' - r$ est multiple de b et $-b < r' - r < b$.

Or 0 est le seul multiple de b strictement compris entre $-b$ et b, donc $r' - r = 0$, c'est-à-dire $r = r'$.

Puisque $b \neq 0$, de $b(q - q') = 0$, on en déduit $q - q' = 0$, c'est-à-dire $q = q'$.

Définition 2

Pour tout entier relatif a et pour tout entier naturel non nul b, les entiers relatifs q et r vérifiant $a = bq + r$ et $0 \leqslant r < b$ sont appelés respectivement le quotient et le reste de la division euclidienne de a par b.

Effectuer une division euclidienne, c'est trouver le couple $(q ; r)$ associé au couple $(a ; b)$.

Exemples :

• $58 = 17 \times 3 + 7$ et $0 \leqslant 7 < 17$, donc 3 et 7 sont respectivement le quotient et le reste de la division euclidienne de 58 par 17.

On remarque que l'égalité ne correspond pas à la division euclidienne de 58 par 3, car 7 ne vérifie pas l'encadrement $0 \leqslant r < 3$.

• $-37 = 11 \times (-3) + (-4)$, -4 ne vérifie pas l'encadrement $0 \leqslant r < 11$, on n'a donc pas effectué la division euclidienne de -37 par 11.

$-37 = 11 \times (-4) + 7$ et $0 \leqslant 7 < 11$, donc -4 et 7 sont respectivement le quotient et le reste de la division euclidienne de -37 par 11.

Remarques :

• Étant donnés un entier relatif a et un entier naturel non nul b, l'entier relatif q est le quotient de la division euclidienne de a par b si et seulement si $bq \leqslant a < b(q + 1)$.

• Étant donnés un entier relatif a et un entier naturel non nul b, b est un diviseur de a si et seulement si le reste de la division euclidienne de a par b est égal à 0.

Savoir-faire 4 Effectuer une division euclidienne

→ Exercice corrigé 40 p. 28
→ Exercices d'application 41 à 42 p. 28

Énoncé

Sachant que $1\,159 = 47 \times 24 + 31$, en déduire le quotient q et le reste r de la division euclidienne de :

a. 1 159 par 47 ;

b. 1 159 par 24 ;

c. –1 159 par 24.

Méthode

- Utiliser la définition de la division euclidienne.
- Si $a < 0$, écrire d'abord l'égalité de la division euclidienne de $-a$ par b.

Solution

a. $1\,159 = 47 \times 24 + 31$ et $0 \leqslant 31 < 47$, donc $q = 24$ et $r = 31$.

b. $31 > 24$, cette égalité ne correspond pas à une division euclidienne. On écrit $1\,159 = 24 \times 47 + 24 + 7$, d'où $1\,159 = 24 \times 48 + 7$ et $0 \leqslant 7 < 24$, donc $q = 48$ et $r = 7$.

c. De $1\,159 = 24 \times 48 + 7$, on déduit $-1\,159 = 24 \times (-48) - 7$, d'où $-1\,159 = 24 \times (-48) - 24 + 24 - 7$, soit $-1\,159 = 24 \times (-49) + 17$ et $0 \leqslant 17 < 24$, donc $q = -49$ et $r = 17$.

Savoir-faire 5 Des inconnues dans une division euclidienne

→ Exercice corrigé 48 p. 28
→ Exercices d'application 49 à 50 p. 28

Énoncé

a. La division euclidienne de 523 par un entier naturel non nul b a un quotient égal à 17. Déterminer les valeurs possibles de b et du reste r.

b. La division euclidienne de 256 par un entier naturel non nul b a un reste égal à 25, déterminer les valeurs possibles de b et du quotient q.

Méthode

Utiliser la définition sans oublier la condition sur le reste pour en déduire un encadrement de l'une des inconnues.

Solution

1. $523 = b \times 17 + r$ et $0 \leqslant r < b$ équivaut à $r = 523 - b \times 17$ et $0 \leqslant 523 - b \times 17 < b$.

$0 \leqslant 523 - b \times 17 < b$ équivaut à $\frac{523}{18} < b \leqslant \frac{523}{17}$ soit $b = 30$, $r = 523 - 30 \times 17 = 13$.

2. $256 = b \times q + 25$ et $0 \leqslant 25 < b$, d'où $b \times q = 231$ avec $b > 25$. q est un diviseur de 231 tel que $0 < q < \frac{231}{25}$ d'où $q = 1$ et $b = 231$ ou $q = 3$ et $b = 77$ ou $q = 7$ et $b = 33$.

Savoir-faire 6 Effectuer la division euclidienne de $a(n)$ par $b(n)$

→ Exercice corrigé 54 p. 28
→ Exercice d'application 55 p. 28

Énoncé

Soit $n \in \mathbb{N}^*$, effectuer la division euclidienne de a par b pour $a = 3n^2\ n$ et $b = n + 1$.

Méthode

Écrire $a(n)$ sous la forme $b(n)q(n) + r(n)$ et vérifier la condition sur le reste.

Solution

On fait une « division en ligne » : on essaie de mettre en facteur $n + 1$ dans $3n^2 + n$.

$3n^2 + n = (3n^2 + 3n) + (-2n - 2) + 2 = 3n(n + 1) - 2(n + 1) + 2 = (n + 1)(3n - 2) + 2$.

On vérifie la condition $0 \leqslant r < b$: $0 \leqslant 2 < n + 1$ qui équivaut à $n > 1$.

Donc si $n > 1$, $q = 3n - 2$ et $r = 2$ et pour $n = 1$, $4 = 2 \times 2 + 0$ donc $q = 2$ et $r = 0$.

2 Écriture d'un entier relatif

Propriété 6

Soit un entier naturel non nul b. Tout entier relatif n s'écrit de manière unique $n = bq + r$ avec $r = 0, 1, 2, \ldots$ ou $b - 1$ et où q est un entier relatif.

Exemple : Tout entier relatif a s'écrit de manière unique sous la forme $2k$ ou $2k + 1$ où k est un entier relatif.

C Congruences

1 Définition

Propriété 7

Soient a et b deux entiers relatifs et n un entier naturel non nul, a et b ont le même reste dans la division euclidienne par n si, et seulement si, $a - b$ est divisible par n.

Démonstration :

• Soient a et b des entiers relatifs ayant le même reste r dans la division euclidienne par n : il existe des entiers relatifs q, q' et r tels que : $a = nq + r$ et $b = nq' + r$, d'où $a - b = n(q - q')$ avec $q - q' \in \mathbb{Z}$, donc $a - b$ est un multiple de n.

• Réciproquement : soient a et b des entiers relatifs tels que $a - b$ est un multiple de n : $a - b = nk$ ($k \in \mathbb{Z}$), soit $b = a - nk$. On effectue la division euclidienne de a par n : il existe deux entiers relatifs q et r tels que $a = nq + r$ et $0 \leqslant r < n$. D'où $b = a - nk = nq + r - nk$, soit $b = n(q - k) + r$ et $0 \leqslant r < n$, donc le reste de la division euclidienne de b par n est aussi r.

Définition 3

Soient a et b deux entiers relatifs et n un entier naturel non nul.
Dire que a et b sont congrus modulo n signifie que a et b ont le même reste dans la division euclidienne par n, ce qui équivaut à dire que $a - b$ est un multiple de n.

Note :
Si a est congru à b modulo n, on note : $a \equiv b$ [n] ou $a \equiv b$ (n) ou encore $a \equiv b$ (mod n).

Exemples : • $21 = 4 \times 5 + 1$ et $25 = 4 \times 6 + 1$,
$-19 - (-5) = -14 = (-2) \times 7$ donc $-19 \equiv -5$ [7].

2 Conséquences

On déduit immédiatement de la définition les propriétés suivantes :

Propriété 8

Soient a un entier relatif et n un entier naturel non nul.
a est divisible par n si, et seulement si, $a \equiv 0$ [n].

Propriété 9

Soient a et r deux entiers relatifs et n un entier naturel non nul. r est le reste de la division euclidienne de a par n si, et seulement si, $a \equiv r$ [n] et $0 \leqslant r < n$.

Propriété 10

Soient a, b, c des entiers relatifs et n un entier naturel non nul.
• $a \equiv a$ [n] ; • si $a \equiv b$ [n], alors $b \equiv a$ [n] ; • si $a \equiv b$ [n] et $b \equiv c$ [n], alors $a \equiv c$ [n].

Savoir-faire 7 Prouver une divisibilité de $a(n)$ par b

→ Exercice corrigé 56 p. 28
→ Exercices d'application 57 à 61 p. 28

Énoncé

Démontrer que pour tout entier relatif n, $n(n^2 - 4)$ est divisible par 3.

Méthode

Méthode 1 : Faire une étude exhaustive suivant les restes de la division euclidienne de n par b.
Méthode 2 : Utiliser les congruence.

Solution

• **Méthode 1**

Il s'agit d'une divisibilité par 3, on fait une étude suivant les restes de la division euclidienne de n par 3 :
n s'écrit sous la forme $n = 3k$ ou $n = 3k + 1$ ou $n = 3k + 2$ ($k \in \mathbb{Z}$).
1er cas : si $n = 3k$, alors $n(n^2 - 4) = 3k(9k^2 - 4)$.
2ème cas : si $n = 3k + 1$, alors
$n(n^2 - 4) = (3k + 1)((3k + 1)^2 - 4) = (3k + 1)(9k^2 + 6k - 3) = 3(3k + 1)(3k^2 + 2k - 1)$.
3ème cas : si $n = 3k + 2$, alors
$n(n^2 - 4) = (3k + 2)((3k + 2)^2 - 4) = (3k + 1)(9k^2 + 12k) = 3(3k + 1)(3k^2 + 4k)$.
Pour tout $n \in \mathbb{Z}$, $n(n^2 - 4) = 3K$ avec $K \in \mathbb{Z}$ et donc $n(n^2 - 4)$ est divisible par 3.

• **Méthode 2**

Montrer que $n(n^2 - 4)$ est divisible par 3 revient à montrer $n(n^2 - 4) \equiv 0$ [3].
On sait que tout entier naturel n est congru modulo 3 à 0 ou 1 ou 2 :
– Si $n \equiv 0$ [3], alors par compatibilité avec la multiplication, $n(n^2 - 4) \equiv 0 \times (n^2 - 4)$ [3], soit $n(n^2 - 4) \equiv 0$ [3].
– Si $n \equiv 1$ [3], alors :
par compatibilité avec les puissances, $n^2 \equiv 1^2$ [3], soit $n^2 \equiv 1$ [3],
par compatibilité avec l'addition, $n^2 - 4 \equiv 1 - 4$ [3], d'où $n^2 - 4 \equiv 0$ [3],
et par compatibilité avec la multiplication, on obtient $n(n^2 - 4) \equiv 0$ [3].
– Si $n \equiv 2$ [3], alors on obtient de même, $n^2 \equiv 2^2$ [3], soit $n^2 \equiv 1$ [3], d'où $n(n^2 - 4) \equiv 0$ [3].
Pour tout $n \in \mathbb{Z}$, $n(n^2 - 4) \equiv 0$ [3], est donc $n(n^2 - 4)$ est divisible par 3.

Savoir-faire 8 Déterminer le reste de la division de a^n par b

→ Exercice corrigé 64 p. 29
→ Exercices d'application 65 à 68 p. 29

Énoncé

Déterminer les restes des divisions euclidiennes par 7 de :
a. 2^{213} ; **b.** 3^{215} ; **c.** 2012^{213}.

Méthode

a) et b) Chercher un entier p tel que a^p est congru à 1 ou –1 modulo 7, lorsque c'est possible.
c) Remplacer, d'abord, a par le reste r de la division euclidienne de a par b.

Solution

a. $2 \equiv 2$ [7] ; $2^2 \equiv 4$ [7] ; $2^3 \equiv 8$ [7], d'où $2^3 \equiv 1$ [7].
• $213 = 3 \times 71$, d'où $2^{213} = (2^3)^{71}$.
• Par compatibilité avec les puissances, $2^3 \equiv 1$ [7] implique $(2^3)^{71} \equiv 1^{71}$ [7].
• Donc $2^{213} \equiv 1$ [7] et $0 \leqslant 1 < 7$, le reste de la division euclidienne de 2^{213} par 7 est 1.
b. $3 \equiv 3$ [7] ; $3^2 = 9$, d'où $3^2 \equiv 2$ [7] ; $3^3 = 27$, d'où $3^3 \equiv -1$ [7].
• Or $215 = 3 \times 71 + 2$, d'où $3^{215} = (3^3)^{71} \times 3^2$.
• Par compatibilité avec les puissances, $3^3 \equiv -1$ [7] implique $(3^3)^{71} \equiv (-1)^{71}$ [7].
• Par compatibilité avec la multiplication, $(3^3)^{71} \equiv -1$ [7] et $3^2 \equiv 2$ [7] impliquent $(3^3)^{71} \times 3^2 \equiv (-1) \times 2$ [7].
• Donc $3^{215} \equiv -2$ [7], soit $3^{215} \equiv 5$ [7] et $0 \leqslant 5 < 7$, le reste de la division euclidienne de 2^{213} par 7 est 5.
c. $2012 = 7 \times 287 + 3$, donc $2012 \equiv 3$ [7] et $2012^{215} \equiv 3^{215}$ [7].
De **b.**, on déduit que le reste de la division euclidienne de 2012^{215} par 7 est 5.

3 Compatibilité avec les opérations

Propriété 11

Soient a, b, c, d des entiers relatifs et n un entier naturel non nul.

1. Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a + c \equiv b + d\ [n]$ et $a - c \equiv b - d\ [n]$.
2. Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $ac \equiv bd\ [n]$.
3. Pour tout entier naturel non nul p, si $a \equiv b\ [n]$, alors $a^p \equiv b^p\ [n]$,
4. Si $a \equiv b\ [n]$, alors $a + c \equiv b + c\ [n]$.
5. Si $a \equiv b\ [n]$, alors $a \times c \equiv b \times c\ [n]$.

REMARQUE : On ne peut pas « simplifier » une congruence : $16 \equiv 20\ [4]$, mais on n'a pas $8 \equiv 10\ [4]$.

DÉMONSTRATION : **1.** Démonstration de la compatibilité avec l'addition et la multiplication.

- $a \equiv b[n] \Leftrightarrow a - b = kn \quad (k \in \mathbb{Z})$ et $c \equiv d[n] \Leftrightarrow c - d = k'n \quad (k' \in \mathbb{Z})$.
- D'où $(a - b) + (c - d) = kn + k'n = (k + k')n$, soit $(a + c) - (b + d) = (k + k')n$, avec $k + k' \in \mathbb{Z}$, et donc $a + c \equiv b + d[n]$.
- D'où $a = b + kn$ et $c = d + k'n$ et $ac = (b + kn)(d + k'n) = bd + (kd + bk' + kk'n)n$, avec $kd + bk' + kk'n \in \mathbb{Z}$ et donc $ac \equiv bd[n]$.

2. Démonstration de la compatibilité avec l'élévation à une puissance.
On démontre cette propriété par récurrence :

- Par hypothèse $a \equiv b[n]$, donc $a^1 \equiv b^1[n]$, la propriété est vraie pour $p = 1$;
- On montre que si la propriété est vraie pour $p \geqslant 1$, alors elle est vraie pour $p + 1$.

Par hypothèse de récurrence : $a^p \equiv b^p[n]$ et par hypothèse $a \equiv b[n]$, par compatibilité avec la multiplication, on a : $a^p \times a \equiv b^p \times b[n]$, soit $a^{p+1} \equiv b^{p+1}[n]$, la propriété est donc vraie au rang $p + 1$;

- D'après le principe de récurrence, on en déduit que pour tout $p \in \mathbb{N}^*$: $a^p \equiv b^p[n]$.

4 Une propriété utile

Propriété 12

- Tout entier relatif a est congru à 0 ou 1 ou 2 ou... $n - 1$ modulo n.
- Soit $k \in \mathbb{Z}$, tout entier relatif a est congru à kn ou $kn + 1$ ou $kn + 2$ ou ... $kn + n - 1$ modulo n.

EXEMPLES : • Tout entier relatif est congru à 0 ou 1 ou 2 modulo 3.
• Tout entier relatif est aussi congru à 25 ou 26 ou 27 modulo 3 car ce sont trois nombres quelconques consécutifs.

REMARQUE : Afin de diminuer l'ordre de grandeur des calculs, il est intéressant de choisir n entiers consécutifs « répartis autour de 0 ». En particulier, si n est impair et s'écrit $n = 2m + 1$, on en déduit que tout entier relatif a est congru modulo n, à $-m$ ou $-m + 1$ ou... ou -2 ou -1 ou 0 ou 1 ou 2 ou ... ou $m - 1$ ou m.

EXEMPLES : • Tout entier relatif est congru à -2 ou -1 ou 0 ou 1 ou 2 ou 3 modulo 6.
• Tout entier relatif est congru à -3 ou -2 ou -1 ou 0 ou 1 ou 2 ou 3 modulo 7.

Savoir-faire 9 Utiliser les négatifs dans les congruences

→ Exercice corrigé 64 p. 29
→ Exercices d'application 65 à 68 p. 29

Énoncé

Montrer que $N = 341^{2011} + 695^{2011}$ est divisible par 17.

Méthode

- Utiliser les congruences.
- Ne pas oublier que, si $a \equiv r[n]$, alors $a \equiv r - n[n]$.
- Faire le bon choix pour simplifier les calculs.

Solution

- $342 = 17 \times 20 + 2$, donc $342 \equiv 2$ [17], et par compatibilité avec les puissances $342^{2011} \equiv 2^{2011}$ [17].
- De même $695 = 17 \times 40 + 15$, donc $695 \equiv 15$ [17] ; or $15 \equiv -2$ [17], d'où $695 \equiv -2$ [17] et par compatibilité avec les puissances, $695^{2011} \equiv (-2)^{2011}$ [17].
- Par compatibilité avec l'addition, on en déduit : $341^{2011} + 695^{2011} \equiv 2^{2011} + (-2)^{2011}$ [17].

Donc $N \equiv 0$ [17] et N est divisible par 17.

Savoir-faire 10 Résoudre dans $\mathbb{Z}$ « une équation modulo n »

→ Exercice corrigé 71 p. 29
→ Exercices d'application 72 à 73 p. 29

Énoncé

a. Déterminer l'ensemble E des entiers x tels que $x + 7 \equiv 3$ [8].
b. Déterminer l'ensemble F des entiers x tels que $3x \equiv 7$ [8].

Méthode

a. Utiliser la compatibilité avec l'addition.
b. Étudier les congruences modulo n du 1er membre suivant celles de x.

Solution

a. Si $x + 7 \equiv 3$ [8] alors $x + 7 - 7 \equiv 3 - 7$ [8], soit $x \equiv -4$ [8] soit $x \equiv 4$ [8].
Réciproquement, si $x \equiv 4$ [8], alors $x + 7 \equiv 11$ [8] soit $x + 7 \equiv 3$ [8].
E est donc l'ensemble des entiers de la forme $4 + 8k$, avec $k \in \mathbb{Z}$.
b. On fait un tableau des congruences modulo 8 de $3x$ suivant celles de x.

$x \equiv \ldots$ [8]	0	1	2	3	4	5	6	7
$3x \equiv \ldots$ [8]	0	3	6	1	4	7	2	5

On en déduit, par disjonction des cas que $3x \equiv 7$ [8] $\Leftrightarrow x \equiv 5$ [8].
F est donc l'ensemble des entiers de la forme $5 + 8k$, avec $k \in \mathbb{Z}$.

Savoir-faire 11 Résoudre une équation par les congruences

→ Exercice corrigé 74 p. 29
→ Exercice d'application 75 p. 29

Énoncé

On considère l'équation dans $\mathbb{Z}$,
(E) $x^2 - 3y^2 = 17$.
a. Montrer que si $(x ; y)$ est solution de (E), alors $x^2 \equiv 2$ [3].
b. Déterminer les congruences modulo 3 de x^2 suivant les congruences modulo 3 de x.
c. Résoudre alors l'équation (E).

Méthode

Se ramener à « une équation modulo n » plus simple. Montrer alors que celle-ci n'a pas de solution.

Solution

a. • $-3 \equiv 0$ [3], d'où $-3y^2 \equiv 0$, d'où $x^2 - 3y^2 \equiv x^2$ [3]. Or $17 \equiv 2$ [3]
• Donc si $(x ; y)$ est solution de (E), alors $x^2 \equiv 2$ [3].
b. Si $x \equiv 0$ [3], alors $x^2 \equiv 0$ [3] ; si $x \equiv 1$ [3], alors $x^2 \equiv 1$ [3] ; si $x \equiv 2$ [3], alors $x^2 \equiv 1$ [3].
c. On raisonne par l'absurde : si $(x ; y)$ est solution de (E), alors $x^2 \equiv 2$ [3], ce qui est faux d'après **b**. Donc l'équation (E) n'a pas de solution dans $\mathbb{Z}$.

TP Algorithmique 1 Deux algorithmes



1. Lire A (entier non nul)
Pour I allant de 1 à A faire
  Si partie fractionnaire de $\frac{A}{I}$ est 0 alors
    afficher I
  FinSi
FinPour

```
PROGRAM:A
:Input A
:For(I,1,A)
:If partDéc(A/I)
=0
:Disp I
:End
:
```

2. Lire A et B (entier non nul)
Q = 0
R = A
TantQue R ⩾ B faire
  Q = Q + 1
  R = R - B
FinTantque
Afficher Q et R

```
PROGRAM:DI
:Prompt A,B
:0→Q
:A→R
:While R≥B
:Q+1→Q
:R-B→R
:End
:Disp "Q",Q,"R",
R
```

Que font ces algorithmes ? Peut-on les améliorer ?

TP Algorithmique 2 Problèmes de numération



Objectif :
- *Découvrir les principes de numération en base et leur application à la base 10 et la base 2.*

Un entier naturel peut être écrit sous différentes formes. De nos jours, on utilise dans le langage courant la numération décimale de position et pour le langage informatique, l'écriture binaire.

1 Principe de numération

Soient b un entier naturel avec $b > 1$ et a un entier naturel.

a. i. On sait que $\lim b^n = +\infty$. En déduire qu'il existe un entier k_0 tel que $b^{k_0} > a$.
ii. Soit M l'ensemble des entiers naturels k tels que $b^k > a$. Montrer que M est une partie non vide. En déduire qu'elle admet un plus petit élément noté $n + 1$, qui vérifie donc $b^n \leqslant a < b^{n+1}$.
iii. Montrer qu'il existe deux entiers a_n et r_n tels que $a = a_n b^n + r_n$ et $0 \leqslant r_n < b^n$ et $0 \leqslant a_n < b$.
iv. Montrer qu'on définit ainsi une suite (a_n) telle que
$a = a_n b^n + a_{n-1} b^{n-1} + \ldots\ldots + a_1 b^1 + a_0 b^0$, avec pour tout i, $0 \leqslant a_i < b$.

b. $a = a_n b^n + a_{n-1} b^{n-1} + \ldots\ldots + a_1 b^1 + a_0 b^0$, avec pour tout i, $0 \leqslant a_i < b$.
i. Quel est le reste dans la division de a par b ?
ii. Quel est le quotient ? On le note q_0. Montrer que $q_0 < a$.
iii. Reprendre les questions précédentes en remplaçant a par q_0. On notera q_1 le nouveau quotient.
iv. On recommence. Montrer que l'on définit ainsi une famille strictement décroissante d'entiers q_i telle que chaque a_i est le reste dans la division de q_{i-1} par b avec $i < n$ et $q_n = a_n$.

c. Soient a et b donnés.
i. Indiquer comment construire les a_i tels que $a = a_n b^n + a_{n-1} b^{n-1} + \ldots\ldots + a_1 b^1 + a_0 b^0$. On dit que l'écriture en base b de a est $a_n a_{n-1} \ldots\ldots a_1 a_0$. Les a_i sont alors appelés chiffres. Justifier qu'il y a b chiffres possibles.
ii. Écrire un algorithme permettant d'écrire un nombre en base b.
iii. Le faire tourner sur la calculatrice pour trouver l'écriture en base 10 de 7^8.
iv. Vérifier la validité de l'algorithme en tapant 7^8 sur la calculatrice.

2 Écriture décimale et écriture binaire

a. i. N a pour écriture 1341 en base 10. L'écrire sous la forme $a_n10^n + a_{n-1}10^{n-1} + \ldots\ldots + a_1 10^1 + a_0 10^0$.

ii. Encadrer N entre deux puissances de 10 consécutives.

b. i. Combien de chiffres sont utilisés pour écrire un nombre en base 2 ?

ii. Soit A un nombre ayant n chiffres 1 en écriture binaire. Montrer qu'on peut l'écrire à l'aide d'une seule puissance de 2.

c. On pose $A = 1101$ et $B = 1011$ écrits en base 2.

i. Effectuer en base 2 les opérations $A + B$ et AB en complétant et utilisant les tables suivantes

ii. Écrire A et B en base 10 et vérifier les résultats obtenus en a.

+	0	1
0		
1		10

×	0	1
0		
1		1

TP TICE 1 Critères de divisibilité

Objectifs :

- *Utiliser un tableur pour faire des conjectures.*
- *Énoncer et démontrer des critères de divisibilité.*

Le nombre 201 527 120 112 011 925 est-il divisible par 3 (Q) ?

On utilisera le résultat suivant :

si l'entier naturel a s'écrit $a = \overline{a_n a_{n-1} \ldots a_1 a_0}$, cela signifie :

$a = a_n 10^n + a_{n-1}10^{n-1} + \ldots\ldots + a_1 10^1 + a_0 10^0$.



Un peu d'histoire...

« Rien de plus connu en arithmétique que la proposition d'après laquelle un multiple quelconque de 9 se compose de chiffres dont la somme est elle-même un multiple de 9... Dans ce petit traité, je justifierai le caractère de divisibilité par 9 et plusieurs autres analogues. »

B. Pascal 1654

1 Critères de divisibilité par 9 et 3

a. Justifier les affirmations $10 \equiv 1$ [9] et, pour tout entier naturel n, $10^n \equiv 1$ [9].

b. Montrer que tout entier naturel est congru à la somme de ses chiffres modulo 9.

c. Retrouver le critère de divisibilité par 9.

d. Énoncer et démontrer le critère de divisibilité par 3. Répondre à (Q).

2 Critères de divisibilité par 5 et 2

a. Montrer que tout entier naturel a s'écrit $a = 10q + u$, avec $0 \leqslant u < 10$, puis en déduire que $a \equiv u$ [2] et $a \equiv u$ [5].

b. En déduire les critères de divisibilité par 2 ou 5.

3 Critères de divisibilité par 11

a. Établir que, pour tout naturel k, $10^k \equiv (-1)^k$ [11].

b. En déduire que $a \equiv (a_0 + a_2 + \ldots\ldots) - (a_1 + a_3 + \ldots)$ [11].

c. En déduire le critère de divisibilité par 11.

4 Critère de divisibilité par 7

n	0	1	2	3	4	5	6	7	8	9
10^n Mod 7	1	3								

a. Sur un tableur, créer le tableau donnant les restes dans la division par 7 de 10^n, pour tout entier naturel n.

b. Que constate-t-on ?

c. Montrer que si $n = 6q + r$, $10^n = 10^r$ [7].

d. Le nombre 798 342 752 est-il divisible par 7 ? Et le nombre 689 243 157 ?

e. Énoncer un critère de divisibilité par 7 et élaborer un algorithme.

Aide

On utilisera la fonction MOD : MOD(a ; b) renvoie le reste de la division euclidienne de a par b.

5 Divisibilité par 13 ?

Sur le même modèle, élaborer un critère de divisibilité par 13.

TP TICE 2 Restes modulo p

Objectif :
- *Constater, à l'aide d'un tableur, la périodicité des restes.*

Le but de cet exercice est d'étudier les restes modulo p (p entier strictement supérieur à 1) des suites (u_n), $n \in \mathbb{N}$, définies par : $u_n = an + b$, a et b étant deux entiers naturels donnés.

1 Construire une feuille de calcul donnant les restes modulo 20 des 20 premiers termes de la suite (u_n), $n \in \mathbb{N}$, définie par $u_n = 12n + 5$.

2 Adapter la feuille de calcul de façon à obtenir les restes modulo p des 20 premiers termes de la suite définie par $u_n = an + b$, $n \in \mathbb{N}$, de telle manière qu'on puisse modifier les valeurs de a, b et p. Notez sur votre feuille les restes obtenus dans les cas particuliers suivants :

a. $p = 20$ et $u_n = 5n - 3$;

b. $p = 7$ et $u_n = 5n - 3$.

Quelle conjecture peut-on formuler quant aux suites formées par ces restes ?

3 Démonstration de la conjecture

a. Montrer que, parmi les nombres u_0, u_1, ..., u_p, il existe deux nombres ayant le même reste dans la division euclidienne par p, pour p entier naturel non nul.

Aide

On pourra utiliser le principe de Dirichlet, appelé parfois principe des tiroirs.
On veut ranger des objets dans des tiroirs. Si on a plus d'objets que de tiroirs, il existe un tiroir contenant au moins deux objets.

b. Soient n_0 et $n_0 + T$ les rangs de ces deux nombres ($T \neq 0$).
Montrer que aT est un multiple de p.

c. En déduire que pour tout entier naturel k, u_{T+k} et u_k ont le même reste dans la division euclidienne par p.

TP TICE 3 Coder et décoder avec un chiffrement affine

Objectif :
- *Utiliser un tableur pour coder et décoder avec un chiffrement affine.*

1 Coder un message de façon automatique à l'aide d'un tableur

On considère le chiffrement affine de clé $(a ; b) = (17 ; 5)$. (voir activité 6)
On note E = {0, 1, 2, ..., 25}. A toute lettre L de rang x ($x \in$ E), on associe la lettre L' de rang y tel que $y \equiv 17x + 5$ [26], $y \in$ EE.
On veut coder à l'aide d'un tableur cette citation de Jules-Henri Poincaré : « C'est par la logique que nous prouvons, c'est par l'intuition que nous inventons ». On commencera par coder le mot « POINCARE ».
On utilise le code ASCII pour associer (par CODE) à chaque lettre L son rang x ou à chaque rang y la lettre correspondante L' (par CAR).

Commentaire

En informatique, le code ASCII associe à chaque caractère un code numérique qui est un entier compris entre 0 et 255 ; c'est la fonction CODE du tableur et sa fonction réciproque est la fonction CAR. Les majuscules de l'alphabet ont un code ASCII compris entre 65 et 91 [code (A) = 65, ..., code (Z) = 91].

Pour simplifier, on écrira le message sans la ponctuation et sans les blancs.

a. i. Écrire POINCARE dans les cellules A1 à H1.
ii. Quelle formule faut-il entrer en A2 et recopier vers le bas pour chiffrer le message ?
iii. Coder alors le message chiffré dans les cellules A3 à H3 à l'aide de la fonction MOD
iv. Quelle formule faut-il entrer en A4 et recopier pour obtenir le message codé en lettres ?
v. Quel est le message codé ?
b. Coder maintenant la citation de Poincaré.

2 Décodage automatique à l'aide d'un tableur d'un message codé par un chiffrement affine connu

a. Détermination de la fonction de décodage du codage précédent
Le problème est, connaissant $y \equiv 17x + 5$ [26], $y \in E$, de trouver l'expression de x en fonction de y.
i. Construire à l'aide de la fonction MOD d'un tableur la table de multiplication modulo 26.
ii. En déduire l'entier naturel u compris entre 0 et 25 tel que $17u \equiv 1$ [26].
iii. En déduire que si $y \equiv 17x + 5$ [26], $y \in E$, alors $x \equiv u(y - 5)$ [26], $x \in E$.
Énoncer et démontrer la réciproque.
iv. En déduire la fonction de décodage.



b. On souhaite décoder le message suivant qui est une citation d'un philosophe mathématicien du XVIII^e siècle.
Son nom codé est : NJSEJINVQ.
La citation codée est :
IVCVQ VIKFQ UVJIL VNJBB VLSHQ LKVAJ HISVZ
FAAKL RHVIR FHGNU JZVZH
ZHVKK VZNVZ QAIJA JZVIE VIVQI FSNUV IKVZI
FNLSV ZEHSF IWIVZ JHZAI
VQVGQ VRHVK KVZSV AJIQV SQAJL SQEVM IHLQZ
Commencer par décoder le nom de ce philosophe, puis décoder la citation en suivant les indications :
i. Écrire le message à décoder en ligne 6.
ii. Chiffrer ce message à décoder en ligne 7, puis le décoder en utilisant la fonction décodage, à la ligne 8.
iii. En déduire le message initial.

3 Recherche de la clé d'un chiffrement affine

On intercepte un message codé par un chiffrement affine du type $y \equiv ax + b$ [26].
Pour déterminer a et b inconnus, on procède par cryptanalyse :
le cryptanaliste sait que les lettres les plus fréquentes sont, dans l'ordre, E puis A.
Dans le texte codé, on voit que les lettres les plus fréquentes sont W puis U. Cela signifie donc que E est codée par W et A par U.

a. Montrer qu'on doit donc résoudre le système $\begin{cases} 4a + b \equiv 22\,[26] \\ 0a + b \equiv 20\,[26] \end{cases}$.

b. En déduire $b \equiv 20$ [26] , puis $4a \equiv 2$ [26]. À l'aide de la table de multiplication modulo 26 du **2.a.i.**, montrer qu'il existe une seule valeur de a comprise entre 0 et 25 vérifiant cette condition.

c. En déduire la fonction de codage.

Exercices Appliquer le cours

Maîtriser le cours

1 $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Que signifie « b divise a » ? Donner des expressions synonymes.

2 $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$. Démontrer la propriété : si a est multiple de b et b est multiple de c, alors a est multiple de c.

3 $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ et $c \in \mathbb{Z}$. Démontrer la propriété : si a divise b et a divise c, alors, pour tous les entiers relatifs u et v, a divise $bu + cv$.

4 $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Donner la définition de la division euclidienne de a par b.

5 $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. On admet l'existence d'un couple $(q ; r)$ d'entiers naturels tel que $a = bq + r$ et $0 \leqslant r < b$. Démontrer l'unicité de ce couple.

6 $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Que signifie « a est congru à b modulo n » ? Donner une propriété équivalente.

7 $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$ et $d \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Démontrer la propriété : $a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow a + c \equiv b + d\ [n]$.

8 $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$ et $d \in \mathbb{Z}$, $n \in \mathbb{N}^*$.
a. Démontrer la propriété :
$a \equiv b\ [n]$ et $c \equiv d\ [n] \Rightarrow ac \equiv bd\ [n]$.
b. En déduire la propriété :
si $a \equiv b\ [n]$, alors, pour tout $k \in \mathbb{N}^*$, $a^k \equiv b^k\ [n]$.

Divisibilité

9 **Vrai ou faux (Justifier)**
a, b et c sont des entiers.
a. Si a divise b et b divise a, alors $a = b$.
b. Si a divise b, alors b divise a.
c. Si a divise b, alors a divise bc.
d. Si a divise bc, alors a divise b ou c.
e. Si a divise b, alors a divise $a + b$.
f. Si a divise $a + b$, alors a divise b.
g. Si a divise b et c, alors a divise $b + c$.
h. Si a divise $b + c$, alors a divise b et c.
i. Si a et b divisent c, alors ab divise c.
j. Si a divise b, alors a^2 divise b^2.

Division euclidienne

10 **Vrai ou faux (Justifier)**
Vérifier l'égalité : $287 = 18 \times 15 + 17$ et en déduire les réponses aux questions **a.**, **b.**, **c.** et **d.**
a. Dans la division euclidienne de 287 par 15, le quotient est égal à 18.
b. Dans la division euclidienne de 287 par 18, le reste est égal à 17.
c. Dans la division euclidienne de –287 par 18, le quotient est égal à –15 et le reste est égal à –17.
d. Dans la division euclidienne de –287 par 18, le quotient est égal à –16 et le reste est égal à 1.
e. Pour tout entier naturel n, le reste de la division euclidienne de $11n^3 + 9$ par n est 9.
f. Dans la division euclidienne de deux entiers non nuls, le quotient et le reste sont augmentés de 1 si on ajoute le diviseur au dividende.
Dans la suite, a est un entier relatif et b un entier naturel non nul.
g. Le reste de la division euclidienne de a par b est nul si, et seulement si, a est un multiple de b.
h. Si 15 est le reste de la division euclidienne de a par b, alors, –15 est le reste de la division euclidienne de $-a$ par b.
i. Si r est le reste de la division euclidienne de a par b alors $r + 1$ est le reste de la division euclidienne de $a + 1$ par b.
j. Si a et b vérifient $a = 6b + 5$, alors 5 est le reste de la division euclidienne de a par 6 et de a par b.

11 Soient a un entier relatif et b un entier naturel non nul. Que fait cet algorithme ?

```
Entrer a,b;
q=E(a/b);
r=a-bq;
Afficher q,r.
```

Congruences

12 **Vrai ou faux**
a. Tout entier relatif est congru modulo 5 à l'un des nombres 1, 2, 3 ou 4.
b. Si un entier naturel n est congru modulo 5 à r, alors r est le reste de la division euclidienne de n par 5.
c. n est un multiple de 14 si et seulement si $n \equiv 0\ [14]$.
d. $257 \equiv 10\ [9]$ et $244 \equiv 205\ [13]$.
e. De l'égalité $751 = 17 \times 43 + 20$, on déduit $751 \equiv 20\ [17]$ et $751 \equiv 20\ [43]$.
f. Pour tout entier naturel n, 18 divise $19^n - 1$.
g. Pour tout entier naturel n, $4^n + 2^n \equiv 0\ [3]$.
Dans la suite, a et b sont des entiers relatifs et n un entier naturel non nul.
h. Si $a \equiv 3\ [7]$ et $b \equiv 5\ [7]$ alors $3a + 8b \equiv 0\ [7]$.
i. Si $2a \equiv 2b\ [n]$ alors $a \equiv b\ [n]$.
j. Si $a \equiv b\ [6]$ alors $a \equiv b\ [3]$.
k. Si $2a \equiv 2b\ [2n]$, alors $a \equiv b\ [n]$.

Appliquer les capacités attendues

Divisibilité

Utiliser la définition de la divisibilité

13 **a.** Déterminer tous les diviseurs entiers relatifs de 21.
b. Déterminer tous les diviseurs entiers naturels de 270.

14 **a.** Déterminer le nombre de multiples de 17 compris entre 2 000 et 3 000.
b. Déterminer le nombre de multiples de 41 compris entre –1 000 et 2 000.

15 **a.** Déterminer les entiers relatifs n tels que 11 divise $n + 5$.
b. Déterminer les entiers relatifs n tels que $n + 5$ divise 11.

16 Déterminer les entiers relatifs n tels que $2n + 3$ divise 10.

17 Démontrer que la somme de deux entiers de même parité est paire.

18 Démontrer que la somme de deux entiers impairs consécutifs est un multiple de 4.

Utiliser les propriétés [savoir-faire 1 p. 15]

19 Déterminer les entiers relatifs n tels que $n - 4$ divise $n + 7$.

20 Déterminer les entiers relatifs n tels que $2n - 5$ divise $n + 3$.

21 Déterminer les entiers relatifs n tels que $n - 3$ divise $2n + 12$.

22 Déterminer les entiers relatifs n tels que $3n + 7$ divise $5n + 15$.

23 n est un entier naturel. Montrer que si a divise $15n + 2$ et $10n + 7$ alors a divise 17.

24 n est un entier naturel. Montrer que les seuls diviseurs positifs de $5n + 29$ et $2n + 11$ sont 1 et 3.

25 **a.** Vérifier que $n^2 - 5n + 11 = (n - 2)(n - 3) + 5$.
b. Déterminer les entiers naturels non nuls n tels que $n - 2$ divise $n^2 - 5n + 11$.

Utiliser la récurrence [savoir-faire 2 p. 15]

26 Montrer par récurrence que, pour tout entier naturel n, $3^{2n} - 2^n$ est divisible par 7.

27 Montrer par récurrence que, pour tout entier naturel n, $5^{2n} + 3$ est divisible par 4.

28 n est un entier naturel non nul.
a. vérifier que pour tous les réels x et a :
$x^n - a^n = (x - a)(x^{n-1} + x^{n-2}a + \ldots + xa^{n-2} + a^{n-1})$.
b. En déduire que $19^n - 12^n$ est divisible par 7.
c. Démontrer ensuite ce résultat par récurrence.

29 Montrer par récurrence que pour tout entier naturel n, $5^{2n} - 2^{3n}$ est divisible par 17.

30 Montrer par récurrence que, pour tout entier naturel n, 6 divise $5n^3 + n$.

Résoudre une équation dans les entiers [savoir-faire 3 p. 15]

31 Déterminer les couples $(x ; y)$ d'entiers naturels tels que $(x-3)(y+5) = 6$.

32 Déterminer les couples $(x ; y)$ d'entiers relatifs tels que $x^2 = y^2 + 13$.

33 Déterminer les couples $(x ; y)$ d'entiers naturels tels que $4x^2 = y^2 + 15$.

34 Déterminer les couples $(x ; y)$ d'entiers relatifs tels que $3xy - y^2 = 25$.

35 Déterminer les entiers naturels x tels que $36 + x^2$ soit un carré.

D'autres équations [activité 1 p. 10]

36 Déterminer les couples $(x ; y)$ d'entiers relatifs tels que $3x^2 + y^2 = 21$.

37 Résoudre dans $\mathbb{Z}$ l'équation $3x + 24y = 14$.

Déterminer n pour que $\frac{a(n)}{b(n)}$ soit un entier

38 Déterminer les entiers naturels n tels que $\frac{5n+7}{n+2}$ soit un entier.

39 n est un entier relatif.
a. Vérifier que $2n^2 - n - 8 = (n + 4)(2n - 9) + 28$.
b. Montrer que $\frac{2n^2 - n - 8}{n+4}$ est un entier relatif si et seulement si $\frac{28}{n+4}$ est un entier relatif.
c. En déduire les valeurs de n telles que $\frac{2n^2 - n - 8}{n+4}$ soit un entier relatif.

Division euclidienne

Effectuer une division euclidienne
[savoir-faire 4 p. 17]

40 Écrire la division euclidienne de 363 par 10.
En déduire la division euclidienne de 363 par 8.
En déduire la division euclidienne de –363 par 10.

41 Écrire la division euclidienne de 121 par 23.
En déduire la division euclidienne de –121 par 23.

42 On sait que dans la division euclidienne de l'entier naturel a par 225, le reste est égal à 136. Quel est le reste de la division euclidienne de a :
a. par 75 ? **b.** par 45 ? **c.** par 9 ?

Savoir utiliser la définition de la division euclidienne [définition 2 p. 16]

43 Trouver tous les entiers naturels qui, divisés par 7, donnent un quotient égal à 4 fois le reste.

44 Trouver un entier naturel qui, divisé par 13, donne pour reste 9 et, divisé par 15, donne le même quotient et pour reste 1.

45 La somme de deux entiers naturels a et b est égale à 324 et la division euclidienne de a par b donne 2 pour quotient et 57 pour reste.
Déterminer a et b.

46 La différence de deux entiers naturels a et b est égale à 779 et la division euclidienne de a par b donne 11 pour quotient et 49 pour reste.
Déterminer a et b.

47 Dans la division euclidienne de l'entier naturel a par 11, le reste est égal à 8 et dans la division euclidienne de l'entier naturel b par 11, le reste est égal à 3.
Donner le reste de la division euclidienne :
a. de $a + b$ par 11 ; **b.** de a^2 par 11.

Des inconnues dans une division euclidienne
[savoir-faire 5 p. 17]

48 Dans la division euclidienne de 838 par l'entier naturel b le quotient est 31 et le reste est r.
a. Prouver que $31b \leqslant 838 < 32b$.
b. En déduire b et r.

49 Dans la division euclidienne de deux entiers naturels, le dividende est 85 et le reste est 3. Donner toutes les valeurs possibles du diviseur et du quotient.

50 Trouver une division euclidienne dont le quotient est 100, le reste 13 et où le dividende est inférieur à 900.

Appliquer la division euclidienne

51 Évariste roule sur un circuit fermé sur lequel sont placés dans l'ordre et dans le sens de parcours direct 8 points A_0, A_1, ..., A_7. Il part de A_0 et il met 10 minutes pour aller de A_0 à A_1, de A_1 à A_2, etc. Il roule ainsi pendant 7 h 40 min. En quel point se trouve-t-il ?

52 Effectuer la division euclidienne de 2843 par 12. En déduire comment placer l'angle de mesure $\frac{2\,843}{6}\pi$ sur le cercle trigonométrique.

53 En utilisant une division euclidienne, donner la mesure principale de $-\frac{3\,749}{4}\pi$.

Effectuer la division euclidienne de $a(n)$ par $b(n)$ [savoir-faire 6 p. 17]

54 n est un entier naturel.
Déterminer selon les valeurs de n le reste de la division euclidienne de $4n + 27$ par $n + 5$.

55 n est un entier naturel. Déterminer selon les valeurs de n le reste de la division euclidienne de $9n + 17$ par $2n + 3$.

Prouver une divisibilité [savoir-faire 7 p. 19]

56 **a.** Montrer que, pour tout entier naturel n, $n(n + 1)$ est un multiple de 2.
b. Montrer que, pour tout entier naturel n, $n(n^2 - 1)$ est un multiple de 3.

57 Montrer que pour tout entier naturel n, $n(n + 5)(n + 7)$ est un multiple de 3.

58 n est un entier naturel. $n(n + 5)(n + 7)$ est-il un multiple de 2 ? de 4 ?

59 n désigne un entier naturel.
a. Pourquoi tout entier naturel peut-il s'écrire $5k$, $5k + 1$, $5k + 2$, $5k + 3$ ou $5k + 4$, avec $k \in \mathbb{N}$?
b. Déterminer les entiers n tels que $n^2 - 3n + 6$ soit divisible par 5.

60 Montrer que tout entier naturel n a un carré de la forme $5q$ ou $5q + 1$ ou $5q - 1$ où q est un entier naturel.

61 Montrer qu'un nombre impair somme de deux carrés s'écrit sous la forme $4k + 1$.

Congruences

Simplifier des congruences [définition 3 p. 18]

62 Pour chaque valeur de a, déterminer un entier b tel que $b \equiv a$ [11] et $0 \leqslant b < 11$.

a. $a = 37$. **b.** $a = 186$. **c.** $a = -7$.
d. $a = 5002$. **e.** $a = -4002$.

63 Pour chaque valeur de a, déterminer un entier b tel que $b \equiv a$ [7] et $-3 \leqslant b \leqslant 3$.

a. $a = 13$. **b.** $a = 19$. **c.** $a = 64$.
d. $a = 88$. **e.** $a = -6$. **f.** $a = -4$.

Calculer un reste avec des congruences [savoir-faire 8 p. 19 et 9 p. 21]

64 En utilisant les congruences, déterminer le reste dans la division euclidienne par 7 des nombres :
$421^{120} \times 99^{15}$ et $93^{120} - 44^{120}$.

65 Montrer, sans calculatrice et sans calcul, que :
a. $16^{31} - 2^{31} \equiv 0$ [14]. **b.** $13^{20} - 9^{20} \equiv 0$ [11].

66 On suppose que $a \equiv 3$ [5] et $b \equiv 4$ [5]. Déterminer le reste de la division euclidienne $7a^2 + 4b^2$ par 5.

67 **a.** Déterminer le reste de la division euclidienne de 2012^{2011} par 5.
b. Déterminer le reste de la division euclidienne de 2012^{2011} par 7.

68 **a.** Démontrer que $7^2 \equiv -1$ [5].
b. En déduire que $7^4 \equiv 1$ [5].
c. En déduire que, pour tout entier naturel k, $7^{4k} \equiv 1$ [5].
d. En déduire que $7^{4k+1} \equiv 2$ [5], $7^{4k+2} \equiv -1$ [5] et $7^{4k+3} \equiv -2$ [5].
e. En déduire les différents restes possibles de la division euclidienne de 7^n par 5.

Déterminer un reste en fonction d'un autre reste [propriété 12 p. 20]

69 **a.** Expliquer pourquoi tout entier naturel x est congru modulo 5 à -2 ou -1 ou 0 ou 1 ou 2.
b. En déduire les congruences correspondantes de x^2 modulo 5.
c. En déduire les congruences correspondantes de x^4 modulo 5.
On pourra présenter ces résultats dans un tableau :

x mod 5	-2	-1	0	1	2
x^2 mod 5					
x^4 mod 5					

d. En déduire les différents restes possibles de la division euclidienne de x^4 par 5.

70 **a.** Déterminer, suivant les congruences modulo 5 de l'entier naturel n, les congruences modulo 5 de $n^2 - 3n + 6$.
b. En déduire les entiers naturels n tels que $n^2 - 3n + 6$ soit divisible par 5.

Résoudre dans $\mathbb{Z}$ une équation modulo n [savoir-faire 10 p. 21]

71 Résoudre dans $\mathbb{Z}$:

1. a. $\begin{cases} x \equiv -3[7] \\ 0 < x < 20 \end{cases}$. **b.** $\begin{cases} x + 3 \equiv -1[7] \\ 100 < x < 120 \end{cases}$.

2. a. $x - 48 \equiv 27$ [11]. **b.** $5x + 18 \equiv 4x - 29$ [13].

72 On souhaite résoudre dans $\mathbb{Z}$ l'équation $4x \equiv 6$ [7].
a. On travaille par disjonction des cas : on étudie suivant les congruences modulo 7 de x, les congruences de $4x$ modulo 7.
On résume les résultats dans un tableau :

x mod 7	0	1	2	3	4	5	6
$4x$ mod 7							

b. En déduire les solutions.

73 Résoudre dans $\mathbb{Z}$:

1. a. $7x \equiv 3$ [11]. **b.** $7x \equiv 3$ [10].
c. $5x \equiv 3$ [10]. **d.** $5x \equiv 0$ [10].

2. a. $5x + 25 \equiv 56$ [7]. **b.** $8x - 23 \equiv 5x - 45$ [17].

Résoudre une équation avec les congruences [savoir-faire 11 p. 21]

74 On considère l'équation dans $\mathbb{Z}$: $2x^2 + 3y^2 = 16$ (E).
a. Montrer que si un couple d'entiers relatifs (x, y) est solution de l'équation (E), alors $2x^2 \equiv 1$ [3].
b. Déterminer les restes de la division de $2x^2$ par 3 et conclure.

75 On considère l'équation dans $\mathbb{Z}$: $3x^2 + 5y^2 = 16$ (E).
a. Montrer que si un couple d'entiers relatifs (x, y) est solution de l'équation (E), alors $3x^2 \equiv 1$ [5].
b. Déterminer les restes de la division de $3x^2$ par 5 et conclure.

Jouer avec les congruences

76 Compléter les tables d'addition et de multiplication modulo 4 :

+	0	1	2	3
0				
1				
2				
3				

×	0	1	2	3
0				
1				
2				
3				

77 Même exercice modulo 5.

Divisibilité

78 **a.** Montrer que si n est impair, 8 divise $n^2 - 1$
b. Montrer que si n est pair, n^2 est multiple de 4.
c. En déduire que n pair si et seulement si n^2 est pair.

79 On considère l'équation (E) : $x^2 - Sx + 56 = 0$ où S est un entier naturel
a. Montrer que si (E) a une solution entière n, alors n divise 56.
b. Montrer que si n est solution de (E), $S - n$ l'est aussi.
c. Déterminer les valeurs de S pour lesquelles (E) admet 2 solutions dans $\mathbb{N}$.

80 On considère l'équation (E) : $x^3 + x^2 + bx + c = 0$ où a, b, c sont des entiers relatifs.
a. Montrer que si l'entier a est une solution de (E), alors a divise c.
b. L'équation $x^3 + 3x + 3 = 0$ a-t-elle des solutions entières ?
c. Et l'équation $x^3 - 15x - 4 = 0$?

81 **a.** Déterminer tous les diviseurs de 56.
b. Soit n un entier naturel ; on pose $a = 2n + 70$ et $b = n + 7$. Quelle valeur doit prendre n pour que b soit diviseur de a ?

82 On cherche pour quelles valeurs de l'entier naturel n la fraction $\frac{n+8}{2n-5}$ est un entier relatif.
a. Condition nécessaire : on suppose que n est tel qu'il existe un entier relatif k tel que $\frac{n+8}{2n-5} = k$
Montrer alors que $2n - 5$ divise $2n + 16$.
En déduire que $2n - 5$ divise 21. Trouver alors l'ensemble E des valeurs possibles pour n.
b. Condition suffisante.
Toutes les valeurs de E conviennent-elles ?

83 Vérifier que $(n + 2)^3 = n^2(n + 6) + 12n + 8$.
Pour quelles valeurs de n le reste dans la division de $(n + 2)^3$ par n^2 est-il $12n + 8$?

84 On considère l'équation (E) d'inconnues (x, y) entiers naturels : (E) $x^2 - 2y^2 = 1$.
Soit (x, y) un couple solution. Montrer que :
- x est impair et y est pair ;
- x et y n'ont aucun diviseur commun ;
- $(3x + 4y, 2x + 3y)$ est encore un couple solution.

Déterminer alors un couple d'entiers supérieurs à 1 000 solution.

85 Le nombre n désigne un entier naturel.
a. Démontrer que $n^2 + 5n + 4$ et $n^2 + 3n + 2$ sont divisibles par $n + 1$.
b. Déterminer l'ensemble des valeurs de n pour lesquelles $3n^2 + 15n + 19$ est divisible par $n + 1$.
c. En déduire que, quelque soit n, $3n^2 + 15n + 19$ n'est pas divisible par $n^2 + 3n + 2$.

Division euclidienne

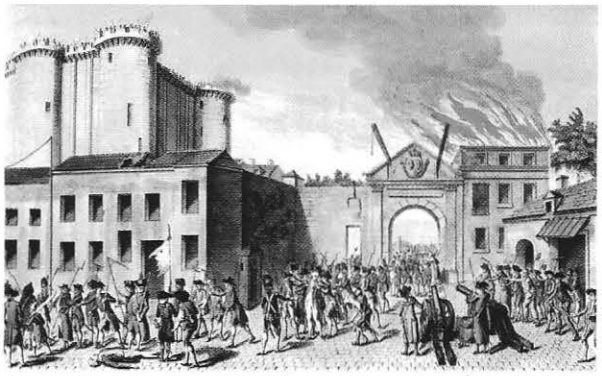
86 Si on divise a par 5, le reste est 3. Mais si on divise a par 25, quel peut être le reste ?

87 Soient a et b deux entiers naturels tels que $0 < b^2 < a$. Dans la division de $-a$ par b, le quotient est q et le reste est r.
a. Que sont les quotient et reste dans la division de a par q ?
b. Que se passe-t-il si $a < b^2$?

88 Dans la division euclidienne de a par b, le quotient et le reste sont les mêmes que dans la division de $a + 28$ par $b + 7$. Quel est le quotient ?

89 Soient a un entier positif et b un entier strictement positif. On sait que dans la division de a par b, le quotient est q, le reste est r. Que peut-on dire sur le quotient et le reste dans la division de :
- a par b ?
- $2a$ par b ?
- na par b pour tout entier relatif n ?

90 Quel jour de la semaine était le 14 juillet 1789 ?



91 Le 5 octobre 1991 était un samedi.
Quelles sont, au cours des cinquante prochaines années, au cours des cinquante prochaines années, les années où le 5 octobre sera également un samedi ?

92 Pierre et son cousin Paul sont nés le même jour de la semaine et leur date d'anniversaire tombe le même jour. Quelle différence d'âge peuvent-ils avoir ?

93 Soient n et $p \geqslant 2$ deux entiers relatifs.
a. Montrer que le produit $n(n + 1)$ est toujours pair.
b. Montrer que le produit de trois nombres consécutifs est toujours divisible par 3.
c. Montrer que le produit de p nombres consécutifs est toujours divisible par p, pour tout entier naturel p.

94 En utilisant des divisions euclidiennes, déterminer les entiers naturels a, b, c tels que : $\frac{142}{5^3} = a + \frac{b}{5} + \frac{c}{5^2} + \frac{d}{5^3}$ et $0 \leqslant b < 5$, $0 \leqslant c < 5$, $0 \leqslant d < 5$. En déduire l'écriture de 142 comme somme de puissances de 5.

Congruences

95 Soient a, b, n trois entiers naturels tels que $a \equiv b\ [n]$. Montrer que b est le reste dans la division de a par n si et seulement si $0 \leqslant b < n$.

Application

Soit n et p deux entiers naturels. Démontrer que si dans la division euclidienne de n par p le reste est $p - 1$, alors dans la division euclidienne de n^2 par p le reste est 1.

96 Soient a, b, n trois entiers naturels tels que $a \equiv b\ [n]$.

a. Montrer que si $a \equiv 0\ [n]$, alors $a.b \equiv 0\ [n]$.

b. Montrer que $4.9 \equiv 0\ [6]$.

c. Est-il vrai que si $a.b \equiv 0\ [n]$; alors $a \equiv 0\ [n]$ ou $b \equiv 0\ [n]$?

97 Recopier et compléter le tableau suivant qui donne modulo 6 les produits des entiers de 0 à 5.

Ex : $5 \times 2 = 10 = 6 + 4$ donc $5 \times 2 \equiv 4\ [6]$

	0	1	2	3	4	5
0						
1						
2						4
3						
4						
5						

a. Y a-t-il des couples (a, b) non nuls tels que $a \times b \equiv 0\ [6]$? De tels nombres sont appelés diviseurs de zéro modulo 6.

b. Y a-t-il des couples (a, b) tels que $a \times b \equiv 1\ [6]$? De tels nombres sont appelés inverses modulo 6.

98 Même question modulo 7.

99 Les entiers seront écrits ici en base dix. En remarquant que $999 = 27 \times 37$, montrer que pour tout entier positif n : $10^{3n} \equiv 1\ (\text{mod}37)$. En déduire le reste de la division par 37 du nombre $10^{10} + 10^{20} + 10^{30}$.

Avec des bases

100 **Preuve par 9 et autres**

Dans l'ancien temps, les écoliers de CM2 devaient, pour entrer en 6ème, savoir faire des multiplications et des divisions à plusieurs chiffres, sans calculatrice. On leur proposait un critère appelé preuve par 9.

Pour tester la division de a par b, $a = bq + r$, on plaçait dans la croix les sommes des chiffres des nombres a, b, q, r. On avait le droit dans la somme d'éliminer les 9.



Au produit $\bar{b}.\bar{q}$ on ajoute $\bar{r}$ et si on ne trouve pas $\bar{a}$, on sait que le résultat est faux.

a. Exemple. Dans la division de 479773 par 937, Hélène a trouvé 515 comme quotient et 218 comme reste. Sa division est elle juste ?

b. En utilisant les congruences modulo 9, expliquer ce test.

c. Si on retrouve $\bar{a}$, est-on sûr que la division soit exacte ?

101 On désigne par N un entier naturel écrit en base dix, on appelle S la somme de ses chiffres.

1. Démontrer que N est divisible par 9 si et seulement si S est divisible par 9.

On suppose que $A = 2\,012^{2\,012}$; on désigne par :

- B la somme des chiffres de A ;
- C la somme des chiffres de B ;
- D la somme des chiffres de C.

2. **a.** Démontrer que $5^6 \equiv 1\ [9]$.

b. En déduire que $A \equiv 7\ [9]$, puis que $D \equiv 7\ [9]$

3. Sachant que $2\,012 < 10\,000$, démontrer que A s'écrit en numération décimale avec au plus 8 048 chiffres. En déduire que $B \leqslant 72\,432$.

4. Démontrer que $C \leqslant 43$.

5. En étudiant la liste des entiers inférieurs à 45, déterminer un majorant de D plus petit que 15.

6. Démontrer que $D = 7$.

Avec des suites

102 On pose $u_n = 55^n + 56^n + 57^n$.

a. Pour quelle valeur de n, u_n est il divisible par 7 ?

b. Pour quelle valeur de n, u_n est il divisible par 10 ?

103 n désigne un entier naturel

On considère la suite (u_n) d'entiers naturels définie par $u_0 = 14$ et $u_{n+1} = 5u_n - 6$ pour tout entier naturel n.

a. Calculer u_1, u_2, u_3 et u_4.

Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?

b. Montrer que, pour tout n, $u_{n+2} \equiv u_n$ (modulo 4).

En déduire que pour tout k, $u_{2k} \equiv 2$ (modulo 4) et $u_{2k+1} \equiv 0$ (modulo 4).

c. Montrer que, pour tout n, $2u_n = 5^{n+2} + 3$.

En déduire que, pour tout n, $2u_n \equiv 28$ (modulo 100).

d. Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.

Soit d un diviseur commun à tous les u_n. Montrer que $d = 1$ ou $d = 2$.

104 Soit a un entier naturel non nul inférieur ou égal à 8.

On définit la suite (u_n) par $u_0 = a$ et pour tout entier naturel n, $u_{n+1} = u_n^2 + u_n$.

Montrer que si $u_n \equiv 0\ [9]$, alors $u_{n+1} \equiv 0\ [9]$

Existe-t-il des valeurs de a pour lesquelles u_n est divisible par 9 à partir d'un certain rang ? Si oui, lesquelles ?

Des équations

105 Étant donné un entier naturel $n > 1$, on se propose d'étudier l'existence de trois entiers naturels x, y et z tels que $x^2 + y^2 + z^2 \equiv 2^n - 1$ (modulo 2^n).

Partie A : Étude de deux cas particuliers

1. Dans cette question on suppose $n = 2$. Montrer que 1, 3 et 5 satisfont la condition précédente.

2. Dans cette question, on suppose $n = 3$.

Soit m un entier naturel. Faire un tableau donnant le reste r de la division euclidienne de m par 8 et le reste R de la division euclidienne de m^2 par 8.

Peut-on trouver trois entiers naturels x, y et z tels que $x^2 + y^2 + z^2 \equiv 7$ (modulo 8) ?

Partie B : Étude du cas général où $n \geqslant 3$.

Supposons qu'il existe trois entiers naturels x, y et z tels que $x^2 + y^2 + z^2 \equiv 2^n - 1$ (modulo 2^n).

1. Justifier le fait que les trois entiers naturels x, y et z sont tous impairs ou que deux d'entre eux sont pairs.

2. On suppose que x et y sont pairs et que z est impair. On pose alors $x = 2q$, $y = 2r$, $z = 2s + 1$ où q, r, s sont des entiers naturels.

a. Montrer que $x^2 + y^2 + z^2 \equiv 1$ (modulo 4).

b. En déduire une contradiction.

3. On suppose que x, y, z sont impairs.

a. Prouver que, pour tout entier naturel k non nul, $k^2 + k$ est divisible par 2.

b. En déduire que $x^2 + y^2 + z^2 \equiv 3$ (modulo 8). Conclure.

106 **a.** Trouver un entier a compris entre 0 et 6 tel que $3a \equiv 1$ [7].

b. Montrer que $3x \equiv 4$ [7] équivaut à $x \equiv 6$ [7].

Aide

Pour cela, on montrera que si $x \equiv 6$ [7], alors $3x \equiv 4$ [7]
Réciproquement, si $3x \equiv 4$ [7] alors $x \equiv 6$ [7].

107 On cherche à déterminer les couples $(n ; m)$ d'entiers naturels non nuls vérifiant la relation :

$$7^n - 3 \times 2^m = 1 \text{ (E)}.$$

1. On suppose $m \leqslant 4$. Montrer qu'il y a exactement deux couples solutions.

2. On suppose maintenant que $m \geqslant 5$.

a. Montrer que si le couple $(n ; m)$ vérifie la relation (E) alors $7^n \equiv 1$ (mod 32).

b. En étudiant les restes de la division par 32 des puissances de 7, montrer que si le couple $(n ; m)$ vérifie la relation (E) alors n est divisible par 4.

c. En déduire que si le couple $(n ; m)$ vérifie la relation (E) alors $7^n \equiv 1$ (mod 5).

d. Pour $m \geqslant 5$, existe-t-il des couples $(n ; m)$ d'entiers naturels vérifiant la relation (E) ?

e. Conclure, c'est-à-dire déterminer l'ensemble des couples d'entiers naturels non nuls vérifiant (E).

108 1. Résoudre dans $\mathbb{R}$ l'équation $6x^2 - 5x - 4 = 0$. Existe-t-il des solutions entières ?

2. On se propose de trouver des entiers relatifs solutions de $6n^2 - 5n - 4 \equiv 0$ [7] (E). On note P le nombre $6n^2 - 5n - 4$.

a. Montrer que $P \equiv -n^2 - 5n - 4$ [7].

b. On souhaite réaliser « une mise sous forme canonique modulo 7 ». Justifier qu'il suffit de trouver a tel que $-n^2 - 5n - a^2 \equiv -(n + a)^2$ [7] et donc qu'il suffit de trouver un entier relatif a tel que $2a \equiv 5$ [7].

c. Pour cela, dresser la table de multiplication modulo 7. En déduire un entier relatif a tel que $2a \equiv 5$ [7].

d. À l'aide des questions précédentes, montrer que $P \equiv -(n + a)^2 + b$ [7] où b est un entier relatif à déterminer.

e. À l'aide de la table dressée à la question c., trouver un entier relatif c tel que $c^2 \equiv 4$ [7].

f. En déduire une factorisation de P, puis, toujours à l'aide du tableau, deux solutions de « l'équation (E) ».

g. Y a-t-il d'autres factorisations possibles ? D'autres solutions de « l'équation » ?

3. Résoudre « l'équation $6n^2 - 5n - 4 \equiv 0$ [7] » d'une autre façon.

109 On considère l'équation $6x + 7y + 8z = 57$. (E)

Soit (x, y, z) un triplet d'entiers naturels solution.

1. Montrer que l'entier y est impair.

2. On pose $y = 2p + 1$ où p est un entier naturel. Montrer que le reste dans la division euclidienne de $p + z$ par 3 est égal à 1.

3. On pose $p + z = 3q + 1$ où q est un entier naturel. Montrer que les entiers naturels x, p et q vérifient la relation : $x + p + 4q = 7$. En déduire que q prend les valeurs 0 ou 1.

4. En déduire les triplets d'entiers naturels solutions de (E).

110 On considère l'équation (E) : $6x^2 - 5y^2 = 7$ dont les inconnues x et y sont des entiers relatifs.

a. Montrer que si un couple $(x ; y)$ est solution de (E) alors $x^2 \equiv 2$ [5].

b. Pour tout entier relatif a, quels sont les restes possibles de la division euclidienne de a^2 par 5 ?

c. Quel est l'ensemble des solutions de l'équation (E) ?

111 Soit E l'ensemble des triplets d'entiers relatifs $(u ; v ; w)$ tels que $3u + 13v + 23w = 0$.

a. Montrer que pour un tel triplet $v \equiv w$ (mod 3).

On pose $v = 3k + r$ et $w = 3k' + r$ où k, k' et r sont des entiers relatifs et $0 \leqslant r \leqslant 2$.

b. Montrer que les éléments de E sont de la forme : $(-13k - 23k' - 12r ; 3k + r ; 3k' + r)$.
c. Déterminer l'ensemble des éléments de E dont les éléments sont compris entre –5 et 5.

Divers

112 Soit n un entier naturel et $A_n = 3^{2n} - 2^n$.
1. Calculer A_0, A_1, A_2, A_3. Montrer que A_1 divise A_0, A_2 et A_3. On va montrer par trois méthodes différentes que A_n est divisible par 7.
2. **Par récurrence**
a. Montrer que $A_{n+1} = 9(A_n + 2^n) - 2 \times 2^n$.
b. Montrer par récurrence sur n que pour tout entier naturel n, A_n est divisible par 7
3. **Par factorisation**
a. Démontrer que pour tout couple (a, b) de réels, $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-1} + b^n)$.
b. En déduire que A_n est divisible par 7.
4. **Avec les congruences**
a. Montrer que pour tout a, $A_n \equiv 0$ [7]
b. Conclure.

113 Montrer que, pour tout $n \geqslant 1$, le nombre $A = 3 \times 5^{2n-1} + 2^{3n-2}$ est divisible par 17.

114 Déterminer les entiers naturels n tels que le nombre $(2 \times 3^n + 3)$ soit divisible par 11.

115 Soit le nombre $N = n^3 - 3n + 5$.
En utilisant la théorie des congruences, déterminer :
a. La forme générale des entiers relatifs n tels que l'on ait $N \equiv 0$ (mod7).
b. La forme générale des entiers relatifs n tels que l'on ait $N \equiv 1$ (mod7).

116 Soient a et b deux entiers naturels.
On veut montrer que $A = ab(a^2 - b^2)$ est divisible par 3.
1. **Méthode 1** : Par factorisation
Montrer que l'un au moins des quatre nombres a, b, $a + b$, $a - b$ est divisible par 3.
2. **Méthode 2** : Avec les congruences
a. Montrer que pour tout entier naturel a, $a^2 \equiv 0$ [3] ou $a^2 \equiv 1$ [3].
b. Conclure.

117 Soit $n = \overline{cdu}$ en écriture décimale.
a. Montrer que n est multiple de 4 si seulement si $2d + u$ est multiple de 4.
b. Montrer que si n est divisible par 107, alors $7d^2 + (7c - u)^2$ est aussi divisible par 107.

118 On considère la suite (u_n) définie par :
$u_n = (3n - 1)^2 - 2 + (-2)^n$. Calculer u_0, u_1, u_2, u_3.
Montrer que $u_{n+1} + 2u_n$ est divisible par 27.
Que dire alors de u_n ?

119 Soit n un entier naturel. Un nombre A s'écrit $abcd$ en base n si, et seulement si, $A = a.n^3 + b.n^2 + c.n + d$, avec $0 \leqslant a < n$, $0 \leqslant b < n$, $0 \leqslant c < n$ et $0 \leqslant d < n$.
On cherche un nombre entier qui s'écrit $abca$ dans le système à base onze et $bbac$, dans le système à base sept.
a. Vérifier que $1\,325\,a + 10\,c = 271\,b$.
b. En raisonnant modulo 10, montrer qu'il n'y a qu'un seul nombre répondant à la question.

120 Trouver les entiers naturels compris entre 100 et 200, divisibles par 9, et qui dans le système de numération de base 6 s'écrivent $x3y$.

121 1. Quel est l'ensemble des diviseurs de 72 ?
2. Soit p un nombre entier naturel.
a. Mettre le nombre entier relatif $p^2 - 6p - 63$ sous la forme d'une différence de deux entiers naturels, l'un d'eux étant un carré parfait, l'autre ne dépendant pas de p.
b. En déduire tous les couples $(p ; q)$ d'entiers naturels, solutions de l'équation $p^2 - 6p - 63 = q^2$.

122 Calculer les restes, dans la division par 7, des puissances successives de 5. Pour quelles valeurs de l'entier naturel n le nombre $5^{6n} + 5^n + 2$ est-il un multiple de 7 ?

123 Écrire, suivant les valeurs de l'entier naturel n, le reste de la division de 2^n par 5. En déduire le reste de la division de 2^{917541} par 5.

124 Démontrer que $N = n(2n + 1)(7n + 1)$ est divisible par 6, quel que soit l'entier n non nul.

125 **a.** Comment faut-il choisir l'entier naturel n pour que $2^n - 1$ soit divisible par 9 ?
b. À quelle condition sur les entiers naturels x et y la division par 9 de $2^x\,11^y$ donne-t-elle 1 pour reste ?

126 **a.** Étudier les restes des divisions par 7 des puissances successives de 4, 5 et 6.
b. Déterminer les entiers naturels n pour lesquels $4^n + 5^n + 6^n$ est divisible par 7. Préciser les solutions comprises entre 105 et 125.

127 Déterminer les entiers naturels s'écrivant $\overline{abca}$ dans le système de numération décimale, divisibles par 7 et dont le reste dans la division par 99 est 1.

128 Soit n un entier naturel.
a. Trouver suivant les valeurs de n, les restes de la division de 5^n par 13.
b. En déduire que $1\,981^{1\,981} - 5$ est divisible par 13.
c. Démontrer que, pour tout entier naturel n supérieur ou égal à 1, le nombre $N = 31^{4n+1} + 18^{4n-1}$ est divisible par 13.

129 1. Démontrer que, pour tout entier naturel n : $2^{3n} - 1$ est un multiple de 7. En déduire que $2^{3n+1} - 2$ est un

multiple de 7 et que $2^{3n+2} - 4$ est un multiple de 7.

2. Déterminer les restes de la division par 7 des puissances de 2.

3. Le nombre p étant un entier naturel, on considère le nombre entier : $A_p = 2^p + 2^{2p} + 2^{3p}$.

a. Si $p = 3n$, quel est le reste de la division de A_p par 7 ?

b. Démontrer que si $p = 3n + 1$ alors A_p est divisible par 7.

c. Étudier le cas où $p = 3n + 2$.

4. On considère les nombres entiers a et b écrits dans le système binaire : $a = 1001001000$ $b = 1000100010000$. Vérifier que ces deux nombres sont des nombres de la forme A_p. Sont-ils divisibles par 7 ?

130 Du codage affine

À toute lettre de l'alphabet on associe dans l'ordre un entier naturel de 0 à 25. A → 0, B → 1, ..., Z → 25.

On code ensuite chaque nombre n par la fonction de codage f, tel que $f(n)$ est le reste dans la division par 26 de $3n+2$. Ainsi, A → 0 → 2 → C. La lettre A est codée par la lettre C.

1. Coder le message suivant : VIVE LES MATHS.
(On pourra utiliser la calculatrice ou le tableur.)
Décoder un message, c'est retrouver de quelle lettre on est parti.

2. On peut coder toutes les lettres (on pourra présenter un tableau), et ainsi par lecture inverse du tableau on pourra décoder le message.
Décoder AFXR BUBR SFCR.

3. On peut aussi trouver la fonction de décodage g, telle que $f(n) = m$ équivaut à $g(m) = n$.

a. Montrer que $3n \equiv m - 2$ [26]

b. À l'aide de la calculatrice, trouver p tel que $3p \equiv 1$ [26].

c. Montrer alors que $3pn \equiv n$ [26], puis que $n \equiv p(m - 2)$ [26].

d. Montrer que si $n \equiv p(m - 2)$ [26], alors $3n + 2 \equiv m$ [26].
En déduire la fonction de décodage.

131 Le chiffrement de Hill (1929)

On code un couple par une fonction f.
$f(n_1 ; n_2) = (p_1 ; p_2)$. Par exemple :
$p_1 = 3n_1 + 5n_2$ [26] et $p_2 = 6n_1 + 11n_2$ [26].
Ainsi le mot CD, associé au couple (2 ; 3), lequel par f devient (21 ; 19) est codé par VT.

1. En séparant par bloc de deux, coder NOMBRE.
Décoder, c'est retrouver $(n_1 ; n_2)$ connaissant $(p_1 ; p_2)$

2. **a.** Montrer que :
$3n_1 = 11p_1 - 5p_2$ [26] et $3n_2 = 3p_1 - 6p_2$ [26].

b. À l'aide de la calculatrice, trouver m tel que $3m \equiv 1$ [26]. Montrer alors que :
$n_1 = m(11p_1 - 5p_2)$ [26] et $n_2 = m(-6p_1 + 3p_2)$ [26].

c. Décoder le message suivant : MPYORQZ.

132

Le code INSEE d'une personne est un nombre A formé de 15 chiffres, 13 chiffres qui forment le numéro INSEE suivis d'une clé de contrôle de 2 chiffres : (voir activité 5) calculée à partir des 13 chiffres précédents de la façon suivante :
Si N désigne le nombre formé des treize premiers chiffres et r le reste de la division euclidienne de N par 97, alors la clé de contrôle K est le nombre $K = 97 - r$.

1. Vérifier que K est bien un nombre à deux chiffres, les deux pouvant être nuls.

2. On note $B = N + K$. Vérifier que $B \equiv 0$ [97]

3. Supposons qu'en tapant son numéro, on se trompe d'un chiffre. On obtient un nouveau numéro N'.

a. Montrer que $|N - N'| = a.10^m$, $1 \leqslant a \leqslant 9$ et $0 \leqslant m \leqslant 12$.

b. À l'aide d'un tableur, montrer que $N - N'$ n'est pas congru à 0 modulo 97.

c. Conclure.

4. Supposons qu'on intervertisse deux chiffres consécutifs, par exemple ... 52 ..... au lieu de ... 25 ...

a. En appelant a et b les chiffres intervertis, montrer que $|N-N'|=9|a-b|10^m$, où $0 \leqslant m \leqslant 11$. À l'aide d'un tableur, prouver que l'erreur est détectée.

133 La clé du RIB

Le relevé d'identité bancaire comporte 5 chiffres pour le code de la banque, 5 chiffres pour le code du guichet et 11 pour le numéro de compte.
B est un nombre de 21 chiffres et R le reste de B dans la division par 97.
La clé K est définie par $K = 97 - R$.
Exemple B = 30003404010000615123**
Déterminer la clé.

134 Numéro de carte bancaire

Un numéro de carte bancaire est formé de 16 chiffres $a_{15}a_{14}...a_1a_0$.
On définit une fonction m telle que $m(x) = 2x$ si $0 \leqslant 2x \leqslant 9$ et $m(x) = x_1 + x_2$ si $2x = 10x_1 + x_2$.
Un numéro doit être tel que $a_0 + m(a_1) + ... + m(a_{15})$ est un multiple de 10. Le numéro suivant est-il un numéro de carte : 4974 9036 9427 8319 ? Montrer que si un seul chiffre est erroné, l'erreur est détectée.

135 Code correcteur de parité

Un octet binaire est composé de 8 chiffres choisis parmi 0 ou 1. Par exemple 10011011. Chaque octet binaire est complété par un bit supplémentaire m de telle sorte que la somme des 9 bits soit nulle modulo 2.
Une erreur de transmission qui change la parité d'une de ces sommes est donc détectée mais évidemment non localisée sur le mot.

a. Pour A = 10011011, calculer m.

b. Montrer que $m = 0$ si et seulement si le nombre de 1 est pair.

c. Montrer que si on met un 1 à la place d'un 0, l'erreur est détectée. Citer des cas ou l'erreur n'est pas détectée.

Devoir de synthèse

Revoir les bases suivantes :
cours A à C, savoir-faire 1 à 11.

[Le devoir est corrigé p. 170]

Chaque exercice peut être fait de manière indépendante.

Premier sujet

136 **Questions de cours** [2 points]
Les questions sont indépendantes.

Question 1
Soient a, b, m, n et d des entiers relatifs.
Montrer la propriété :
Si d divise m et n, alors d divise $am + bn$.

Question 2
Soient a un entier naturel et b un entier naturel non nul. On admet l'existence d'un couple d'entiers naturels $(q ; r)$ tels que $a = bq + r$ et $0 \leqslant r < b$.
Montrer l'unicité de ce couple $(q ; r)$.

137 [3 points]
Déterminer tous les couples d'entiers relatifs tels que : $9x^2 = y^2 + 20$.

138 [2 points]
Déterminer tous les entiers relatifs n tel que $n + 3$ divise $4n + 7$.

139 [3 points]
Démontrer par récurrence que, pour tout entier naturel n, 7 divise $3^{2n+1} + 2^{n+2}$.

140 [3 points]
a. Justifier que tout entier relatif est de la forme $3k$ ou $3k + 1$ ou $3k + 2$ où k est un entier relatif.
b. En déduire que, pour tout entier relatif n, 3 divise $n^3 - 7n$.

141 [3 points]
n et d sont des entiers naturels.
a. Déterminer tous les entiers naturels d tels que d divise $3n + 13$ et $2n + 17$.
b. En déduire tous les couples d'entiers naturels $(d ; n)$ tels que d divise $3n + 13$ et $2n + 17$.

142 [2 points]
Déterminer les entiers naturels n tels que $n^2 + 3n + 1$ soit divisible par $n - 1$.

143 [2 points]
Les entiers naturels a, b et c sont les mesures des longueurs des côtés d'un triangle rectangle et on suppose que $a < b < c$. Montrer que l'un au moins des trois entiers naturels a, b, c est pair.

Deuxième sujet

144 **Question de cours** [3 points]
a, b, c et d sont des entiers relatifs et n est un entier naturel non nul.

a. Montrer les trois propriétés :
P1 : $a \equiv b[n]$ et $b \equiv c[n] \Rightarrow a \equiv c[n]$;
P2 : $a \equiv b[n] \Rightarrow a + c \equiv b + c[n]$;
P3 : $a \equiv b[n] \Rightarrow ac \equiv bc[n]$.

b. En déduire les propriétés :
P4 : $a \equiv b[n]$ et $c \equiv d[n] \Rightarrow a + c \equiv b + d[n]$
P5 : $a \equiv b[n]$ et $c \equiv d[n] \Rightarrow ac \equiv bd[n]$

145 [6 points]
a. Déterminer suivant les valeurs de l'entier naturel n, les restes de la division euclidienne de 5^n par 13.
b. En déduire le reste de la division euclidienne de $1\,981^{1\,981}$ par 13.
c. Démontrer que, pour tout entier naturel non nul n, $31^{4n+1} + 18^{4n-1}$ est divisible par 13.

146 [6 points]
On considère l'équation (E) $11x^2 - 7y^2 = 5$, où x et y sont des entiers relatifs.
a. Démontrer que si le couple $(x ; y)$ est solution de (E), alors $x^2 \equiv 2y^2[5]$.
b. Soit x et y des entiers relatifs. Recopier et compléter les tableaux.

Modulo 5, x est congru à	0	1	2	3	4
Modulo 5, x^2 est congru à					

Modulo 5, y est congru à	0	1	2	3	4
Modulo 5, $2y^2$ est congru à					

c. En déduire que si $(x ; y)$ est solution de (E), alors x et y sont des multiples de 5.
d. Conclure sur la résolution de l'équation (E).

147 [5 points]
Les chiffres en base 12
sont : 0, 1, 2, ..., 9, α, β (α pour dix et β pour onze).
Soit N d'écriture en base 12 : $N = \overline{a_n \ldots a_1 a_0}$,
c'est-à-dire $N = a_n \times 12^n + \ldots + a_1 \times 12 + a_0$ où a_0, a_1, ..., a_n sont des « chiffres » de la base 12.

1. **a.** Démontrer que $N \equiv a_0$ [3].
b. En déduire un critère de divisibilité par 3 pour un nombre écrit en base 12.

2. **a.** Démontrer que $N \equiv a_n + \ldots + a_1 + a_0$ [11].
b. En déduire un critère de divisibilité par 11 pour un nombre écrit en base douze.

3. Soit le nombre écrit en base 12 : $N = \overline{\beta 1 \alpha}$. Le nombre N est-il divisible par 3 et par 11 ?

Exercices guidés BAC

148 Le code d'identification d'un article est formé de sept chiffres entre 0 et 9. Les six premiers chiffres identifient l'article, le septième est une clé de contrôle destinée à déceler une erreur dans l'écriture des six premiers.
On notera $x_1\,x_2\,x_3\,x_4\,x_5\,x_6\,x_7$ un tel code.
La clé de contrôle x_7 est le reste de la division euclidienne par 10 de la somme :
$N = (x_1 + x_3 + x_5) + 7(x_2 + x_4 + x_6)$.

1. **a.** Vérifier que le code suivant est correct : 2341547.
b. Calculer la clé du code suivant : 923451•.
c. Un des chiffres du code suivant a été effacé : 11•2774. Le calculer.
d. Un des chiffres du code suivant a été effacé : 134•752. Le calculer.

2. Dans cette question un des chiffres du code est erroné : au lieu de saisir $x_1\,x_2\,x_3\,x_4\,x_5\,x_6\,x_7$, le dactylographe a frappé $x_1\,x_2\,x_3\,x_3\,x_5\,x_6\,x_7$.
a. Écrire les sommes N_1 et N_2 associées respectivement aux deux codes précédents, puis calculer la différence $N_1 - N_2$.
b. Montrer que l'équation $7a \equiv 0$ [modulo 10], où a est un entier compris entre 0 et 9, a pour seule solution 0.
c. L'erreur de frappe sera-t-elle détectée ?

3. Dans cette question, deux des chiffres du code ont été intervertis : au lieu de saisir $x_1\,x_2\,x_3\,x_4\,x_5\,x_6\,x_7$, le dactylographe a frappé $x_1\,x_3\,x_2\,x_4\,x_5\,x_6\,x_7$.
Donner un exemple de valeurs de x_2 et x_3 pour lesquelles la clé de contrôle ne détecte pas l'erreur.

Guide

1. **a.** Vérifier que le chiffre des unités de N est 7.
b. Calculer le chiffre des unités de N.
c. Résoudre d'équation d'inconnue x_3 modulo 10.
d. Plus difficile, chercher les produits $7N$ modulo 10.

2. **b.** Faire une étude exhaustive des cas.
c. Comment une erreur pourrait-elle être détectée ?

3. Procéder comme au 2.

149 On considère les suites (x_n) et (y_n) définies par : $x_0 = 1$, $y_0 = 8$ et

$$\begin{cases} x_{n+1} = \dfrac{7}{3}x_n + \dfrac{1}{3}y_n + 1 \\ y_{n+1} = \dfrac{20}{3}x_n + \dfrac{8}{3}y_n + 5 \end{cases}$$

1. Montrer par récurrence que tous les points M_n de coordonnées (x_n, y_n) sont sur la droite Δ d'équation $5x - y + 3 = 0$.
En déduire que $x_{n+1} = 4x_n + 2$.

2. Montrer que tous les x_n sont des entiers naturels.
En déduire que les y_n le sont aussi.

3. **a.** Montrer par une étude exhaustive des cas que si $5x \equiv 0$ [3], alors $x \equiv 0$ [3].
b. En déduire x_n est divisible par 3 si, et seulement si, y_n est divisible par 3.
c. Montrer que si x_n n'est pas divisible par 3, x_n et y_n ont 1 pour seul diviseur positif commun.

4. **a.** Montrer que $x_n = \dfrac{1}{3}(4^n \times 5 - 2)$.
b. En déduire que $4^n \times 5 - 2$ est un multiple de 3.
c. Proposer deux autres méthodes pour prouver le 4.b.

Guide

1. Un point est sur une droite si ses coordonnées vérifient l'équation de la droite.
Utiliser une récurrence.

2. Une récurrence encore.

3. **a.** Dans la division par 3, il n'y a que 3 restes possibles. Étudier les 3 cas.
b. Ne pas oublier l'étude directe et la réciproque par 3a.
c. Si d divise x_n et y_n, alors ...
Utiliser 1., puis 3b.

4. **a.** Une récurrence.
b. Se déduit du 4a. et du 2.
c. Penser à la récurrence et aux congruences.

QCM - Vrai ou faux BAC

150 **Vrai ou faux (Justifier)**

a. On considère l'entier $N = 11^{2011}$. L'entier N est congru à 4 modulo 7.

b. On considère l'équation (E) : $x^2 + y^2 = 0$ [3] où $(x ; y)$ est un couple d'entiers relatifs.
Il existe des couples $(x ; y)$ d'entiers relatifs solutions de (E) qui ne sont pas des couples de multiples de 3.

c. $2\,009^{8002} \equiv 2\,009$ [16].

d. a et b sont deux entiers relatifs quelconques, n et p sont deux entiers naturels premiers entre eux.
$a \equiv b$ (p) si, et seulement si, $na \equiv nb$ (p).

151 **Vrai ou faux (Justifier)**

a. x et y sont des entiers naturels.
7 divise $x^2 + y^2$ équivaut à 7 divise x et 7 divise y.

b. Soit x un entier relatif.
$x^2 + x + 3 = 0$ (modulo 5) si, et seulement si, $x \equiv 1$ (modulo 5).

c. Soit N un entier naturel dont l'écriture en base 10 est $aba7$.
Si N est divisible par 7 alors $a + b$ est divisible par 7.

d. Pour tout entier naturel n non nul :
$5^{6n+1} + 2^{3n+1}$ est divisible par 5.

e. Pour tout entier naturel n non nul :
$5^{6n+1} + 2^{3n+1}$ est divisible par 7.

152 **QCM (Justifier, une seule des trois réponses est exacte)**

a. On considère dans l'ensemble des entiers relatifs l'équation : $x^2 - x + 4 \equiv 0$ [6] .
A : toutes les solutions sont des entiers pairs.
B : il n'y a aucune solution.
C : les solutions vérifient : $x \equiv 2$ [6] ou $x \equiv 5$ [6].

b. On considère les deux nombres $n = 1\,789$ et $p = 1\,789^{2\,005}$. On a alors :
A : $n \equiv 4$ (modulo 17) et $p \equiv 0$ (modulo 17).
B : $p \equiv 4$ (modulo 17).
C : $p \equiv 1$ (modulo 17).

c. On considère l'équation $3x - 5y = 1$, d'inconnues (x, y) entiers relatifs.
A : L'équation n'a pas de solution.
B : si (x, y) est solution, $5y \equiv 1$ [3].
C : si (x, y) est solution, $3x \equiv 1$ [5].

d. Dans la division de a par b, le reste est r et le quotient est q.
A : Dans la division de $-a$ par b, le reste est $-r$.
B : Dans la division de $2a$ par b, le reste est $2r$.
C : $3a \equiv 3r$ [b].

e. A : Si $3a \equiv 0$ [6], alors $a \equiv 0$ [6].
B : Si $2a \equiv 4$ [10], alors $a \equiv 2$ [10].
C : Si $3a \equiv 1$ [5], alors $a \equiv 2$ [5].

Exercice BAC

153 **1. a.** Déterminer le reste dans la division euclidienne de 2 009 par 11.

b. Déterminer le reste dans la division euclidienne de 2^{10} par 11.

c. Déterminer le reste dans la division euclidienne de $2^{2\,009} + 2\,009$ par 11.

2. On désigne par p un nombre entier naturel.
On considère pour tout entier naturel non nul n le nombre $A_n = 2^n + p$.
Soit d_n un diviseur commun à de A_n et A_{n+1}.

a. Montrer que d_n divise 2^n.

3. Déterminer la parité de A_n en fonction de celle de p.

4. Dans cette question, toute trace de recherche, même incomplète, ou d'initiative même non fructueuse, sera prise en compte dans l'évaluation.
Déterminer la parité de d_n en fonction de celle de p.
Quels sont les diviseurs communs à $2^{2\,009} + 2\,009$ et $2^{2\,010} + 2\,009$?

154 **1.** Déterminer suivant les valeurs de l'entier naturel n le reste de la division euclidienne de 4^n par 7.

2. a. Montrer que $851 \equiv 4$ [7].

b. Déterminer suivant les valeurs de l'entier naturel n, le reste de la division euclidienne de
$A = 8\,513^{3n} + 8\,512^{2n} + 851^n$ par 7 (on pourra remarquer que $851 \equiv 4$ [7]).

3. On considère le nombre B qui s'écrit en base 4 : $\overline{2103211}^{4}$ ce qui signifie que
$B = 2\,4^6 + 1\,4^5 + \ldots + 1\,4^1 + 1\,4^0$.
En utilisant la question 1, sans calculer explicitement B, déterminer dans le système décimal le reste de la division euclidienne de B par 7.

155 Le but de cet exercice est de déterminer tous les entiers naturels n vérifiant la propriété P : « $n^2 + 11$ est divisible par $n + 11$ ».

1. À l'aide de la calculatrice, faire une conjecture sur la nature de tels nombres.

2. a. Calculer pour tout n, $n^2 + 11 - (n + 11)(n - 11)$.

b. En déduire tous les entiers naturels vérifiant la propriété P.

6, 8, 10, 13, 15}. A pose alors 3 autres questions :

Q5. Le nombre est-il dans G ?

Q6. Le nombre est-il dans H ?

Q7. Le nombre est-il dans I ?

Supposons maintenant que B ait le droit de mentir au plus une fois au cours des 7 questions. On obtient alors un nombre M de 7 chiffres en binaire.

On pose $a = m_1 + m_3 + m_5 + m_7$ [2],

$b = m_2 + m_3 + m_6 + m_7$ [2] et $c = m_4 + m_5 + m_6 + m_7$ [2].

On pose enfin $k = \overline{cba}^2$.

Le nombre choisi est 12.

a. Vérifier que si B ne ment pas, $k = 0$

b. B ment à la question 5.

Calculer a, b, c et montrer que $k = 5$.

On admet que si $k = 0$, B n'a pas menti.

c. Sinon B a menti à la question k. On change alors la réponse et $N = m_1m_2m_3m_4$

Exemple : A trouve $M = 0001100$.

B a-t-il menti ? Que vaut N ?

162 Déterminer les entiers naturels s'écrivant $abca$ dans le système de numération décimale, divisibles par 7 et dont le reste dans la division par 99 est 1.

163 On veut montrer que :

si d divise n, alors $a^d - 1$ divise $a^n - 1$. (P)

Soient d et s tels que $n = ds$.

a. En utilisant la somme des termes d'une suite géométrique, prouver (P).

b. Avec les congruences, montrer que : $a^d \equiv 1$ [$a^d - 1$].

Prouver (P).

164 On considère l'équation $ax + by = c$, d'inconnues $(x ; y)$ entiers relatifs.

Montrer que si $(x ; y)$ est solution, alors $ax \equiv c$ [b] et $by \equiv c$[a].

Montrer que l'équation $3x + 6y = 7$ n'a pas de solutions dans $\mathbb{Z} \times \mathbb{Z}$.

Montrer que l'équation $3x + 6y = 15$ a des solutions dans $\mathbb{Z} \times \mathbb{Z}$.

165 Soit E ={1 , 2, 3,4, 5, 6}.

a. Faire un tableau résumant les produits modulo 7 deux à deux d'éléments de E.

Soit a un élément de E et A = {a, 2a, 3a, 4a, 5a, 6a}. On appelle r_k le reste dans la division de ka par 7.

b. Montrer, en utilisant le tableau de la question a) que les r_k pour k dans E sont non nuls et distincts.

c. Montrer en utilisant la question a) que pour tout b de E, il existe un élément b^* de E tel que $b \times b^* \equiv 1$ [7].

En effectuant de deux façons le produit de tous les éléments de A modulo 7, montrer que $a^6 \equiv 1$ [7].

Défis

166 Soient $n + 1$ entiers naturels dont aucun n'est supérieur à $2n$, montrer qu'au moins l'un d'entre eux doit en diviser un autre.

167 Démontrer que pour tout entier naturel n,

$2 \times 7^{2n+1} + 3^{n+2}$ est divisible par 23.

168 Soit N un nombre de p chiffres, avec $4 \leqslant p \leqslant 6$,

écrit en système décimal avec les chiffres 1, 3, 7, 9, chacun y figurant au moins une fois.

Montrer qu'il existe un nombre utilisant les mêmes chiffres que N, divisible par 7.

169 Déterminer tous les couples $(m ; n)$ d'entiers strictement positifs tels que $\dfrac{n^3 + 1}{mn - 1}$ soit un entier.

(Olympiades internationales 1994)

Communiquer à l'écrit ou à l'oral

Des problèmes de chiffrement

Chercher le sens des mots suivants :

Stéganographie, cryptographie, cryptanalyse, chiffrement.

Qu'est ce qu'un chiffrement monoalphabétique ?

Comment peut-on décrypter de tels messages si on ne connaît pas la clé ?

Comment marchait la machine à congruence ? Enigma ?

Qu'est ce que le code ASCII ?



Un message à décoder :

Dans le message suivant, chaque lettre est remplacée par le chiffre des unités de son numéro dans l'alphabet. De plus on a supprimé les blancs.

Retrouver le message.

259453285995406259445359058 59

Accompagnement personnalisé

Soutien

AP 1 Analyser une réponse

Objectif :
- *Revoir les bases du premier chapitre.*

A. Chercher l'erreur et la corriger

1. a divise b signifie qu'il existe un réel k tel que $b = ak$.
2. a divise b signifie qu'il existe un entier relatif tel que $a = kb$.
3. $8x = 7b$ implique que $x = \frac{7}{8}b$, donc x est multiple de b.
4. d divise 4 et d divise 6 équivaut à d divise $4a + 6b$ pour tout couple d'entiers relatifs $(a ; b)$.
5. d est multiple de 4 et de 6 donc d est multiple de 24.
6. si $a \equiv b$ [c], alors b est le reste dans la division euclidienne de a par c.
7. $a = 21 \times 23 + 22$, donc 22 est le reste dans la division de a par 21.
8. $27 \equiv 15$ [12], donc $9 \equiv 5$ [12].
9. $a \equiv b$ [c] équivaut à $2a \equiv 2b$ [c].
10. si $ab \equiv 0$ [c], alors $a \equiv 0$ [c] ou $b \equiv 0$ [c].

B. Analyser une solution

Énoncé : Résoudre dans Z l'équation $x^2 - 9y^2 = 20$.

Et voici le début de la solution d'un élève :
Pour $x = 0$, $-9y^2 = 20$, impossible.
Pour $x = 1$, $-9y^2 = 19$, impossible.
Pour $x = 2$, $-9y^2 = 16$, impossible.

1. Que penser de cette méthode ?
2. Quelle remarque le professeur a pu inscrire sur la copie ?
3. Pour quel type d'équation l'étude exhaustive des cas est une bonne méthode ?
4. Quelles sont les méthodes pour résoudre cette équation ?

Découvrir un métier

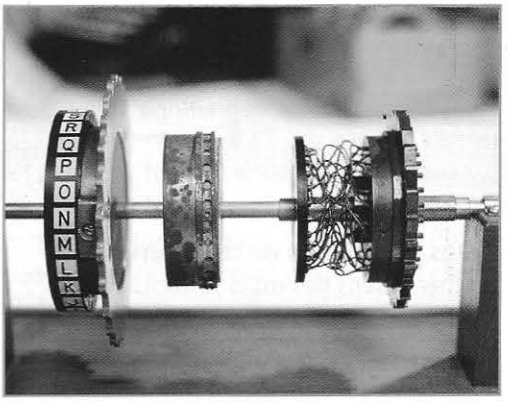
AP 2 Les métiers de la cryptographie : un secteur d'avenir

Objectif :
- *Se familiariser avec les métiers de l'arithmétique.*

Le développement des échanges marchands et des transactions marchandes sur Internet rend indispensable l'authentification des partenaires et la confidentialité des échanges, ceci ne peut se faire qu'avec l'utilisation de techniques cryptographiques de plus en plus performantes car ils sont soumis à des attaques de plus en plus perfectionnées et puissantes du fait des progrès des processeurs informatiques. Ce secteur offrira donc de nombreux débouchés.

Ingénieur cryptographe : concepteur de systèmes destinés à chiffrer, à authentifier, à assurer l'intégrité des données.

Ingénieur cryptanalyste : s'opposant au cryptographe, il cherche à déjouer les techniques destinées à protéger les informations.



1. De quel type d'attaque est-il question ?
2. Quelle formation faut-il suivre pour accéder aux métiers de la cryptographie ?
3. Qu'est ce qu'un ingénieur du chiffre ?

POUR EN SAVOIR PLUS
Pour plus d'informations, consultez la brochure de l'ONISEP, Les Métiers des Mathématiques.

Approfondir

AP 3 Du bon usage des congruences

Objectif :
- *Comprendre l'outil congruence.*

Parmi les outils proposés dans ce premier chapitre, la théorie des congruences est dans certains cas la plus efficace :

	Méthodes
❶ Critère de divisibilité Soit un nombre d'écriture décimale : $a = a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_1 10 + a_0$. Démontrer les critères de divisibilité par 3 et 11.	• Vérifier que $10 \equiv 1$ [3], puis que pour tout entier naturel n, $10^n \equiv 1$ [3]. • Vérifier que $10 \equiv -1$ [11].
❷ Détermination du reste de 5^n dans la division par 7 en fonction de n. **a.** Vérifier que $5^2 \equiv 4$ [7], puis que $5^3 \equiv 4 \times 5$ [7], donc $5^3 \equiv -1$ [7]. Enfin que $5^6 \equiv 1$ [7]. **b.** Démontrer que si r est le reste de n dans la division par 6, alors $5^n \equiv 5^r$ [7]. **c.** Application : quel est le reste dans la division par 7 de 5^{2014} ?	• Soit $a \equiv b$ [n]. À quelle condition b est-il le reste dans la division de a par n ? • Rappeler les règles de compatibilité des congruences avec la multiplication et l'élévation à une puissance. • Les restes sont cycliques, il suffit de trouver la période.
❸ Résoudre des équations diophantiennes. En raisonnant modulo 11 montrer que $x^5 - y^2 = 4$ n'a pas des solutions dans $\mathbb{N}$.	• Combien y a-t-il de restes possibles dans la division par 11 ? • pour chacun de ces restes r, étudier les congruences modulo 11 de r^2, puis de r^5.
❹ Soient a et b deux entiers tels que $a^2 + b^2$ soit divisible par 7. Montrer que a et b sont divisibles par 7.	• Comme les puissances figurent au carré, on a intérêt à prendre des représentants négatifs et positifs. • Faire un tableau donnant les carrés des restes centrés modulo 7, c'est-à-dire de –3 à 3. • Faire les sommes des carrés deux à deux.

Une étude directe est parfois plus rapide.
Exemple : Pour montrer que si n est impair alors n^2 est congru à 1 modulo 8, poser $n = 2k + 1$, calculer n^2, puis factoriser et conclure en montrant que $k(k + 1)$ est pair.

AP 4 La cryptographie

Objectif :
- *Découvrir l'histoire de la cryptographie.*

Un peu d'histoire

De tout temps, les hommes ont cherché à communiquer en secret notamment pour des raisons politiques ou religieuses. La cryptographie est née dans l'antiquité de la nécessité de conserver le secret des communications entre les chefs militaires et leurs armées, ainsi qu'entre les États qui avaient noué des alliances.
Le procédé le plus simple, substitution d'une lettre par une autre, sous réserve que le procédé utilisé fasse correspondre à toutes lettres une et une seule lettre, fut utilisé, depuis Jules César, durant dix siècles.
Évidemment, l'étude de la fréquence d'apparition des lettres permet aisément de trouver les correspondances et ce procédé fut abandonné.
Furent alors envisagés des procédés utilisant cette méthode de correspondance, mais de façon « irrégulière », par exemple grâce à des machines ayant une rotation irrégulière des disques de codage ou encore grâce à des circuits électriques ; un exemple célèbre est la machine « Enigma ».

Un exemple : Le chiffre de Vigenère

Ce chiffrement utilise une clef, un mot choisi par l'expéditeur et transmis au destinataire, que l'on écrit autant de fois que nécessaire, sous le message à coder et on décale chaque lettre du message à coder du rang de la lettre de la clef située en dessous.

clair	a	l	b	e	r	t	i	v	i	g	e	n	e	r	e
Clef	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D
chiffré	C	Z	E	I	T	H	L	Z	K	U	H	R	G	F	H

Vérifier l'exactitude du chiffrement. Reproduire le carré de Vigenère et expliquer avec cet exemple son utilisation.
Dans certains romans d'espionnage, il est question d'un livre, plus spécialement, d'une phrase d'une page d'un livre, pour pouvoir décoder (ou coder) un message. À quoi pouvait servir ce livre ?

2 PGCD, théorème de Bézout

Vérifier ses acquis

1 Multiple ou diviseur ?

Vrai ou Faux (sans calculatrice)

1. Si $N = 144^2 - 36^2$, alors

a. 6 est un diviseur de N.

b. N est un multiple de 180.

c. N est divisible par 81.

d. 60 est un diviseur de N.

2. a. 11 divise 999.

b. 9 999 est divisible par 11.

c. 33 est un diviseur de 9 999.

d. 9 999 est divisible par 11×33.

3. a. Si d divise a et b, alors d divise $2a - 3b$.

b. Si $2a - 3b = 1$ et d divise a et b, alors $d = 1$ ou $d = -1$.

c. Si $2a - 3b = 1$, alors a et b sont premiers entre eux.

d. Si d est multiple de a et b, alors d est multiple de ab.

2 Division euclidienne

1. a. Effectuer la division de 12 452 par 89.

b. Écrire l'égalité et l'encadrement qui traduisent ensemble la division euclidienne de 12 452 par 89.

2. Les égalités suivantes traduisent-elles des divisions euclidiennes par 11 ?

a. $310 = 11 \times 25 + 35$. **b.** $310 = 11 \times 28 + 2$.

c. $-310 = 11 \times (-28) - 2$. **d.** $-310 = 11 \times (-29) + 9$.

3 PGCD

1. a. Écrire la liste des diviseurs de 140.

b. Écrire la liste des diviseurs de 105

c. En déduire le PGCD de 140 et 105.

d. Existe-t-il une autre façon de calculer le PGCD ?

2. a. Utiliser l'algorithme d'Euclide pour calculer le PGCD de 2000 et 2011.

b. Calculer le PGCD de 3 795 et 6 555.

c. Vérifier avec la calculatrice.

4 Nombres premiers entre eux

1. a. Montrer que tout diviseur commun de 2011 et 2012 divise 1.

b. Que pouvez-vous en déduire sur les entiers 2011 et 2012 ?

2. Vérifier que $77 \times 345 - 58 \times 458 = 1$.

En déduire que 345 et 458 sont premiers entre eux.

5 Fractions irréductibles

a. Donner la forme irréductible des fractions suivantes : $f = \frac{190}{114}$ et $g = \frac{8\,569}{9\,889}$.

b. Quelle est la fraction égale à g dont le numérateur est égal à 8 091 ?

6 Congruences

1. a. Traduire à l'aide d'une égalité $3a \equiv 1$ [5].

b. Traduire par une phrase la proposition suivante : « si $ab \equiv 0$ [6], alors $a \equiv 0$ [6] ou $b \equiv 0$ [6] » et dire si cette proposition est vraie.

2. QCM Choisir la (ou les) bonne(s) réponse(s)

Si 5 divise $n - 4$, alors

a. $n \equiv 5$ [4].

b. $n \equiv 4$ [5].

c. $n = 4 + 5k$ avec k entier relatif.

d. $n = -1 + 5k$ avec k entier relatif.

3. QCM Choisir la (ou les) bonne(s) réponse(s)

Si $2a \equiv 2b$ [10], alors

a. $a \equiv b$ [10].

b. $2a = 2b + 10k$ avec k entier relatif.

c. $a = b + 5k$ avec k entier relatif.

d. $a \equiv b$ [5].

7 Des équations

1. Déterminer tous les couples d'entiers naturels $(x ; y)$ solutions des équations suivantes :

a. $xy = 72$ et $x \leqslant y$. **b.** $(x + 2)(y - 3) = 63$.

c. $x^2 - y^2 = 11$. **d.** $x^2 - y^2 = 70$.

e. $4x^2 - 9y^2 = 99$.

2. Déterminer, si c'est possible, un couple d'entiers relatifs $(x ; y)$ solution de chaque équation :

a. $4x - 6y = 21$. **b.** $5x - 3y = 2$.

c. $5x + 3y = 1$. **d.** $55x + 33y = 11$.

3. Le but est de résoudre dans $\mathbb{Z}$: (E) $5x - 3y = 2$.

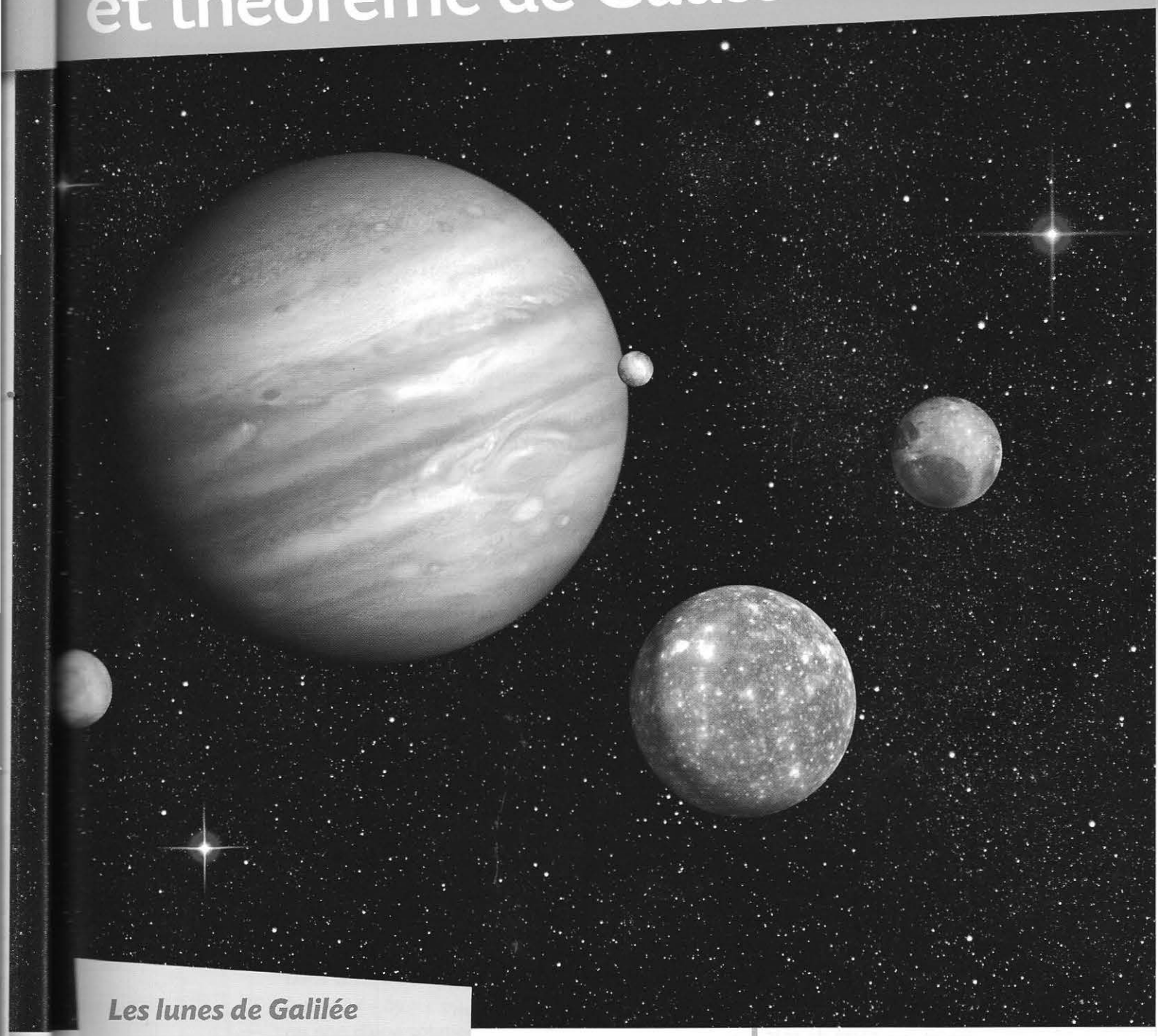
a. Montrer que si $(x ; y)$ est solution de (E), alors $-3y \equiv 2$ [5].

b. Faire un tableau donnant les congruences modulo 5 de $-3y$ suivant les congruences modulo 5 de y.

c. En déduire la résolution de $-3y \equiv 2$ [5].

d. Déterminer alors toutes les solutions de (E).

et théorème de Gauss



Io, Europe, Ganymède et Callisto, les quatre lunes galiléennes de Jupiter.

Les lunes de Galilée

Le 7 janvier 1610, Galilée observe trois corps situés près de Jupiter, qu'il considère d'abord comme des étoiles fixes. Quelques jours plus tard, il en observe un quatrième et prend conscience que ces corps tournent autour de Jupiter. Ces « lunes galiléennes » (Io, Europe, Ganymède et Callisto) sont les premiers objets célestes à avoir été découverts à l'aide d'un instrument optique autre que l'œil nu.

?

La durée de révolution de Ganymède est de 172 h et celle de Callisto de 400 h. Un astronome aperçoit le premier à 0 h le jour J, le deuxième à 8 h le même jour. Pourra-t-il un jour les voir simultanément ?

Activités d'introduction

Activité 1 Pavage d'un rectangle par des carrés

Objectifs
Revoir : la notion de PGCD et le calcul du PGCD par « différences successives».
Découvrir : le principe de la « descente infinie ».



Dans un club de patchwork, l'animatrice propose le sujet suivant : réaliser un patchwork de 1 m 80 sur 1 m 40 en assemblant des carrés de tissu de même côté, les plus grands possibles et dont la longueur c du côté soit un nombre entier de centimètres.
Le problème est de déterminer c.

1 Méthode 1

Voici la méthode proposée par l'animatrice.
Les dimensions du patchwork étant, en cm, L = 180 et l = 120, c doit être le plus grand diviseur commun de 180 et 140.

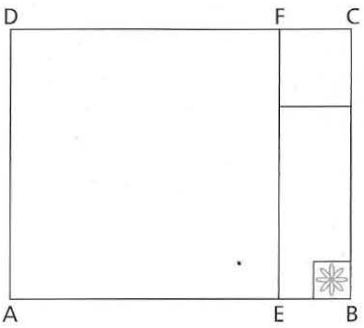
Commentaire

Le PGCD de deux entiers naturels non nuls a et b est le plus grand diviseur commun de a et b. On le note PGCD (a ; b).

a. Déterminer l'ensemble des diviseurs positifs de 180.
b. Déterminer l'ensemble des diviseurs positifs de 140.
c. En déduire l'ensemble des diviseurs communs à 180 et 140 et déterminer le plus grand diviseur commun.
Conclure sur la longueur c.

2 Méthode 2

Pendant ce temps, un membre du club de patchwork a fait le dessin ci-dessous et trouvé la même solution. Voici sa méthode :
« • Étape 0 : Je trace un rectangle ABCD de dimensions AB = L = 180 et AD = l = 140.
• Étape 1 : Je trace à l'intérieur le carré AEFD. Il reste un rectangle EBCF de dimensions L_1 et l_1.
• Je répète les opérations de l'étape 1 dans le rectangle EBCF et je recommence jusqu'à recouvrir totalement le rectangle ABCD. À la fin il reste un carré de côté c. »



a. Exécuter cet algorithme.
b. Noter L_i et l_i la longueur et la largeur du rectangle obtenu à l'étape n° i. Démontrer qu'à chaque étape, c est un diviseur commun de L_i et l_i.
c. i. Montrer que (L_i) est une suite strictement décroissante d'entiers naturels.
ii. Justifier que cet algorithme s'arrête. (On pourra utiliser le principe de la descente infinie)
iii. Quel est le nombre maximum d'étapes ?
d. Montrer qu'à la fin on obtient bien le PGCD de L et l.

Commentaire

Le principe de la descente infinie « Toute suite strictement décroissante d'entiers naturels est finie » a été mis en évidence par Pierre Fermat en 1638.

Activité 2 Les propriétés du PGCD

Objectifs
Revoir : le PGCD.
Découvrir : des propriétés du PGCD.

À l'aide d'un tableur, faire un tableau à double entrée qui donne la valeur du PGCD (a ; b) en fonction des entiers naturels a et b, a et b variant de 1 à 50.
Utiliser la fonction PGCD.

1. Que vaut PGCD (a ; a) si $a \in \mathbb{N}^*$?
2. Quelle symétrie remarque-t-on ? Interpréter.
3. Que vaut PGCD (a ; 2) ? PGCD (a ; 3) ? PGCD (a ; 5) ? Que peut-on conjecturer ?
4. Que vaut PGCD (a ; 4) ? PGCD (a ; 6) ?
5. a. Dans quel cas a-t-on PGCD (a ; 4) = 4 ? PGCD (a ; 6) = 6 ?
b. Conjecturer une condition nécessaire et suffisante pour que PGCD (a ; b) = b.
c. Démontrer cette conjecture.

	A	B	C	D	E	F
1	a \ b	1	2	3	4	5
2	1	1	1	1	1	1
3	2	1	2	1	2	1
4	3	1	1	3	1	1
5	4	1	2	1	4	1
6	5	1	1	1	1	5

=PGCD($A5;F$1)

Commentaire

Pour tous les entiers naturels a et b : Si b divise a, alors PGCD (a ; b) = b.

6. a. Observer la colonne (E) $b = 4$. Quelle périodicité observe-t-on ? Même question pour les colonnes $b = 5$, $b = 6$... Quelle conjecture peut-on faire sur la longueur de la période de la colonne $b = 4$? $b = 5$? $b = 6$?
b. Soient a et b entiers naturels tels que $a > b > 0$. Faire une conjecture sur PGCD ($a - b$; b) et PGCD (a ; b).
c. Démontrer cette conjecture.

Commentaire

Pour tous les entiers naturels a et b tels que $0 < b < a$: PGCD (a ; b) = PGCD ($a - b$; b).

7. En utilisant ces résultats, retrouver le PGCD (180 ; 140).

Activité 3 Existe-t-il une solution entière de l'équation $ax + by = c$?

Objectifs
Revoir : la notion de nombres premiers entre eux.
Découvrir : • la propriété : les entiers de la forme $ax + by$ sont les multiples du PGCD de a et b ;
• une condition nécessaire et suffisante pour que des entiers soient premiers entre eux.

Dans cette activité, on s'intéresse uniquement aux équations diophantiennes de la forme $ax + by = c$ où a, b et c sont des entiers et on se pose le problème de l'existence ou non d'une solution.

1 Étude d'exemples

Dans chaque cas, déterminer, si c'est possible, un couple (x ; y) d'entiers relatifs solution :
a. $6x + 5y = 1$;
b. $6x + 5y = 4$;
c. $12x + 30y = 42$;
d. $12x + 30y = 40$.
Quelles conjectures peut-on faire ?

Aide

Une équation diophantienne est une équation à coefficients entiers et dont les inconnues sont des entiers.

2 Une autre approche

On va s'intéresser à l'ensemble des combinaisons linéaires entières $ax + by$ des deux entiers naturels non nuls a et b.

Activités d'introduction

a. À l'aide d'un tableur, faire un tableau à double entrée qui donne toutes les valeurs de $12x + 30y$ pour des valeurs entières de x et y variant entre -4 et 4.
b. Faire la liste des entiers strictement positifs du tableau. Que constate-t-on ?
c. Faire de même pour les valeurs de $6x + 5y$. Répondre aux mêmes questions.
d. Peut-on faire une conjecture ?

H7 =12*$A7+30*H$2

	A	B	C	D	E	F	G	H	I	J
1			12x+30y							
2	x \ y	-4	-3	-2	-1	0	1	2	3	4
3	-4	-168	-138	-108	-78	-48	-18	12	42	72
4	-3	-156	-126	-96	-66	-36	-6	24	54	84
5	-2	-144	-114	-84	-54	-24	6	36	66	96
6	-1	-132	-102	-72	-42	-12	18	48	78	108
7	0	-120	-90	-60	-30	0	30	60	90	120
8	1	-108	-78	-48	-18	12	42	72	102	132
9	2	-96	-66	-36	-6	24	54	84	114	144
10	3	-84	-54	-24	6	36	66	96	126	156
11	4	-72	-42	-12	18	48	78	108	138	168

3 Étude du cas général

Soient a et b deux entiers naturels non nuls et D = PGCD (a ; b).
Soit E l'ensemble des entiers relatifs qui s'écrivent sous la forme $ax + by$, avec x et y entiers relatifs.
a. On note $E' = E \cap \mathbb{N}^*$. Démontrer que E' est une partie non vide de $\mathbb{N}$. En déduire que E admet un plus petit élément d.
Il existe donc deux entiers relatifs u et v tels que $d = au + bv$.
b. Démontrer que tout multiple de d est un élément de E.
c. Soit $e = am + bn$, un élément de E et q et r le quotient et le reste de la division euclidienne de e par d.
Démontrer que r est un élément de E. En déduire que $r = 0$ et que d divise e.
d. En déduire que E est l'ensemble des multiples de d.
e. i. Justifier que a et b sont des éléments de E, en déduire que d divise a et b et que $d \leqslant D$.
ii. Démontrer que D divise d et en déduire $D \leqslant d$.
iii. En déduire que $D = d$.
f. En déduire que l'équation $ax + by = c$ admet des solutions si et seulement si c est un multiple du PGCD de a et b.
g. Montrer que si PGCD (a ; b) = 1 alors toute équation de la forme $ax + by = c$ admet des solutions.

4 Reprendre les exemples et vérifier si les réponses.

Commentaire

L'ensemble des combinaisons linéaires $ax + by$, à coefficients entiers relatifs, des entiers naturels non nuls a et b est l'ensemble des multiples de leur PGCD.
Deux entiers naturels a et b tels que PGCD (a ; b) = 1 sont dits premiers entre eux.

5 Des conséquences

a. Démontrer que l'ensemble des diviseurs communs de deux entiers naturels est égal à l'ensemble des diviseurs de leur PGCD. (Cette propriété a souvent été utilisée au collège).
b. Démontrer que PGCD (a ; b) = 1 si et seulement si il existe il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Commentaire

Ce résultat est le théorème de Bézout : deux entiers naturels a et b sont premiers entre eux, si et seulement si, il existe deux entiers relatifs a et b tels que $au + bv = 1$.

Activité 4 Chiffrement affine : des réponses aux questions

Objectifs
Revoir : le chiffrement affine de clé $(a ; b)$.
Découvrir : l'utilité de choisir a premier avec 26, et aborder le théorème de Gauss.

Mémo

Principe du chiffrement affine : on assimile les 26 lettres de l'alphabet aux nombres 0, 1, ..., 25. On code un nombre x de la façon suivante : le nombre codé noté $c(x)$ est le reste de la division euclidienne de $ax + b$ par 26.
Le couple $(a ; b)$ est la clé du codage ; c'est une clé secrète, elle n'est connue que par le chiffreur et le déchiffreur.

1 **Exemples**

a. Coder le mot Fermat avec le chiffrement affine de clé $(a ; b) = (6 : 5)$.
b. Coder le mot Fermat avec le chiffrement affine de clé $(a ; b) = (3 ; 5)$.
c. Que remarquez-vous ?

2 **Question 1** : Quelles sont les « bonnes clés » c'est-à-dire telles que deux lettres différentes sont codées par des lettres différentes ?

a. On se place dans le cas où $a = 3$ et $b = 5$.
i. Justifier l'existence d'un couple $(u ; v)$ d'entiers relatifs tel que $3u - 26v = 1$. Trouver un tel couple.
ii. Vérifier que 9 est solution de l'équation $3u \equiv 1$ [26].
iii. Démontrer en utilisant ii. que si $c(x) \equiv c(x')$ [26], alors $x \equiv x'$ [26].

b. Cas général
i. Montrer que pour trouver u tel que $au \equiv 1$ [26], il suffit de trouver un couple $(u ; v)$ tel que $au + 26v = 1$.
À quelle condition un tel couple existe-t-il ?
ii. En déduire que le codage affine est bon si et seulement si a et b sont premiers entre eux.
iii. En déduire le nombre de « bons » codages affines possibles.

3 **Question 2** : Trouver la fonction de décodage

a. Un exemple : on se place dans le cas où $a = 3$ et $b = 5$
i. Montrer que si $y \equiv 3x + 5$ [26] alors $x \equiv 9y + 7$ [26].
ii. Montrer que si $x \equiv 9y + 7$ [26], alors $y \equiv 3x + 5$ [26].
iii. En déduire la fonction de décodage.

b. Cas général
Trouver la fonction de décodage d'un chiffrement affine de clé $(a ; b)$ lorsque a est premier avec 26.

4 **Complément** :

a. Dans le cas où a et 26 sont premiers entre eux, on a trouvé u tel que $au \equiv 1$ [26].
i. En déduire que si a et 26 sont premiers entre eux et si $ab \equiv 0$ [26], alors $b \equiv 0$ [26].
ii. Traduire ce résultat en termes de divisibilité.

b. En déduire une généralisation, connue sous le nom de théorème de Gauss.

Un peu d'histoire...
Carl Friedrich Gauss (1777-1855), surnommé « le prince des mathématiques » publia dès 1801 un important ouvrage de théorie des nombres.



A PGCD de deux entiers

1 Diviseurs communs à deux entiers

Notation : Pour tous les entiers relatifs a et b, on note $D(a\ ;\ b)$ l'ensemble des diviseurs communs à a et b. On a donc $D(a\ ;\ b) = D(b\ ;\ a) = D(a) \cap D(b)$.

Exemple : $D(12) = \{-12\ ;\ -6\ ;\ -4\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 4\ ;\ 6\ ;\ 12\}$
et $D(18) = \{-18\ ;\ -9\ ;\ -6\ ;\ -3\ ;\ -2\ ;\ 1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 6\ ;\ 9\ ;\ 18\}$,
d'où $D(12\ ;\ 18) = \{-6\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 6\}$.

Remarques : Soient a et b deux entiers relatifs.

1. $D(a\ ;\ b) \subset D(b)$;
2. $D(a\ ;\ 0) = D(a)$;
3. $D(1\ ;\ a) = \{-1\ ;\ 1\}$;
4. $D(a\ ;\ b) = D(|a|\ ;\ |b|)$;
5. Si b divise a, alors $D(a\ ;\ b) = D(b)$.

Propriétés 1

Soient a et b deux entiers relatifs.

1. Pour tout entier relatif k, $D(a\ ;\ b) = D(a - kb\ ;\ b)$;
2. En particulier, $D(a\ ;\ b) = D(a - b\ ;\ b)$.

Soient maintenant a un entier relatif et b un entier naturel non nul.

3. Si r est le reste de la division euclidienne de a par b, alors $D(a\ ;\ b) = D(b\ ;\ r)$.

Note : Pour les démonstrations de ces propriétés, voir savoir-faire 1.

2 Définition et propriétés du PGCD

Propriété 2

Étant donnés deux entiers relatifs a et b non simultanément nuls, l'ensemble des diviseurs communs de a et b admet un plus grand élément.

Démonstration : On suppose $b \neq 0$. $D(a\ ;\ b)$ est une partie de $\mathbb{Z}$ non vide (elle contient 1) et majorée par $|b|$. On en déduit que $D(a\ ;\ b)$ admet un plus grand élément.

Définition 1

Étant donnés deux entiers relatifs a et b non simultanément nuls, le plus grand élément de l'ensemble des diviseurs communs de a et b est appelé plus grand diviseur commun de a et b. On le note $PGCD(a\ ;\ b)$.

Exemple : $D(12\ ;\ 18) = \{-6\ ;\ -3\ ;\ -2\ ;\ -1\ ;\ 1\ ;\ 2\ ;\ 3\ ;\ 6\}$, on en déduit $\text{PGCD}(12\ ;\ 18) = 6$.

Remarques : Soient a et b deux entiers relatifs tels que $b \neq 0$.

1. $PGCD(b\ ;\ 0) = |b|$;
2. $PGCD(a\ ;\ 1) = 1$;
3. $PGCD(a\ ;\ b) = PGCD(|a|\ ;\ |b|)$;
4. Si b divise a alors $PGCD(a\ ;\ b) = |b|$.
5. $PGCD(a\ ;\ b) = PGCD(b\ ;\ a)$.

Propriété 3

Soient a et b deux entiers relatifs tels que $b \neq 0$.

1. Pour tout $k \in \mathbb{Z}$, $\text{PGCD}(a\ ;\ b) = \text{PGCD}(a - kb\ ;\ b)$;
2. $\text{PGCD}(a\ ;\ b) = \text{PGCD}(a - b\ ;\ b)$.

Note : Pour les démonstrations des propriétés 3 et 4, voir savoir-faire 1.

Propriété 4

Lemme d'Euclide : Soient a un entier relatif et b un entier naturel non nul.
Si r est le reste de la division euclidienne de a par b, alors $\text{PGCD}(a\ ;\ b) = \text{PGCD}(b\ ;\ r)$.

Savoir-faire 1 Démontrer PGCD(a ; b) = PGCD($a - kb$; b)

→ Exercice corrigé 18 p. 61
→ Exercices d'application 19 à 22 p. 61

Énoncé

a, b et k sont des entiers relatifs.
a. Montrer $D(a\ ;\ b) = D(a - kb\ ;\ b)$.
b. En déduire PGCD(a ; b) = PGCD($a - kb$; b).
c. Si r est le reste de la division euclidienne de l'entier relatif a par l'entier naturel b, montrer alors que PGCD(a ; b) = PGCD(b ; r).

Méthode

a. Pour montrer l'égalité de deux ensembles A et B, montrer A ⊂ B et B ⊂ A.
b. Utiliser la définition du PGCD.

Solution

a. • Soit d, un diviseur commun à a et b. d divise toute combinaison linéaire à coefficients entiers de a et b, en particulier d divise $a - kb$. d est donc un diviseur commun à $a - kb$ et b, d'où $D(a\ ;b) \subset D(a - kb\ ;b)$.
• Soit d, un diviseur commun de $a - kb$ et b. d divise toute combinaison linéaire à coefficients entiers de $a - kb$ et b, en particulier d divise $(a - kb) + kb$, soit d divise a. d est donc un diviseur commun de a et b, d'où $D(a - kb\ ;b) \subset D(a\ ;b)$.
• En conclusion, $D(a\ ;\ b) = D(a - kb\ ;\ b)$.
b. Puisque $D(a\ ;\ b) = D(a - kb\ ;\ b)$, leurs plus grands éléments sont égaux, d'où PGCD(a ; b) = PGCD($a - kb$; b).
c. $r = a - bq$ avec $q \in \mathbb{Z}$, donc PGCD(a ; b) = PGCD($a - bq$; b) = PGCD(r ; b).

Savoir-faire 2 Calculer le PGCD de deux entiers $a(n)$ et $b(n)$

→ Exercice corrigé 30 p. 61
→ Exercices d'application 31 à 33 p. 61

Énoncé

Déterminer selon les valeurs de l'entier n le PGCD de $a = 2n + 1$ et $b = n - 6$.

Méthode

Utiliser la propriété PGCD(a ; b) = PGCD($a - kb$; b).

Solution

• On utilise la propriété PGCD(a ; b) = PGCD($a - kb$; b) ($k \in \mathbb{Z}$).
PGCD($2n + 1\ ;\ n - 6$) = PGCD($2n + 1 - 2(n - 6)\ ;\ n - 6$) = PGCD($13\ ;\ n - 6$).
• Le PGCD de a et b est donc le PGCD de $n - 6$ et de 13, il ne peut donc être égal qu'à 1 ou 13 et il n'est égal à 13 que si 13 divise $n - 6$, soit $n - 6 \equiv 0\ [13]$.
• En conclusion, le PGCD de a et b est égal à 13 lorsque $n \equiv 6\ [13]$ et à 1 dans les autres cas.

Savoir-faire 3 Montrer l'égalité de deux PGCD

→ Exercice corrigé 34 p. 610
→ Exercices d'application 35 p. 61

Énoncé

Soient a et b deux entiers non nuls. Montrer que PGCD($4a + 9$b ; $3a + 7$b) = PGCD(a ; b).

Méthode

Utiliser plusieurs fois la propriété PGCD(a ; b) = PGCD($a - kb$; b).

Solution

En utilisant la propriété PGCD(a ; b) = PGCD($a - kb$; b) ($k \in \mathbb{Z}$), on obtient successivement :
PGCD($4a + 9b$; $3a + 7b$) = PGCD($(4a + 9b) - (3a + 7b)$) = PGCD($a + 2b$; $3a + 7b$).
PGCD($a + 2b$; $3a + 7b$) = PGCD($a + 2b$; $3a + 7b - 3(a + 2b)$) = PGCD($a + 2b$; b)
PGCD($a + 2b$; b) = PGCD($a + 2b - 2b$; b) = PGCD(a ; b).
D'où PGCD($4a + 9b$; $3a + 7b$) = PGCD(a ; b).

3 Algorithme d'Euclide

Propriété 5

Soient a et b deux entiers naturels tels que $0 < b \leqslant a$.
L'algorithme suivant permet en un nombre fini d'étapes de calculer le PGCD de a et b :
1. Calculer le reste r de la division euclidienne de a par b.
2. Si $r = 0$, alors $PGCD(a\,;b) = b$, sinon remplacer a par b et b par r et revenir en 1.

Le PGCD de a et b est le dernier reste non nul.

Démonstration :

	Divisions euclidiennes	PGCD
On divise a par b	$a = bq_1 + r_1$ et $0 \leqslant r_1 < b$	$PGCD(a\,;b) = PGCD(b\,;r_1)$
$r_1 \neq 0$, on divise b par r_1	$b = r_1q_2 + r_2$ et $0 \leqslant r_2 < r_1$	$PGCD(b\,;r_1) = PGCD(r_1\,;r_2)$
$r_2 \neq 0$, on divise r_1 par r_2	$r_1 = r_2q_3 + r_3$ et $0 \leqslant r_3 < r_2$	$PGCD(r_1\,;r_2) = PGCD(r_2\,;r_3)$
• • •		
$0 \leqslant .... < r_3 < r_2 < r_1 < b$, est une suite strictement décroissante d'entiers naturels, donc en un nombre fini d'opérations, on obtient $r_n \neq 0$ et $r_{n+1} = 0$ (principe de la descente infinie)	$r_{n-2} = r_{n-1}q_n + r_n$ et $0 \leqslant r_n < r_{n-1}$ $r_{n-1} = r_nq_{n+1} + 0$	$PGCD(r_{n-2}\,;\,r_{n-1}) = PGCD(r_{n-1}\,;\,r_n)$ $PGCD(r_{n-1}\,;\,r_n) = PGCD(r_n\,;0) = r_n$

4 Conséquences

Propriété 6

Soient a et b deux entiers relatifs tels que $b \neq 0$.
L'ensemble de leurs diviseurs communs est l'ensemble des diviseurs de leur PGCD.

Démonstration : • 1er cas : a et b sont des entiers naturels : on utilise l'algorithme d'Euclide et on reprend les mêmes notations.
On a alors $D(a\,;b) = D(b\,;r_1) = D(r_1\,;r_2) = \ldots = D(r_n\,;0) = D(r_n)$.
Or $r_n = PGCD(a\,;b)$, d'où $D(a\,;b) = D(PGCD(a\,;b))$. L'ensemble des diviseurs communs de a et b est donc l'ensemble des diviseurs de leur PGCD.
• 2e cas : a et b sont des entiers relatifs, on utilise les propriétés :
$D(a\,;b) = D(|a|\,;|b|)$ et $PGCD(a\,;b) = PGCD(|a|\,;|b|)$.

Propriété 7

Homogénéité du PGCD
Soient a et b deux entiers relatifs tels que $b \neq 0$. Pour tout entier relatif non nul k, $PGCD(ka\,;kb) = |k|\,PGCD(a\,;b)$.

Démonstration :
• 1er cas : a et b sont des entiers naturels : on utilise l'algorithme d'Euclide du calcul du PGCD de a et de b. En multipliant par $|k|$ égalités et inégalités, on a l'algorithme d'Euclide du calcul du PGCD de $|k|a$ et $|k|b$.
On a donc $PGCD(|k|a\,;|k|b) = |k|r_n = |k|PGCD(a\,;b)$.
Or $PGCD(ka\,;kb) = PGCD(|ka|\,;|kb|) = PGCD(|k|a\,;|k|b)$.
On a donc $PGCD(ka\,;kb) = |k|\,PGCD(a\,;b)$.
• 2e cas : a et b sont des entiers relatifs $PGCD(ka\,;kb) = PGCD(|ka|\,;|kb|) = PGCD(|k||a|\,;|k||b|) = |k|PGCD(|a|\,;|b|) = |k|\,PGCD(a\,;b)$ d'après le 1er cas.

Savoir-faire 4 Calculer le PGCD avec l'algorithme d'Euclide

→ Exercice corrigé 36 p. 62
→ Exercices d'application 37 à 39 p. 62

Énoncé

Déterminer le PGCD de 8 856 et 1 676 par l'algorithme d'Euclide.

Méthode

Utiliser PGCD(a ; b) = PGCD(b ; r), où r est le reste de la division euclidienne de a par b.

Solution

$8\,856 = 1\,676 \times 5 + 476$	$0 \leqslant 476 < 1676$
$1\,676 = 476 \times 3 + 248$	$0 \leqslant 248 < 476$
$476 = 248 \times 1 + 228$	$0 \leqslant 228 < 248$
$248 = 228 \times 1 + 20$	$0 \leqslant 20 < 228$
$228 = 20 \times 11 + 8$	$0 \leqslant 8 < 20$
$20 = 8 \times 2 + 4$	$0 \leqslant 4 < 8$
$8 = 4 \times 2 + 0$	

Disposition pratique sur tableur

Division	a	b	r
1	8 856	1 676	476
2	1 676	476	248
3	476	248	228
4	248	228	20
5	228	20	8
6	20	8	4
7	8	4	0

PGCD(8 856 ; 1 676) = PGCD(1 676 ; 476) = PGCD(476 ; 248) = PGCD(248 ; 228) = PGCD(228 ; 20) = PGCD(20 ; 8) = PGCD(8 ; 4) = 4.

Savoir-faire 5 Recherche de diviseurs communs

→ Exercice corrigé 40 p. 62
→ Exercices d'application 41 à 44 p. 62

Énoncé

Soit b un entier naturel. En divisant 4 373 par b, on trouve pour reste 8 et en divisant 826 par b, on trouve pour reste 7. Déterminer b.

Méthode

Pour chercher un diviseur commun, chercher le PGCD, puis utiliser la propriété 6.

Solution

Soit b une solution $4\,373 = bq + 8$ et $0 \leqslant 8 < b$ et $826 = bq' + 70 \leqslant 7 < b$.
$4\,365 = bq$ et $819 = bq'$, b est donc un diviseur commun à 4 365 et 819, c'est donc un diviseur de leur PGCD. Or PGCD(4 365 ; 819) = 9.
Donc b est un entier naturel diviseur de 9 strictement supérieur à 8, d'où $b = 9$.
Réciproquement, on a $4\,373 = 9 \times 485 + 8$ et $826 = 9 \times 91 + 7$.
Il y a donc une seule solution : $b = 9$.

Savoir-faire 6 Le PGCD avec les TICE

→ Exercice corrigé 36 p. 62
→ Exercices d'application 37 à 39 p. 62

Énoncé

a. Retrouver avec la calculatrice le PGCD de 8 856 et 1 676.
b. Faire un algorithme calculant le PGCD de $a^{n+1} - 1$ et $a^n - 1$, pour a et n entiers naturels. Tester le sur différentes valeurs de a et n. Quelle conjecture faire ?

Méthode

Pour calculer PGCD(a ; b), on procède de la manière suivante :

TI	Math → NUM → pgcd(
Casio	OPT → F6 → F4(NUM) → F6 → F2 GCD(
Xcas	gcd(
scilab	pgcd(
Maxima	gcd

Solution

Entrer A, N
$A^{N+1} - 1 \to B$
$A^N - 1 \to C$
PGCD(B ; C) → D
Afficher D
Conjecture : Pour tout entier n, PGCD($a^{n+1} - 1$; $a^n - 1$) = $a - 1$.

B Entiers premiers entre eux

Définition 2

On dit que deux entiers relatifs non nuls sont premiers entre eux lorsque leur PGCD est égal à 1, ce qui est équivalent à dire que leurs seuls diviseurs communs sont 1 et –1.

Propriété 8

Soient a et b deux entiers relatifs non nuls.
$d = PGCD(a\ ;\ b)$ si, et seulement si, il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Démonstration : • d divise a et b, donc il existe deux entiers relatifs a' et b' tels que $a = da'$ et $b = db'$. Par homogénéité du PGCD : $d = \text{PGCD}(a\ ;\ b) = \text{PGCD}(da'\ ;\ db') = d.\ \text{PGCD}(a'\ ;\ b')$. Et puisque $d \neq 0$, $\text{PGCD}(a'\ ;\ b') = 1$.
• Réciproquement : si $\text{PGCD}(a'\ ;\ b') = 1$, alors
$\text{PGCD}(a\ ;\ b) = \text{PGCD}(da'\ ;\ db') = d\text{PGCD}(a'\ ;\ b') = d$.

Conséquence : Tout nombre rationnel s'écrit sous forme irréductible $\frac{a}{b}$, où a et b sont des entiers premiers entre *eux*.

C Le théorème de Bézout

1 Coefficients de Bézout

Propriété 9

Soient a et b deux entiers relatifs non nuls.
Si $D = \text{PGCD}(a,b)$, alors il existe un couple d'entiers relatifs (u, v) tel que $D = au + bv$.

Note :
Un tel couple, appelé couple de coefficients de Bézout de a et b, n'est pas unique.

Démonstration : On considère l'ensemble E des entiers naturels non nuls de la forme $ax + by$ où x et y sont des entiers relatifs.
• E est une partie non vide de $\mathbb{N}$ (elle contient $|a|$), donc E admet un plus petit élément d qui s'écrit donc sous la forme $d = au + bv$ (avec u et v entiers relatifs).
• D divise a et de b, donc divise $au + bv = d$. D'où $D \leqslant d$.
• On va montrer que d est un diviseur de a et b. La division euclidienne de a par d s'écrit : $a = dq + r$ avec $0 \leqslant r < d$. On en déduit $r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq)$.
r est s'écrit donc sous la forme $ax + by$ et vérifie $0 \leqslant r < d$. On en déduit que $r = 0$, car sinon d ne serait pas le plus petit élément de E. Donc $a = dq$ et d divise a. On démontre de même que d divise b.
• Donc d est un diviseur commun de a et b vérifiant $D \leqslant d$. D étant le plus grand diviseur commun, $D = d$.
• Puisque $D = d$, il existe donc deux entiers relatifs u et v tels que $D = au + bv$.

Remarque : Pour déterminer les coefficients de Bézout, on peut examiner les premiers multiples de a et b.

Exemple : • $\text{PGCD}(6\ ;\ 15) = 3$ et $3 = 6 \times 3 - 15 \times 1 = 15 \times 3 - 6 \times 7$.
• $\text{PGCD}(22\ ;\ 15) = 1$ et $1 = 15 \times 3 + 22 \times (-2)$.

Remarque : La réciproque est fausse. En effet, $15 \times 30 + 22 \times (-20) = 10$, mais $\text{PGCD}(15\ ;\ 22) \neq 10$.

Savoir-faire 7 Prouver que des entiers sont premiers entre eux

→ Exercice corrigé 49 p. 62
→ Exercices d'application 50 à 52 p. 62

Énoncé

a et b sont deux entiers premiers entre eux.
Montrer que $a + b$ est premier avec a et b.

Méthode

Montrer que leur PGCD est égal à 1 ou montrer que leurs seuls diviseurs communs sont 1 et – 1.

Solution

Méthode 1 : PGCD($a + b$; a) = PGCD($a + b - a$; a) = PGCD(b ; a) = 1.
Donc $a + b$ et a sont premiers entre eux.

Méthode 2 : Soit d le PGCD de $a + b$ et a. d divise donc $a + b$ et a, donc divise la différence $a + b - a$. Donc d est un diviseur de a et b et puisque a et b sont premiers entre eux $d = 1$, $a + b$ et a sont donc premiers entre eux. On montre de même que $a + b$ et b sont premiers entre eux.

Savoir-faire 8 Trouver deux entiers dont on connaît le PGCD

→ Exercice corrigé 57 p. 63
→ Exercices d'application 58 à 61 p. 63

Énoncé

Déterminer les entiers naturels a et b tels que $a + b = 60$ et PGCD(a ; b) = 15.

Méthode

Se ramener à la recherche de nombres premiers entre eux.

Solution

• On suppose que (a ; b) est une solution.
PGCD(a ; b) = 15, il existe donc des entiers a' et b' premiers entre eux tels que $a = 15a'$ et $b = 15b'$.
a et b étant des entiers naturels, a' et b' sont aussi des entiers naturels.
De plus, $a + b = 60$ implique $a' + b' = 4$.
a' et b' sont donc des entiers naturels premiers entre eux tels que $a' + b' = 4$. Il y a deux cas possibles : (a' ; b') = (1 ; 3) et (a' ; b') = (3 ; 1), d'où deux solutions possibles (a ; b) = (15 ; 45) et (a ; b) = (45 ; 15).

• On vérifie que ces deux couples sont solutions.

• Conclusion : les solutions sont les couples (15 ; 45) et (45 ; 15).

Savoir-faire 9 Calculer des coefficients de Bézout avec l'algorithme d'Euclide

→ Exercice corrigé 62 p. 63
→ Exercices d'application 63 à 66 p. 63

Énoncé

Pour $a = 155$ et $b = 55$, déterminer un couple (u ; v) d'entiers relatifs tels que $au + bv$ = PGCD(a ; b).

Solution

On a $a = 155$ et $b = 55$.

$155 = 55 \times 2 + 45$	$45 = 155 - 2 \times 55 = a - 2b$
$55 = 45 \times 1 + 10$	$10 = 55 - 45 = b - (a - 2b) = 3b - a$
$45 = 10 \times 4 + 5$	$5 = 45 - 4 \times 10 = (a - 2b) - 4(3b - a)$
$10 = 5 \times 2 + 0$	$= 5a - 14b$

Donc PGCD(155 ; 55) = 5 et $5 = ax5 + bx(-14)$. Le couple (u ; v) = (5 ; –14) vérifie $155u + 55v = 5$.

Méthode

Écrire l'algorithme d'Euclide pour calculer PGCD(a ; b), puis « en descendant cet algorithme » exprimer chaque reste en fonction de a et b.

2 Identité de Bézout

Propriété 10 Deux entiers relatifs non nuls a et b sont premiers entre eux si et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Démonstration : • Si a et b sont premiers entre eux, PGCD(a ; b) = 1, et d'après l'identité de Bézout, il existe deux entiers relatifs u et v tels que $1 = au + bv$.
• Réciproquement, s'il existe deux entiers relatifs u et v tels que $au + bv = 1$, alors tout diviseur commun de a et b divise $au + bv$, donc divise 1, donc est égal à 1 ou –1. Donc PGCD(a ; b) = 1 et a et b sont premiers entre eux.

D Le théorème de Gauss

1 Théorème de Gauss

Propriété 11 Soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et a est premier avec b alors a divise c.

Démonstration : Puisque a divise bc, il existe $k \in \mathbb{Z}$, tel que $bc = ak$.
Puisque a et b sont premiers entre eux, d'après le théorème de Bézout il existe deux entiers relatifs u et v tels que $au + bv = 1$.
De $au + bv = 1$, on déduit $c = cau + cbv = acu + akv = a(cu + kv)$
D'où $c = a(cu + kv)$ avec $cu + kv \in \mathbb{Z}$, donc a divise c.

Remarque : l'hypothèse « a et b sont premiers entre eux » est indispensable.

Contre-exemple : $14 \times 15 = 210$ et 6 divise 210 et pourtant 6 ne divise ni 14 ni 15.

2 Une conséquence du théorème de Gauss

Propriété 12 Soient a, b et c trois entiers relatifs non nuls. Si les deux entiers a et b divisent c et sont premiers entre eux alors leur produit ab divise c.

Démonstration : Puisque a divise c, il existe $k \in \mathbb{Z}$, tel que $c = ak$.
Puisque b divise c, il existe $k' \in \mathbb{Z}$, tel que $c = bk'$.
On en déduit $ak = bk'$, d'où a divise bk' et puisque a est premier avec b, d'après le théorème de Gauss, on en déduit que a divise k'.
Il existe donc $k'' \in \mathbb{Z}$ tel que $k' = ak''$ et puisque $c = bk'$, on a $c = bak''$, donc ab divise c.

Exemple : 1 450 860 est divisible par 10 et par 3, comme 10 et 3 sont premiers entre eux, on en déduit 1 450 860 est divisible par $10 \times 3 = 30$. De plus 1 450 860 est divisible par 11, donc 1 450 860 est divisible par 30 et 11 qui sont premiers entre eux, on en déduit donc que 1 450 860 est divisible par $30 \times 11 = 330$.

Remarque : L'hypothèse « a et b sont premiers entre eux » est indispensable.

Contre-exemple : 60 est divisible par 6 et 4 mais n'est pas divisible par leur produit $6 \times 4 = 24$.

TP Algorithmique 1 Algorithme d'Euclide



Objectif :
- *Savoir programmer l'algorithme d'Euclide.*

1 Rappel de l'Algorithme d'Euclide

Pour calculer le PGCD des entiers naturels a et b avec $a > b$, on utilise la séquence d'opérations ci-dessous :

(1) Diviser a par b ; obtenir le reste r.

(2) Si $r = 0$, alors l'algorithme se termine : PGCD(a ; b) = b.

(3) Si $r \neq 0$, remplacer a par b, b par r et recommencer à partir de (1).

Exécuter cet algorithme à la main pour calculer le PGCD de 513 et 350.

2 Programmation de cet algorithme :

a. Voici un algorithme en langage de programmation utilisant l'instruction Tant que. Vérifier cet algorithme pour a = 1 404 et b = 64. Peut-on l'appliquer avec a = 264 et b = 1 404 ?

Modifier cet algorithme en utilisant l'instruction qui calcule le reste de la division euclidienne de a par b (souvent notée MOD(a ; b))

b. Tester cet algorithme sur la calculatrice.

Algorithme	Commentaires	Famille TI	Famille Casio
Saisir a, b ; Tantque b ≠ 0 faire q = E(a/b) ; r = a - bq ; a = b ; b = r ; FinTantque Afficher a	**On saisit les valeurs de a et b** Début de la boucle calcul du quotient entier de a par b Calcul du reste Le nouveau dividende est b Le nouveau diviseur est r **On sort de la boucle, b = 0(= r)** a contient le PGCD (dernier reste non nul).	Prompt A,B While B≠0 ent (A/B) → Q A – B*Q → R B → A R → B End Disp A	« A » ? → A ↩ « B » ? → B ↩ While B≠0 ↩ Intg(A ÷ B) → Q ↩ A – B × Q → R ↩ B → A ↩ R → B ↩ WhileEnd ↩ A

3 Programmation de cet algorithme sur un tableur

Chaque ligne correspond à une division.

La 1re colonne donne les valeurs successives de a ;

la 2e colonne donne les valeurs successives de b.

En A1 et B1 on saisit les valeurs initiales de a et b.

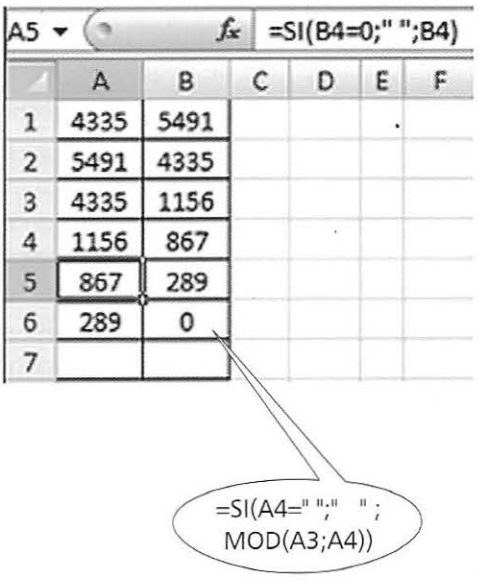
La ligne 2 est la ligne de calcul.

a. Quelles formules doit-on écrire en A2 et B2 ?

b. On recopie ensuite la ligne vers le bas. Quand s'arrête-t-on ? Où lit-on le PGCD ?

c. Faire fonctionner cet algorithme avec plusieurs valeurs.

d. Modifier les formules de la 2e ligne pour que l'affichage s'arrête tout seul dès que le reste est nul.



TP Algorithmique 2 Coefficients de Bézout



Objectif :
- *a, b étant des entiers naturels tels que $0 < b < a$, déterminer des coefficients de Bézout u et v tels que PGCD(a ; b) = au + bv.*

1 Exemple

Trouver u et v pour $a = 51$ et $b = 35$.

Indication : On écrit toutes les étapes de l'algorithme d'Euclide et à chaque étape on exprime le reste en fonction de a et b.

À la fin le dernier reste non nul qui est le PGCD sera écrit sous la forme $au + bv$.

2 Étude théorique : on utilise l'algorithme d'Euclide

				u	v	PGCD
	si b divise a					b
Division 1	$a = bq_2 + r_2$	$r_2 = a - bq_2$	$r_2 = au_2 + bv_2$	1	$-q_2$	
Division 2	$b = r_2q_3 + r_3$	$r_3 = b - r_2q_3 = b - (a - bq_2)q_3$	$r_3 = au_3 + bv_3$	$-q_3$	$1 + q_2q_3$	
Division 3	$r_2 = r_3q_4 + r_4$	$r_4 = r_2 - r_3q_4$	$r_4 = au_4 + bv_4$			
•••	•••	•••	•••	•••	•••	
Division n – 1	$r_{n-2} = r_{n-1}q_n + r_n$		$r_n = au_n + bv_n$			r_n
Division n	$r_{n-1} = r_nq_{n+1} + 0$					

On souhaite démontrer que, pour tout entier $k \geqslant 2$, il existe deux entiers relatifs u_k et v_k tels que $r_k = au_k + bv_k$ et trouver une formule de récurrence pour les calculer.

a. Vérifier que $u_2 = 1$ et $v_2 = -q_2$ et que $u_3 = -q_3$ et $v_3 = 1 + q_2q_3$.

b. Montrer par récurrence que pour tout $k \geqslant 4$, $u_k = u_{k-2} - u_{k-1}q_k$ et $v_k = v_{k-2} - v_{k-1}q_k$.

c. Montrer qu'en choisissant $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ et $v_1 = 1$, les formules permettent de retrouver les valeurs de u_2, v_2, u_3 et v_3.

d. Faire tourner cet algorithme à la main et vérifier que vous obtenez $1 = 11 \times 51 + (-16) \times 35$.

3 Mise en œuvre de cet algorithme sur le tableur

	A	B	C	D	E
1	r	q	u	v	commentaires: utiliser les fonctions quotient et mod
2	a		u_0	v_0	
3	b		u_1	v_1	
4					

La colonne A contient les restes successifs et la colonne B contient les quotients successifs.

Les colonnes C et D contiennent les valeurs successives des suites u et v.

Dans la ligne 4, on écrit les formules permettant de calculer le reste, le quotient et les coefficients u et v.

a. Initialisation : Remplir les cellules A2, A3, C2, C3, D3 et D4.

b. Ligne 4 de calcul : Quelles formules doit-on écrire dans les cellules A4 et B4 ? Pourquoi doit-on écrire la formule C2-C3*B4 dans la cellule C4 ?

Écrire de la même façon la formule qui convient dans la cellule D4.

c. Recopier les formules vers le bas. Quand doit-on s'arrêter ?

d. Faire fonctionner cet algorithme avec a = 51 et b = 35. Recommencer avec d'autres valeurs de a et b.

C4 ▾ f_x =C2-C3*$B4

	A	B	C	D
1	r	q	u	v
2	51		1	0
3	35		0	1
4	16	1	1	-1
5	3	2	-2	3
6	1	5	11	-16
7	0	3	-35	51

4 **Programmation de cet algorithme sur calculatrice**

Algorithme	Commentaires	Famille TI	Famille Casio
Saisir A, B $U_0 = 1$; $U_1 = 0$ $V_0 = 0$; $V_1 = 1$ TantQue B ≠ 0 faire $Q = E\left(\frac{A}{B}\right)$; $T = U_1$; $U_1 = U_0 - QU_1$; $U_0 = T$; … … R = A - BQ A = B ; B = R ; FinTantQue Afficher U_0, V_0, A A = B ;	$U_0 = U$, $U_1 = X$ $V_0 = V$, $V_1 = W$ Début de la boucle Pour affecter des nouvelles valeurs à U_0 et U_1 on utilise une variable auxiliaire T. Idem pour V_0 et V_1. Affectation des nouvelles valeurs de A et B Fin de la boucle Afficher U, V et le PGCD, A	Prompt A, B 1 → U : 0 → X 0 → V : 1 → W While B ≠ 0 ent(A/B) → Q X → T U – Q*X → X T → U : W → T V – Q*W → W T → V A – B*Q → R B → A : R → B End Disp "U", U "V", V, "PGCD", A	"A" ? → A : "B" ? → B ↩ 1 → U : 0 → X ↩ 0 → V : A → W ↩ While B = 0 ↩ Intg(A ÷ B) → Q ↩ X → T ↩ U – Q × X → X : T → U ↩ W → T ↩ V – Q × W → W : T → V ↩ A – B × Q → R : B → A : R → B ↩ WhileEnd ↩ "U" : U "V" : V "PGCD" : A

Commentaire

- On utilise 2 variables U_0 (ici U) et U_1 (ici X) pour stocker les valeurs successives de la suite (u_n).
- Un problème se pose sur une calculatrice : l'affectation $U_0 = U_1$ écrase le contenu de U_0 et U_0 ne contient plus la bonne valeur pour l'affectation $U_1 = U_0 - QU_1$. On utilise une variable auxiliaire T pour effectuer l'affectation $\begin{pmatrix} U_0 \\ U_1 \end{pmatrix} = \begin{pmatrix} U_1 \\ U_0 = QU_1 \end{pmatrix}$: $T = U_0$; $U_0 = U_1$; $U_1 = T - QU_1$.

On fait de même pour la suite (v_n) avec les mêmes variables V_0, V_1 et la même variable auxiliaire T.

a. Où sont stockés les restes ? Quelle est la variable auxiliaire utilisée pour faire les affectations de ces variables ?

b. Compléter l'algorithme ci-dessus, puis l'installer et l'exécuter sur votre calculatrice.

TP TICE 1 Quel est le nombre de billes ?

Objectifs :
- *Utiliser un tableur pour conjecturer les solutions d'un système.*
- *Démontrer cette conjecture.*

Un enfant dispose de n billes. S'il distribue équitablement les billes à 5 camarades, il reste 3 billes. S'il distribue équitablement les billes à 7 camarades, il reste alors 2 billes. Est-il possible de déterminer n ?

1 **a.** À l'aide d'un tableur, déterminer les restes des divisions euclidiennes par 5 et par 7 des entiers naturels inférieurs ou égaux à 1 000.

b. Quels entiers inférieurs ou égaux à 1 000 vérifient les conditions exposées ?

2 Montrer que le problème revient à trouver un entier naturel n tel que

$$(S)\begin{cases} n \equiv 3\,[5] \\ n \equiv 2\,[7] \end{cases} \text{ ou } \begin{cases} n = 5k + 3 \quad \text{avec } k \in \mathbb{Z} \\ n = 7k' + 2 \quad \text{avec } k' \in \mathbb{Z} \end{cases}.$$

a. Soit n un entier relatif solution du système (S).

i. Montrer qu'alors $7k' - 5k = 1$.

ii. Déterminer tous les couples $(k\ ;\ k')$ d'entiers relatifs solutions de l'équation $7k' - 5k = 1$.

iii. En déduire qu'il existe un entier relatif p tel que $n = -12 + 35p$.

b. Réciproquement, montrer que si $n = -12 + 35p$ où p est un entier relatif, alors n est solution du système.

3 **a.** Vérifier la conjecture émise à la question **1.**
b. Sachant qu'il y a moins de 100 billes, peut-on déterminer le nombre de billes ?

TP TICE 2 Codage et décodage

Objectifs :
- *Revoir le principe d'un codage affine.*
- *Utiliser le théorème de Gauss pour montrer que deux lettres distinctes sont codées par deux lettres distinctes.*
- *Utiliser le théorème de Bézout pour trouver la fonction de décodage.*

On utilisera le codage informatique des lettres avec le code ASCII.
Le message choisi est une citation (McLaughlin 1913-1983).

1 Expérimentation

Commentaire

En informatique, le code ASCII consiste à associer à chaque caractère (lettre de l'alphabet, chiffre, signe de ponctuation, ...) un code numérique n tel que $0 \leqslant n \leqslant 255$ appelé code ASCII.
Syntaxe : Dans la plupart des tableurs, la fonction « code » renvoie le code ASCII. La fonction réciproque est notée car ; exemple : code("A") renvoie le nombre 65 et « = car(65) » renvoie la lettre A.

a. Codage

i. Pour coder le message suivant : « Dans l'arithmétique de l'amour, un plus un égale... » :

- Entrer le message en ligne 1 à partir de la cellule B1.
- Coder le message avec le code ASCII en ligne 2 à partir de la cellule B2.
- Crypter le message en ligne 3 par la fonction de cryptage C qui, à tout n entier appartenant à [0 ; 255] associe le reste $C(n)$ de la division de $7n$ par 256.

Le tableau ci-dessous donne le début de la phrase et du codage à obtenir :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	message	D	a	n	s		l	'	a	r	i	T	h	m
2	Code ASCII	68	97	110	115	32	108	39	97	114	105	116	104	109
3	Message codé	220	167	2	37	224	244	17	167	30	223	44	216	251

Reproduire ce tableau sur un tableur et complétez-le.

b. Décodage à l'aide de la clef secrète

La fin de cette citation est cryptée par : 244 224 223 2 202 223 2 223 224 195 44 224 188 195 51 72 224 251 9 223 2 37 224 51 2 224 95 209 167 244 224 86 95 30 9
Pour décoder la fin de cette citation, on note D la fonction de décodage qui, à tout entier k appartenant à [0 ; 255], associe le reste de la division de 183k par 256.
Entrer en ligne 4 les nombres codés ci-dessus, puis en ligne 5, utiliser la fonction D pour trouver le code ASCII et enfin sur une nouvelle ligne, à l'aide de la fonction CAR, lire la fin de la citation.

2 Justifications

a. Justification du codage

Pour le codage ASCII, deux lettres de l'alphabet sont codées par deux nombres distincts. Il faut s'assurer que le cryptage choisi au **1.a** code deux nombres n et p distincts, compris entre 0 et 255, par deux nombres distincts.

i. Montrer que, si $C(n) = C(p)$, alors $7(n - p) \equiv 0$ modulo 256.
ii. En déduire que $n = p$. Justifier alors que le codage est valide.

b. Explication du décodage

La fonction de codage est définie par $C(n) \equiv 7n[256]$ et $0 \leqslant C(n) \leqslant 255$. Le décodage consiste donc, connaissant $C(n)$, à trouver n tel que $C(n) \equiv 7n[256]$ et $0 \leqslant n \leqslant 255$.

i. Déterminer un entier u tel que $0 \leqslant u \leqslant 255$ et $7u \equiv 1[256]$.
ii. En déduire $u \times (7n) \equiv n$ modulo 256.
iii. Expliquer pourquoi la fonction D, qui associe à k le reste de la division de $183k$ par 256, assure le décodage attendu.

Maîtriser le cours

Définition et propriétés du PGCD

1 **a.** Déterminer l'ensemble $D(44)$ des diviseurs de 44 et l'ensemble $D(154)$ des diviseurs de 154.
b. En déduire l'ensemble des diviseurs communs de 44 et 154, puis le PGCD de 44 et 77.

2 **a.** Vérifier l'égalité : $117 \times 8 - 85 \times 11 = 1$.
b. En déduire les diviseurs communs de 117 et 85, puis le PGCD de 117 et 85.

3 **a.** Démontrer la propriété $PGCD(a ; b) = PGCD(a - b ; b)$.
b. En appliquant plusieurs fois cette propriété, calculer PGCD(216 ; –168).

4 **a.** Démontrer la propriété $PGCD(a ; b) = PGCD(a - kb ; b)$.
b. Soit n un entier naturel. En utilisant la propriété précédente, montrer que $PGCD(3n + 2 ; n - 3) = PGCD(11 ; n - 3)$. En déduire les valeurs possibles de ce PGCD.

5 La proposition $PGCD(a ; b) = PGCD(a - c ; b - c)$ est-elle vraie ? Justifier la réponse.

6 n est un entier naturel non nul.
a. Vérifier que $(3n + 5) - 3(n + 2) = -1$.
b. En déduire $PGCD(3n + 5 ; n + 2)$.

Algorithme d'Euclide et conséquences

7 **a.** Rappeler l'algorithme d'Euclide.
b. En utilisant l'algorithme d'Euclide, calculer PGCD(1 320 ; 825).
c. En utilisant l'algorithme d'Euclide, montrer que 1 849 et 1 517 sont premiers entre eux.

8 Retrouver les PGCD de l'exercice 7 avec la calculatrice.

9 Un philatéliste possède 1 320 timbres français et 825 timbres étrangers. Il souhaite vendre toute sa collection en réalisant des lots identiques, c'est-à-dire ayant le même nombre de timbres et la même répartition de timbres français et de timbres étrangers. On souhaite trouver le nombre de lots possibles.
a. On note n le nombre de lots identiques. Justifier que n est un diviseur commun de 1 320 et 825.
b. Quelle propriété utiliser pour en déduire les différentes valeurs possibles de n ? Conclure.

10 **a.** Compléter, pour a, b et c entiers naturels : $PGCD(ac ; bc) = \ldots$
b. Utiliser l'égalité précédente pour en déduire : $PGCD(2\,012 \times 11 ; 2\,012 \times 12)$.
c. Calculer de même PGCD(50 ; –120).

Théorème de Bézout et théorème de Gauss

11 **a.** Énoncer le théorème de Bézout.
b. De l'égalité $117 \times 8 - 85 \times 11 = 1$, déduire toutes les paires possibles d'entiers premiers entre eux.

12 On suppose que a est premier avec b et c.
a. Traduire en utilisant le théorème de Bézout que les entiers a et b sont premiers entre eux.
b. Faire de même pour les entiers a et c.
c. Multiplier membre à membre ces égalités et justifier que a et bc sont premiers entre eux.

13 **a.** Le théorème de Bézout étant admis, énoncer et démontrer le théorème de Gauss.
b. Démontrer la conséquence suivante : si un entier a est divisible par deux entiers b et c premiers entre eux alors a est divisible par leur produit bc.
c. Donner un exemple d'application de la propriété précédente.

14 En utilisant le théorème de Gauss, résoudre les équations suivantes :
a. $5x = 7y$; **b.** $18x = 27y$;
c. $5(x - 2) = 7(y + 3)$; **d.** $21(x + 5) = 18y$.

15 On suppose qu'un entier relatif x vérifie les conditions : $x \equiv 3$ [5] et $x \equiv 3$ [7].
a. Montrer que $x \equiv 3$ [35].
b. En déduire qu'il existe un entier k tel que $x = 3 + 35k$.

16 **Vrai ou Faux**
Si x est un entier relatif tel que $x \equiv 3$ [10] et $x \equiv 3$ [6] alors :
a. $x - 3$ est divisible par 60. **b.** $x - 3$ est divisible par 30
c. $x = 3 + 30k$, où k est un entier relatif.

17 **Vrai ou Faux**
Si a et b sont deux entiers premiers entre eux, alors :
a. $a + b$ et $a - b$ sont premiers entre eux.
b. $a + b$ est premier avec a et b.
c. $a + b$ est premier ab. **d.** a est premier avec b^2.
e. a est premier avec b^n (n entier naturel non nul).
f. a^p est premier avec b^n (où n et p sont des entiers naturels non nuls).
g. tout diviseur de a est premier avec b.

Appliquer les capacités attendues

PGCD

Utiliser les propriétés 2 [savoir-faire 1 p. 49]

18 **a.** a et b sont des entiers relatifs non nuls. Démontrer que l'ensemble des diviseurs communs de a et b est égal à l'ensemble des diviseurs communs de $a - 6b$ et b.
b. Que peut-on en déduire en termes de PGCD ?

19 **a.** Soit une égalité triviale : 1 635 – 1 633 = 2.
En déduire les diviseurs communs possibles de 1 635 et 1 633.
b. En utilisant un argument de parité, en déduire les diviseurs communs de 1 635 et 1 633.
c. En déduire le PGCD de 1 635 et 1 633.

20 Soient deux entiers consécutifs $a = n$ et $b = n + 1$.
a. Déterminer leurs diviseurs communs.
b. En déduire leur PGCD.
c. Énoncer le résultat démontré.

21 Soient deux entiers pairs consécutifs $a = 2n$ et $b = 2n + 2$.
a. En utilisant l'égalité $a - b = 2$, déterminer les diviseurs communs de a et b.
b. En déduire le PGCD de a et b.
c. Énoncer le résultat démontré.

22 n est un entier naturel.
On considère les entiers $a = n + 2$ et $b = 3n + 1$.
a. Démontrer que si un entier d divise a et b, alors d divise 5.
b. En déduire les valeurs possibles du PGCD de a et b.

Utiliser la définition du PGCD [cours partie A p. 48]

23 Soient $a = 1\,320$ et b un entier naturel tel que PGCD(a ; b) = 66 et $400 < b < 700$.
Déterminer les valeurs de b.

24 Déterminer les entiers naturels non nuls a tels que : PGCD(225 ; a) = 75 et $a < 225$.

Utiliser les différences successives

25 **a.** Soient a et b des entiers relatifs non nuls.
Démontrer PGCD(a ; b) = PGCD($a - b$; b)
b. Calculer par la méthode des différences successives le PGCD de $a = 616$ et $b = 280$.

26 Calculer par la méthode des différences successives le PGCD de $a = 620$ et $b = 452$.

27 **a.** Montrer PGCD(275 ; 134) = PGCD(7 ; 134).
b. Vérifier que 7 ne divise pas 134 et en déduire PGCD(275 ; 134).

28 Déterminer PGCD(257 ; 123).

29 **a.** Que fait cet algorithme ?
b. Faire tourner cet algorithme sur votre calculatrice.
c. Calculer avec cet algorithme PGCD(432 ; 168).

```
Entrer a,b
c = 1
TantQue c ≠ 0 faire
c = abs(a - b) ;
a = b ;
b = c ;
Fin TantQue
Afficher abs(b)
```

Calculer le PGCD de $a(n)$ et $b(n)$ [savoir-faire 2 p. 49]

30 n est un entier naturel non nul.
a. Démontrer PGCD(n ; $3n + 7$) = PGCD(n ; 7).
b. Déterminer PGCD(n ; $3n + 7$) lorsque n est un multiple de 7.
c. Déterminer PGCD(n ; $3n + 7$) lorsque n n'est pas un multiple de 7.

31 n est un entier naturel. Déterminer suivant les valeurs de n, les valeurs de PGCD(n ; $3n + 13$).

32 n est un entier naturel. Soient $a = 5n + 4$ et $b = 3n - 1$.
a. Montrer PGCD(a ; b) = PGCD($-n + 6$; $3n - 1$).
b. Montrer PGCD($3n - 1$; $-n + 6$) = PGCD(17 ; $-n + 6$).
c. En déduire PGCD(a ; b) = PGCD(17 ; $-n + 6$)
d. Quelles sont les valeurs possibles de PGCD(a ; b) ?
e. En déduire les valeurs de PGCD(a ; b) en fonction des valeurs de n.

33 n est un entier naturel. $a = 2n + 15$ et $b = n + 3$
a. Montrer que PGCD(a ; b) = PGCD(9 ; $n + 3$).
b. i. Montrer que PGCD(a ; b) = 9 si, et seulement si, $n \equiv 6[9]$
ii. Montrer que PGCD(a ; b) = 3 si, et seulement si, $n \equiv 0$ [9] ou $n \equiv 3$ [9].
iii. Déterminer les valeurs de n telles que PGCD(a ; b) = 1.

Montrer l'égalité de deux PGCD [savoir-faire 3 p. 49]

34 a et b sont deux entiers naturels non nuls.
On pose $A = 2a + b$ et $B = 3a + b$.
Montrer que PGCD(A ; B) = PGCD(a ; b).

35 a et b sont deux entiers naturels non nuls
On pose $A = 5a + 9b$ et $B = 4a + 7b$.
a. Montrer que PGCD(A ; B) = PGCD(a ; b)
b. Retrouver ce résultat en montrant que tout diviseur commun de a et b est un diviseur commun de A et B et que tout diviseur commun de A et B est un diviseur commun de a et b.

Algorithme d'Euclide et applications

Calculer le PGCD avec l'algorithme d'Euclide [savoir-faire 4 p. 51] et vérifier avec la calculatrice [savoir-faire 6 p. 51]

Pour les exercices **36** à **39**, à l'aide de l'algorithme d'Euclide, calculer PGCD(a ; b) dans chacun des cas suivants et vérifier le résultat avec la calculatrice.

36 **a.** $a = 2\,400$ et $b = 210$; **b.** $a = 660$ et $b = 792$; **c.** $a = 128$ et $b = 48$.

37 **a.** $a = 455$ et $b = 312$; **b.** $a = 276$ et $b = 978$; **c.** $a = 1\,938$ et $b = 589$.

38 **a.** $a = 2\,011$ et $b = 2\,001$; **b.** $a = 6\,002$ et $b = 2\,006$; **c.** $a = 1\,515$ et $b = 1\,918$.

39 **a.** Montrer que $2^{21} = 2^{12} \times 2^9$.
b. En déduire que $2^{21} - 1 = (2^{12} - 1)2^9 + 2^9 - 1$.
c. En déduire que PGCD($2^{21} - 1$; $2^{12} - 1$) = PGCD1($2^{12} - 1$; $2^9 - 1$).
d. Recommencer et en déduire à l'aide de l'algorithme d'Euclide, le PGCD(a ; b) pour $a = 2^{21} - 1$ et $b = 2^{12} - 1$.

Rechercher des diviseurs communs [savoir-faire 5 p. 51]

40 Déterminer les diviseurs communs positifs de : $a = 2\,574$ et $b = 630$.

41 Même énoncé que **49** pour : $a = -2\,420$ et $b = 1\,716$.

42 Soit n un entier naturel tel que, quand on divise 2 790 par n, on obtient pour reste 7, et quand on divise 2 657 par n, le reste est 6.
a. Démontrer que n est un diviseur commun à 2 783 et 2 651.
b. Déterminer n.

43 Soit n un entier naturel tel que, quand on divise 2 380 et 2 215 par n, on obtient le même reste 10. Déterminer n.

44 Monsieur Bricolage veut daller sa terrasse de 2,10 m sur 3,60 m avec des carreaux carrés les plus grands possibles et dont la mesure d'un côté est un nombre entier de centimètres.
Quelle est, en cm, la mesure du côté du carreau choisi ?



Utiliser l'homogénéité [propriété 7 p. 50]

45 Déterminer sans calculatrice le PGCD de a et b dans chacun des cas suivants :
a. $a = -240 \times 17$ et $b = 240 \times 9$.
b. $a = 4\,000$ et $b = 700$.
c. $a = 3\,600$ et $b = 21\,000$.

46 m et n sont deux entiers naturels non nuls.
a. Montrer PGCD(m ; $3m + 1$) = 1
b. En déduire PGCD(nm ; $n(3m + 1)$).

47 n est un entier naturel non nul.
On pose $a = n^2 + 5n$ et $b = n^2 + 7n + 10$.
a. Factoriser a et b.
b. En distinguant les cas n pair et n impair, déterminer PGCD(n ; $n + 2$).
c. Déterminer alors PGCD(a ; b) en fonction de n.

48 n est un entier naturel non nul.
Calculer PGCD($5n^2 + 4n$; $4n^2 + 3n$).

Nombres premiers entre eux

Prouver que des entiers sont premiers entre eux [savoir-faire 7 p. 53]

49 **Vrai ou faux**. Justifier votre réponse.
Soient a et b deux entiers naturels.
a. Si a et b sont premiers entre eux, alors $a + b$ et $a - b$ sont premiers entre eux.
b. Si $a + b$ et $a - b$ sont premiers entre eux, alors a et b sont premiers entre eux.

50 Soient a et b des entiers naturels. On pose $A = 2a + 5b$ et $B = 3a + 7b$.
a. Montrer que si d divise a et b, d divise A et B.
b. Vérifier que $3A - 2B = b$.
c. Trouver de même une relation donnant a en fonction de A et B.
d. Montrer que si d divise A et B, alors d divise a et b.
e. Montrer que a et b sont premiers entre eux si et seulement si A et B le sont aussi.

51 a, b et c sont des entiers naturels non nuls tels que a est premier avec b et c.
a. Montrer que tout diviseur commun de a et bc est un diviseur de PGCD(ac ; bc).
b. En déduire que tout diviseur commun de a et bc est un diviseur de c.
c. En déduire que a est premier avec bc.

52 a et b sont deux entiers naturels.

a. Montrer que si a et b sont premiers entre eux, alors $a + b$ est premier avec a et b.
b. En déduire que si a et b sont premiers entre eux, alors $a + b$ et ab sont premiers entre eux.

Aide

Utiliser la technique et le résultat de l'exercice précédent.

Fractions irréductibles

53 n est un entier naturel.
a. Montrer que n et $3n + 1$ sont premiers entre eux.
b. En déduire que la fraction $\frac{n}{3n+1}$ est une fraction irréductible.

54 Soit n un entier naturel.
a. Montrer que $3n + 2$ et $6n + 5$ sont premiers entre eux.
b. En déduire que la fraction $\frac{3n+2}{6n+5}$ est irréductible.

55 n est un entier naturel non nul.
Démontrer que la fraction $\frac{9n+5}{7n+4}$ est irréductible.

56 Soit a et b deux entiers naturels non nuls.
a. Montrer que PGCD$(2a + 3b ; 5a + 7b)$ = PGCD$(a ; b)$.
b. En déduire que $\frac{2a+3b}{5a+7b}$ est irréductible si et seulement si $\frac{a}{b}$ est irréductible.

Trouver deux entiers dont on connaît le PGCD et une autre condition [savoir-faire 8 p. 53]

57 Déterminer tous les couples d'entiers naturels $(a ; b)$ tels que : $a + b = 210$ et PGCD$(a ; b) = 14$.

58 Déterminer tous les couples d'entiers naturels $(a ; b)$ tels que $a + b = 72$ et PGCD$(a, b) = 8$.

59 Déterminer tous les couples d'entiers relatifs $(a ; b)$ tels que PGCD$(a ; b) = 14$ $ab = 10\,780$.

60 Déterminer tous les couples d'entiers naturels $(a ; b)$ ayant pour PGCD 169 et dont le produit est égal à 856 830.

61 Déterminer tous les couples d'entiers naturels $(a ; b)$ tels que $a^2 - b^2 = 7\,695$ et PGCD$(a ; b) = 9$.

Théorème de Bézout

Calculer les coefficients de Bézout [savoir-faire 9 p. 53]

62 Montrer que 88 et 63 sont premiers entre eux et déterminer des entiers relatifs u et v tels que $88u + 63v = 1$.

63 Déterminer un couple d'entiers relatifs $(u ; v)$ tel que $83u + 47v = 1$.

64 **a.** Déterminer un couple d'entiers relatifs $(u ; v)$ tel que $936u + 275v = 1$.
b. En déduire un couple $(x ; y)$ d'entiers relatifs solution de l'équation $936x + 275y = 3$.

65 Soient $a = 155$ et $b = 65$.
a. À l'aide de l'algorithme d'Euclide, déterminer PGCD$(a ; b)$.
b. En déduire un couple d'entiers relatifs $(u ; v)$ tel que PGCD$(a ; b) = au + bv$.

66 Justifier que cet algorithme permet de trouver lorsque a et b sont des entiers premiers entre eux des entiers relatifs u et v tels que $au + bv = 1$.

```
Entrer a,b
u = 1
c = a
TantQue a n'est pas congru à 1 modulo b
u = u + 1
a = uc
Fin TantQue
v = (1 - a)/b
Afficher u,v
```

Utiliser le théorème de Bézout [savoir-faire 10 p. 55]

Pour les exercices **67** à **69**, utiliser l'identité de Bézout pour démontrer que a et b sont premiers entre eux.

67 **a.** $a = n$ et $b = 3n + 1$; **b.** $a = 2n + 1$ et $b = 3n + 1$.

68 **a.** $a = n^3 + 1$ et $b = n$;
b. $a = 2n(n + 3) + 1$ et $b = n + 3$.

Aide

Penser que les coefficients u et v peuvent être des fonctions de n.

69 **a.** $a = 3n + 7$ et $b = 2n + 5$; **b.** $a = 7n + 4$ et $b = 5n + 3$.

70 **a.** Utiliser le théorème de Bézout pour démontrer que si a et b^2 sont premiers entre eux alors a et b sont premiers entre eux.
b. Démontrer aussi la réciproque en utilisant le théorème de Bézout.

71 a et b sont des entiers strictement positifs tels que $(a^2 + ab - b^2)^2 = 1$.
Démontrer en utilisant le théorème de Bézout que a et b sont premiers entre eux.

72 Utiliser seulement le théorème de Bézout.
a et b sont deux entiers naturels premiers entre eux.

a. Vérifier que $au + bv = (a + b)u + b(v - u)$.
b. En déduire que $a + b$ et b sont premiers entre eux.
c. Démontrer que $a + b$ est premier avec a.
d. Que dire de $a + b$ et ab ?

Théorème de Gauss

Résoudre une équation du type $ax = b$

[cours, partie D p. 54]

73 On souhaite trouver tous les couples d'entiers relatifs $(a ; b)$ tels que $5a = 7b$.
a. On suppose qu'il existe des entiers a et b tels que $5a = 7b$, en déduire à l'aide du théorème de Gauss que 7 divise b et qu'il existe un entier relatif k tel que $b = 5k$ et $a = 7k$.
b. Étudier la réciproque et conclure.

74 Utiliser le théorème de Gauss pour résoudre dans $\mathbb{Z}^2$, l'équation $4(x - 2) = 5(y - 3)$.

75 Utiliser le théorème de Gauss pour résoudre dans $\mathbb{Z}^2$, l'équation $55(x + 2) = 10(y - 7)$.

Montrer une divisibilité à l'aide de la propriété 12

[cours, partie D p. 54]

76 **a.** En utilisant les critères de divisibilité et la propriété 12, démontrer que 38 808 est divisible par 18.
b. Démontrer que 38 808 est divisible par 198.

77 Soit n un entier naturel. On pose $a = n(n + 7)(n + 11)$.
Montrer que a est divisible par 2 et 3, puis par 6.

Équation $ax + by = c$

78 **a.** Démontrer que pour tout entier naturel n, $10^n \equiv 1$ [9].
b. En déduire que $10^n + 8$ est divisible par 9.
c. En déduire que $10^n + 8$ est divisible par 18.

Équation $ax + by = c$

Existence ou non d'une solution

79 **a.** Justifier l'existence d'une solution $(u ; v)$ dans $\mathbb{Z}$ de l'équation $9x - 14y = 1$.
b. En déduire l'existence d'une solution $(u_1 ; v_1)$ dans $\mathbb{Z}$ de l'équation $9x - 14y = 11$.
c. Justifier l'existence d'une solution dans $\mathbb{Z}$ de l'équation $18x - 28y = 6$.
d. Que penser de l'équation $18x - 28y = 3$?

80 Déterminer, s'il existe, un couple d'entiers relatifs solution pour chacune des équations :
a. $9x + 11y = 1$; **b.** $18x + 15y = 6$;
c. $7x + 12y = 3$. **d.** $18x + 15y = 8$.

81 En utilisant l'algorithme d'Euclide, déterminer un couple $(x ; y)$ d'entiers relatifs solution de l'équation : $41x + 12y = 1$.

82 En utilisant l'algorithme d'Euclide, déterminer un couple $(x_0 ; y_0)$ d'entiers relatifs solution de $77x + 50y = 1$.
En déduire un couple $(x_1 ; y_1)$ d'entiers relatifs solution de $77x + 50x = 5$.

Résoudre une équation du type $ax + by = c$

[savoir-faire 11 p. 55]

83 Soit l'équation (E) $4x - 3y = 2$.
a. Déterminer une solution évidente $(x_0 ; y_0)$ de l'équation (E).
b. Démontrer qu'un couple $(x ; y)$ d'entiers relatifs est solution de l'équation (E) si et seulement si $4(x - x_0) = 3(y - y_0)$.
c. En déduire tous les couples d'entiers relatifs solutions de l'équation (E).

84 Soit l'équation (E) : $8x + 5y = 1$
a. Déterminer un couple d'entiers relatifs $(x_0 ; y_0)$ solution de l'équation (E).
b. Démontrer qu'un couple $(x ; y)$ d'entiers relatifs est solution de l'équation (E) si et seulement si $8(x - x_0) = 5(y_0 - y)$.
c. En déduire toutes les solutions de l'équation (E).

85 **a.** Soit l'équation $23x - 13y = 1$
i. Justifier que cette équation admet une solution dans $\mathbb{Z}^2$.
ii. À l'aide de l'algorithme d'Euclide, déterminer une solution $(x_0 ; y_0)$.
b. En déduire une solution particulière de l'équation (E) $23x - 13y = 2$.
c. En déduire toutes les solutions de l'équation (E).

86 Le but de l'exercice est de résoudre dans $\mathbb{Z}^2$ l'équation $34x + 24y = 6$.
a. Montrer que cette équation est équivalente à l'équation (E) $17x + 12y = 3$.
b. Déterminer une solution de l'équation (E_0) $17x + 12y = 1$.
c. En déduire une solution de l'équation (E).
d. En déduire tous les couples $(x ; y)$ d'entiers relatifs solutions de l'équation (E).
e. Déterminer tous les couples $(x ; y)$ d'entiers naturels solutions de l'équation (E).

87 **Vrai-faux**

L'exercice propose cinq affirmations numérotées de 1 à 5. Pour chacune de ces affirmations, dire si elle est vraie ou si elle est fausse, en justifiant le choix effectué.

1. Si un nombre est divisible par 4, alors il est divisible par 8.
2. Si un nombre est divisible par 2 et par 3, alors il est divisible par 6.
3. Si un nombre est divisible par 4 et par 6, alors il est divisible par 24.
4. Si deux entiers a et b sont premiers entre eux, les entiers $a + b$ et $a - b$ sont nécessairement premiers entre eux.
5. Si deux entiers a et b sont premiers entre eux, les entiers $2a + b$ et $3a + 2b$ sont nécessairement premiers entre eux.

88 **QCM**. Pour chaque question indiquer si les propositions sont justes ou fausses.

1. Soient a et b deux entiers naturels.

a. S'il existe deux entiers relatifs u et v tels que $au + bv = 3$, alors PGCD$(a ; b) = 3$.

b. Si PGCD$(a ; b) = 3$, alors il existe deux entiers relatifs u et v tels que $au + bv = 3$.

c. S'il existe deux entiers relatifs u et v tels que $au + bv = 1$, alors PGCD$(a ; b) = 1$.

d. Si PGCD$(a ; b) = 1$, alors il existe deux entiers relatifs u et v tels que $au + bv = 1$.

2. On considère les deux équations (E) $3x - 5y = 1$ et (E') : $3x - 5y = 2$.

a. Si $(u ; v)$ est une solution dans Z de (E), alors $(2u ; 2v)$ est solution dans Z de (E').

b. Les solutions dans Z de (E') sont des couples d'entiers pairs.

c. Si $(u ; v)$ est une solution dans Z de (E), alors $u \equiv 1$ [3].

d. Si $(u ; v)$ est une solution dans Z de (E), alors $v \equiv 1$ [3].

3. Soient a, b, c trois entiers naturels deux à deux distincts.

a. si a divise bc, alors a divise b et a divise c.

b. Si d = PGCD $(a + b ; c)$, alors d divise a et d divise b.

c. Si d = PGCD $(a + b ; a + c)$, alors d divise b et d divise c.

d. Si d = PGCD $(a + b ; a + c)$, alors d divise $b - c$.

PGCD et nombres premiers entre eux

Algorithmique

89 Le nombre n est un entier naturel non nul. On pose : $a = 4n + 3$, $b = 5n + 2$ et on note d le PGCD de a et b.

1. Que fait cet algorithme ? Donner plusieurs valeurs à N, puis conjecturer les valeurs possibles de D.

```
Entrer N
A = 4N + 3, B = 5N + 2
D = PGCD(A, B)
Afficher D
```

2. Calculer $5a - 4b$ et en déduire les valeurs possibles de d.
3. **a.** Déterminer les entiers naturels n et k tels que $4n + 3 = 7k$.

b. Déterminer les entiers naturels n et k tels que $5n + 2 = 7k$.

4. Soit r le reste de la division euclidienne de n par 7. Déduire des questions précédentes la valeur de r pour laquelle d vaut 7. Pour quelles valeurs de r, d est-il égal à 1 ?

90 Soit n un entier naturel, $a = 5n + 4$, $b = 2n + 1$.

a. À l'aide de la calculatrice ou d'un tableur, dire quel semble être PGCD $(a ; b)$.

b. Soit d un diviseur commun à a et b. Montrer que d divise 3.

c. Montrer que a est congru à b modulo 3.

Pour quelles valeurs de n, PGGCD$(a ; b) = 3$?

91 Soit n un entier naturel, $a = 5n^2 + 7$, $b = n^2 + 1$.

a. À l'aide de la calculatrice ou d'un tableur, dire quel semble être PGCD $(a ; b)$.

b. Soit d un diviseur commun à a et b. Montrer que d divise 2.

c. Pour quelles valeurs de n, PGGCD$(a ; b) = 2$?

92 **a.** Déterminer suivant les valeurs de n, PGCD$(3n ; n + 1)$.

b. En déduire PGCD$(6n^2 ; 2n(n + 1))$

93 Soit n un entier naturel supérieur ou égal à 2.

a. Montrer que PGCD $(n + 10 ; n - 2)$ = PGCD$(n - 2 ; 12)$.

b. Déterminer les valeurs possibles de PGCD $(n + 10 ; n - 2)$

c. Si PGCD $(n + 10 ; n - 2) = 12$, quelles sont les valeurs possibles de n ?

d. Pour quelles valeurs de n la fraction $\frac{n+10}{n-2}$ est-elle irréductible ?

94 1. **a.** Montrer que, pour tout entier naturel n, $3n^3 - 11n + 48 = (n + 3)(3n^2 - 9n + 16)$

b. Montrer que, pour tout entier naturel n, $3n^2 - 9n + 16$ est un entier naturel non nul.

2. Montrer que, pour tous les entiers naturels non nuls a, b et c, l'égalité suivante est vraie : PGCD$(a ; b)$ = PGCD$(bc - a ; b)$.
3. Montrer que, pour tout entier naturel n, supérieur ou égal à 2, l'égalité suivante est vraie : PGCD$(3n^3 - 11n ; n + 3)$ = PGCD$(48 ; n + 3)$.
4. **a.** Déterminer l'ensemble des diviseurs entiers naturels de 48.

b. En déduire l'ensemble des entiers naturels n tels que $\frac{3n^3 - 11n}{n+3}$ soit un entier naturel.

95 Pour tout entier naturel n supérieur ou égal à 5, on considère les nombres $a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$.

1. En utilisant l'algorithme d'Euclide, déterminer PGCD (a ; b) pour $n = 11$ et $n = 12$.
2. Montrer, après factorisation, que a et b sont des entiers naturels divisibles par $n - 4$.
3. On pose $\alpha = 2n + 1$ et $\beta = n + 3$ .On note d le PGCD de α et β.
a. Démontrer que d est un diviseur de 5.
b. Démontrer que les nombres α et β sont multiples de 5 si et seulement si $n - 2$ est multiple de 5.
4. Déterminer PGCD (a ; b) suivant les valeurs de n.

96 Soit n un entier naturel non nul, on considère les entiers suivants : $N = 9n + 1$ et $M = 9n - 1$.
On pose $d(n) = PGCD(M ; N)$
1. Montrer que $d(n)$ divise 2. Quelles sont les valeurs possibles de $d(n)$?
2. Dans cette question, n est pair.
Quelle est la parité de N ? En déduire $d(n)$.
3. Dans cette question, n est impair.
Quelle est la parité de N ? En déduire $d(n)$.
4. Pour tout entier naturel non nul n, on considère l'entier $81n^2 - 1$.
a. Exprimer l'entier $81n^2 - 1$ en fonction des entiers M et N.
b. Démontrer que $81n^2 - 1$ est divisible par 4 si et seulement si n est impair.

Algorithmique

97 Soit c un entier naturel supérieur ou égal à 2.
On pose pour tout entier naturel a non nul,
$C(n) = c^n - 1$ et $d_C(n) = PGCD(C(n + 1) ; C(n))$.

```
Algorithme
Entrer c,n
cn + 1 - 1 → a
cn - 1 → b
   Tant que b≠0
   E(a/b) → q
   a - bq → r
   b → a
   r → b
Fin Tant que
Afficher a
```

1. Justifier que cet algorithme donne les valeurs de $d_C(n)$ pour c et n fixés.
2. Conjecturer la valeur de $d(n)$ en fonction de c et n.
3. Pour quelle valeur de c, $C(n + 1)$ et $C(n)$ sont-ils premiers entre eux ?
4. Soit d_C la valeur conjecturée en 2.
a. Montrer que quel que soit n, d_C divise $C(n)$. En déduire que d_C divise $d_C(n)$
b. Montrer qu'il existe deux entiers naturels a et b tels que : $aC(n) - b\,C(n + 1) = d_C$. En déduire $d_C(n)$.
5. Quel est le PGCD de $2012^{2013} - 1$ et de $2012^{2012} - 1$?

98 On se propose d'étudier des couples (a ; b) d'entiers strictement positifs, tels que : $a^2 = b^3$.
1. Soit k un entier naturel non nul. Vérifier que le couple (k^3 ; k^2) répond à la question.
2. Soit (a ; b) un tel couple et $d = PGCD(a ; b)$. On note u et v les entiers tels que $a = du$ et $b = dv$.
a. Montrer que $u^2 = dv^3$.
b. En déduire que v divise u, puis que $v = 1$.
3. Soit (a ; b) un couple d'entiers strictement positifs. Démontrer que l'on a $a^2 = b^3$ si et seulement si a et b sont respectivement le cube et le carré d'un même entier.
4. Montrer que si n est le carré d'un nombre entier naturel et le cube d'un autre entier, alors $n \equiv 0$ [7] ou $n \equiv 1$ [7].

Nombres premiers entre eux et théorème de Bézout

99 **a.** Montrer, en utilisant le théorème de Bézout, que si a est premier avec b et c, il est premier avec bc.
b. Montrer que quel que soit l'entier naturel n, $n + 1$ est premier avec n et avec $2n + 1$.
c. Que peut-on en conclure ?

100 On cherche les solutions entières de l'équation :
$xy = (x - y)^2$ (E). Soit (x ; y) une solution.
1. Montrer que si $x = 0$, alors $y = 0$.
2. On suppose x non nul.
a. Montrer que $x^2 - 3 \times y + y^2 = 0$.
En déduire qu'il existe x' et y' premiers entre eux, tels que $x'^2 - 3x'y' + y'^2 = 0$.
c. Montrer que x' divise y'^2, puis que x' divise y'.
d. Montrer alors que y' et solution de $1 - 3y' + y'^2 = 0$.
3. Conclure

101 On considère deux entiers naturels, non nuls, x et y premiers entre eux. On pose $S = x + y$ et $P = x\,y$.
1. **a.** Démontrer que x et S sont premiers entre eux, de même que y et S.
b. En déduire que $S = x + y$ et $P = xy$ sont premiers entre eux.
c. Démontrer que les nombres S et P sont de parités différentes (l'un pair, l'autre impair).
2. **a.** Déterminer les diviseurs positifs de 84 et les ranger par ordre croissant.
b. Trouver les nombres premiers entre eux x et y tels que : $SP = 84$.
3. Déterminer les deux entiers naturels a et b vérifiant les conditions suivantes :
$a + b = 84$ et $ab = d^3$, où $d = pgcd(a ; b)$.
(On pourra poser $a = d\,a'$ et $b = d\,b'$ avec a' et b' premiers entre eux)

102 1. Montrer que, pour tout entier naturel non nul k et pour tout entier naturel x :

$$(x-1)(1+x+x^2+\ldots+x^{k-1})=x^k-1$$

Dans toute la suite de l'exercice, on considère un nombre entier a supérieur ou égal à 2.

2. Soient n un entier naturel non nul et d un diviseur positif de n : $n = dk$

Montrer que $a^d - 1$ est un diviseur de $a^n - 1$.

3. Soient m et n deux entiers naturels non nuls et d leur PGCD.

a. On définit m' et n' par $m = dm'$ et $n = dn'$.

Montrer que m' et n' sont premiers entre eux.

b. En appliquant le théorème de Bézout à m' et n', montrer qu'il existe des entiers relatifs u et v tels que $mu - nv = d$.

c. On suppose u et v strictement positifs. Montrer que : $(a^{mu} - 1) - (a^{nv} - 1)\,a^d = (a^d - 1)$. En déduire que $(a^d - 1)$ est le PGCD $(a^{mu} - 1)$ et de $(a^{nv} - 1)$.

d. Calculer, en utilisant le résultat précédent, le PGCD de $2^{63} - 1$ et de $2^{60} - 1$.

Théorème de Gauss

103 1. Soient a, b, c trois entiers naturels.

Montrer que si a et b, premiers entre eux, divisent c, alors ab divise c.

2. Montrer que quel que soit n entier naturel non nul,

a. $n(n+1)(n+2)(n+3)$ est multiple de 24.

b. $n(n+1)(n+2)(n+3)(n+4)$ est multiple de 120.

104 Soit a un entier relatif et b un entier naturel non nul.

On pose $x = \dfrac{a}{b}$. x est un nombre rationnel.

a. Montrer qu'il existe deux entiers a' relatif et b' naturel non nuls premiers entre eux, tels que $x = \dfrac{a'}{b'}$

b. Montrer que s'il existe deux autres entiers c relatif et d naturel non nuls premiers entre eux, tels que $x = \dfrac{c}{d}$, alors $c = a'$ et $d = b'$.

105 **a.** Déterminer l'ensemble des diviseurs 78 et l'ensemble des diviseurs de 14.

b. Soit $\dfrac{p}{q}$ une solution rationnelle de l'équation (1) d'inconnue x : $78x^3 + ux^2 + vx - 14 = 0$, où u et v sont des entiers relatifs. Montrer que si p et q sont des entiers relatifs premiers entre eux, alors p divise 14 et q divise 78.

c. En déduire le nombre de rationnels, non entiers, pouvant être solutions de l'équation (1) et écrire, parmi ces rationnels, l'ensemble de ceux qui sont positifs.

106 On considère la suite d'entiers définie par $a_n = 111\ldots11$ (l'écriture décimale de a_n est composée de n chiffres 1). On se propose de montrer que l'un, au moins, des termes de la suite est divisible par 2 013.

a. En écrivant a_n sous la forme d'une somme de puissances de 10, montrer que pour tout entier naturel n non nul, $9\,a_n = 10^n - 1$.

b. On considère la division euclidienne par 2 013 : expliquer pourquoi parmi les 2 014 premiers termes de la suite, il en existe deux, au moins, ayant le même reste. Soit a_n et a_p deux termes de la suite admettant le même reste ($n < p$). Quel est le reste de la division euclidienne de $a_p - a_n$ par 2 013 ?

c. Soient k et m deux entiers strictement positifs vérifiant $k < m$. Démontrer l'égalité $a_m - a_k = a_{m-k} \times 10^k$.

d. Calculer le PGCD de 2 013 et de 10. Montrer que si 2 013 divise $a_m - a_k$, alors 2 013 divise a_{m-k}.

e. Démontrer alors que l'un, au moins, des termes de la suite est divisible par 2 013.

f. Écrire un algorithme permettant de trouver la rang n tel que a_n soit divisible par 2 013.

(On pourra remarquer que $a_{n+1} = 10\,a_n + 1$).

Équations $ax + by = c$

107 Soit l'équation (1) d'inconnue rationnelle x :

$$78x^3 + ux^2 + vx - 14 = 0.$$

où u et v sont des entiers relatifs.

1. On suppose dans que $\dfrac{14}{39}$ est solution de l'équation (1).

a. Prouver que les entiers relatifs u et v sont liés par la relation $14u + 39v = 1\ 129$ (2).

b. Utiliser l'algorithme d'Euclide, en détaillant les étapes du calcul pour trouver un couple $(x ; y)$ d'entiers relatifs vérifiant l'équation $14x + 39y = 1$. Vérifier que le couple $(-25 ; 9)$ est solution de cette équation.

c. Donner la solution générale de l'équation (2).

d. Déterminer, parmi les couples $(u ; v)$ précédents, celui pour lequel le nombre u est l'entier naturel le plus petit possible.

108 1. On considère l'équation (E) : $11x - 7y = 5$, où x et y sont des entiers relatifs.

a. Justifier, en énonçant un théorème, qu'il existe un couple d'entiers relatifs $(u ; v)$ tels que $11u - 7v = 1$. Trouver un tel couple.

b. En déduire une solution particulière de l'équation(E).

2. Dans le plan rapporté à un repère $(O ; \vec{i}, \vec{j})$, on considère la droite D d'équation cartésienne $11x - 7y - 5 = 0$. On note C l'ensemble des points $M(x ; y)$ du plan tels que $0 \leqslant x \leqslant 50$ et $0 \leqslant y \leqslant 50$.

Déterminer le nombre de points de la droite D appartenant à l'ensemble C et dont les coordonnées sont des nombres entiers.

109 On considère l'équation où les inconnues x et y appartiennent à l'ensemble $\mathbb{Z}$ des nombres entiers naturels $20x - 9y = 2$ (1).

1. **a.** Montrer que si le couple $(u ; v)$ d'entiers relatifs est une solution de l'équation (1), alors v est un multiple de 2.

b. On désigne par d le PGCD de u et v. Quelles sont les valeurs possibles de d ?

2. Déterminer une solution particulière de l'équation (1), puis déterminer l'ensemble des solutions de cette équation.

3. Déterminer l'ensemble des solutions $(x ; y)$ de (1) telles que PGCD$(x ; y) = 2$.

Les congruences simultanées

110 1. On considère l'équation (E) : $8x + 5y = 1$,où$(x ; y)$ est un couple de nombres entiers relatifs.

a. Donner une solution particulière de l'équation (E).

b. Résoudre l'équation (E).

2. Soit N un nombre naturel tel qu'il existe un couple $(a ; b)$ de nombres entiers vérifiant :

$$\begin{cases} N = 8a + 1 \\ N = 5b + 2 \end{cases}.$$

a. Montrer que le couple $(a ; b)$ est solution de (E).

b. Quel est le reste, dans la division de N par 40 ?

3. Résoudre l'équation $8x + 5y = 100$, où $(x ; y)$ est un couple de nombres entiers relatifs.

4. Au VIII^{e} siècle, un groupe composé d'hommes et de femmes a dépensé 100 pièces de monnaie dans une auberge. Les hommes ont dépensé 8 pièces chacun et les femmes 5 pièces chacune. Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?

111 Un astronome a observé au jour J_0 le corps céleste A. Il apparaît périodiquement tous les 105 jours. Six jours plus tard $(J_0 + 6)$, il observe le corps B, dont la période d'apparition est de 81 jours. On appelle J_1 le jour de la prochaine apparition simultanée des deux objets aux yeux de l'astronome. Le but de cet exercice est de déterminer la date de ce jour J_1.



1. Soient u et v le nombre de périodes effectuées respectivement par A et B entre J_0 et J_1. Montrer que le couple $(u ; v)$ est solution de l'équation (E1) :

$$35x - 27y = 2.$$

2. **a.** Déterminer un couple d'entiers relatifs $(x_0 ; y_0)$ solution particulière de l'équation (E_2) : $35x - 27y = 1$.

b. En déduire une solution particulière $(u_0 ; v_0)$ de (E_1).

c. Déterminer toutes les solutions de l'équation (E_1).

d. Déterminer la solution $(u ; v)$ permettant de déterminer J_1. Combien de jours s'écouleront entre J_0 et J1 ?

3. **a.** Le jour J_0 était le samedi 16 décembre 2011, quelle est la date exacte du jour J_1 ? (L'année 2012 était bissextile.)

b. Si l'astronome manque ce futur rendez-vous, combien de jours devra-t-il attendre jusqu'à la prochaine conjonction des deux astres ?

112 Chloé joue avec des jetons. Si elle fait des tas de 7 jetons, il lui en reste 5. Si elle fait des tas de 5 jetons, il lui en reste 3. Combien a-t-elle de jetons ?

Soit n le nombre de jetons.

1. **a.** Montrer que n vérifie le système (1) $\begin{cases} n \equiv 5\,[7] \\ n \equiv 3\,[5] \end{cases}$.

b. En utilisant la calculatrice ou un tableur déterminer le plus petit entier n_0 répondant à la question. Quel est le nombre suivant répondant à la question ? Quelle conjecture faire sur tous les nombres répondant à la question ?

2. On désigne par S l'ensemble des solutions du système (1). On désigne par $(u ; v)$ un couple d'entiers relatifs tel que $7u + 5v = 1$.

a. Justifier l'existence d'un tel couple $(u ; v)$.

b. On pose $n_2 = 3 \times 7u + 5 \times 5v$. En utilisant les congruences, démontrer que n_2 appartient à S.

c. Donner un exemple d'entier n appartenant à S.

2. Caractérisation des éléments de S

a. Soit n un entier relatif appartenant à S.

Démontrer que $n - n_2 \equiv 0\,[35]$.

b. En déduire qu'un entier relatif n appartient à S si et seulement si il peut s'écrire sous la forme $n = 33 + 35k$ où k est un entier relatif.

3. Sachant que Chloé a entre 150 et 200 jetons, combien en a-t-elle ?

113 1. On se propose, dans cette question, de déterminer tous les entiers relatifs N tels que

$$\begin{cases} N \equiv 5\,[13] \\ N \equiv 1\,[17] \end{cases}.$$

a. Vérifier que 239 est solution de ce système.

b. Soit N un entier relatif solution de ce système. Démontrer que N peut s'écrire sous la forme

$N = 1 + 17x = 5 + 13y$ où x et y sont deux entiers relatifs vérifiant la relation $17x - 13y = 4$.

2. **a.** Résoudre l'équation $17x - 13y = 4$ où x et y sont des entiers relatifs.

b. En déduire qu'il existe un entier relatif k tel que $N = 18 + 221k$.

3. Démontrer l'équivalence entre $N \equiv 18\,(221)$ et $\begin{cases} N \equiv 5\,[13] \\ N \equiv 1\,[17] \end{cases}$.

Devoir de synthèse

Revoir les bases suivantes :
cours A à D, savoir-faire 1 à 11.

[Le devoir est corrigé p. 172]

Chaque exercice peut être fait de manière indépendante

Premier sujet

114 [5 points]

Les questions sont indépendantes.

a. Démontrer que, pour tout entier relatif k, les entiers $12k + 7$ et $5k + 3$ sont premiers entre eux.

b. Existe-il des couples d'entiers tels que $51x + 69y = 1$?

c. Déterminer les entiers naturels a et b tels que $a + b = 132$ et PGCD$(a ; b) = 11$.

115 [5 points]

a. Montrer que l'équation (E) : $7x - 3y = 1$ a pour solutions les entiers relatifs de la forme $(x ; y) = (1 + 3k ; 2 + 7k)$ où k est un entier relatif.

b. Vérifier que les couples $(1 ; -1)$ et $(10 ; 20)$ sont solutions de l'équation (E') $7x - 3y = 10$.

c. Le raisonnement suivant est-il correct ? : Les solutions de l'équation (E') s'obtiennent en multipliant les solutions de l'équation (E) par 10, donc sont les couples $(x ; y) = (10 + 30k ; 20 + 70k)$ où k est un entier relatif.

d. Résoudre l'équation (E').

116 **Vrai ou faux.** Justifier [5 points]

L'équation $ax + by = c$, avec a, b et c entiers relatifs,

a. n'a des solutions que si $c = 1$

b. n'a des solutions que si PGCD$(a ; b) = c$

c. a toujours des solutions.

d. n'a des solutions que si PGCD$(a ; b)$ divise c.

117 [4 points]

On considère les entiers :

$a = 2n^3 + 5n^2 + 4n + 1$ et $b = 2n^2 + n$, où $n \in \mathbb{N}$.

a. Montrer que $2n + 1$ divise a et b.

b. Montrer que les entiers $c = n^2 + 2n + 1$ et $d = n$ sont premiers entre eux.

c. En déduire que PGCD$(a ; b) = 2n + 1$.

118 [5 points]

a. Montrer que l'équation $65x - 40y = 1$ n'a pas de solution dans $\mathbb{Z}^2$.

b. Justifier que l'équation (E) $17x - 40y = 1$ admet au moins une solution dans $\mathbb{Z}^2$.

c. Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation (E).

d. Résoudre alors l'équation (E).

e. En déduire qu'il existe un unique entier naturel inférieur à 40 tel que $17x_0 \equiv 1$ [40].

f. Soit a un entier naturel. Démontrer que si $a^{17} \equiv b$ [55] et $a^{40} \equiv 1$ [55], alors $b^{33} \equiv a$ [55].

Deuxième sujet

119 **Vrai ou faux.** Justifier [5 points]

a. Si 2 divise $7n$, alors 2 divise n.

b. Si $3a + 5b = 6$, alors PGCD$(a ; b) = 6$.

c. Si $7a + 8b = 1$, alors PGCD$(a ; b) = 1$.

d. Si n est divisible par 4 et 15, alors 60 divise n.

e. Si $p = 5n - 3$ et $q = n + 1$ (n entier naturel) alors PGCD$(p ; q)$ = PGCD$(8 ; n + 1)$.

120 [3 points]

a. Rappeler le théorème de Bézout pour deux entiers a et b.

b. Soient a et b deux entiers premiers entre eux. On considère l'algorithme ci-dessous.

```
Algorithme
Entrer a,b
1 → u
a → c
TantQue a n'est pas congru à 1 modulo b
u + 1 → u
uxc → a
Fin TantQue
(1 - a)/b → v
Afficher u,v
```

Faire tourner cet algorithme sur un exemple.
Que fait-il ?

121 [8 points]

1. **Préliminaire : ROC**

Prérequis : le théorème de Bézout

Énoncer et démontrer le théorème de Gauss.

2. **a.** En utilisant l'algorithme d'Euclide, déterminer une solution particulière de l'équation $19x + 29y = 1$ où x et y sont des entiers.

b. En déduire une solution entière de l'équation $19x + 29y = 818$(avec x et y entiers).

c. Déterminer alors toutes les solutions de l'équation $19x + 29y = 818$.

3. Un théâtre pratique deux tarifs : 19 euros pour les abonnés et 29 euros pour les autres.

À la fin d'une séance, la recette s'élève à 818 euros. La caissière a perdu les talons des billets et veut retrouver le nombre de billets de chaque sorte vendu. Aider la caissière à résoudre son problème.

122 [4 points]

1. Montrer en utilisant le théorème de Bézout que si a est premier avec b, alors

a. a est premier avec $a + b$.

b. a est premier avec b^2.

2. Peut-on démontrer **1.a.** et **1.b.** sans utiliser le théorème de Bézout ?

Exercices guidés BAC

123 **Partie A**

On considère l'équation (E) : $11x - 26y = 1$, où x et y désignent deux nombres entiers relatifs.

1. Vérifier que le couple $(-7 ; -3)$ est solution de (E).
2. Résoudre alors l'équation (E).
3. En déduire le couple d'entiers relatifs $(u ; v)$ solution de (E) tel que $0 \leqslant u \leqslant 25$.

Partie B

On assimile chaque lettre de l'alphabet à un nombre entier suivant l'ordre naturel : A → 0, B → 1, Z → 25. On « code » tout nombre entier x compris entre 0 et 25 de la façon suivante :

- on calcule $11x + 8$;
- on calcule le reste de la division euclidienne de $11x + 8$ par 26 que l'on appelle y.

x est alors « codé » par y. Ainsi, par exemple, la lettre L est assimilée au nombre 11 ; $11 \times 11 + 8 = 129$ or $129 \equiv 25$ [26], 25 est le reste de la division euclidienne de 129 par 26. Au nombre 25 correspond la lettre Z. La lettre L est donc codée par la lettre Z.

1. Coder la lettre W.
2. Le but de cette question est de trouver la fonction de décodage.
   a. Montrer que pour tous nombres entiers relatifs x et j, on a : $11x \equiv j$ [26] équivaut à $x \equiv 19\,j$ [26],
   b. En déduire un procédé de décodage.
3. Décoder la lettre W.
4. Écrire un algorithme permettant de coder, puis un autre algorithme pour décoder toutes les lettres.

Guide

Partie A

1. $11 \times (-7) - 26 \times 3 = 1$.
2. *Si (x, y) est solution alors .....
   $11(x + 7) = 26(y + 3)$
   Utiliser le théorème de Gauss ($x = -7 + 26k$.....)
   **Ne pas oublier la réciproque
3. $0 \leqslant u \leqslant 25 \Leftrightarrow 0 \leqslant -7 + 26k \leqslant 25$ donc $k = ...$

Partie B

1. On a le schéma :
   $W \rightarrow 22 \rightarrow 22 \times 11 + 8$ [26] $= 16 \rightarrow Q$
2. **a.** D'après A3, $11 \times 19 - 8 \times 26 = 1$, donc $11 \times 19 \equiv 1$ [26].
   Si $11x \equiv j$ [26], alors $19 \times 11x \equiv 19\,j$ [26].
   Si $x \equiv 19\,j$ [26], alors $11x \equiv 11 \times 19\,j$ [26].
   donc ...
   b. $y \equiv 11x + 8$ [26], donc $y - 8 \equiv 11x$ [26],
   donc $x \equiv 19(y - 8)$ [26]
3. $W \rightarrow 22$, donc si $y = 22$, $x \equiv 19 \times 14$ [26].
4. Algorithme pour coder :
   Début.
   Pour x variant de 0 à 25
   Mod $(11x + 8, 26) \rightarrow L1$
   Fin

124 Les suites d'entiers naturels (x_n) et (y_n) sont définies sur N par : $x_0 = 3$ et $x_{n+1} = 2x_n - 1$, $y_0 = 1$ et $y_{n+1} = 2y_n + 3$.

1. Démontrer par récurrence que pour tout entier naturel n, $x_n = 2^{n+1} + 1$.
2. **a.** Calculer le PGCD de x_2 et x_3. Que peut-on en déduire ?
   b. x_n et x_{n+1} sont-ils premiers entre eux pour tout entier naturel n ?
3. **a.** Démontrer que pour tout entier naturel n, $2x_n - y_n = 5$.
   b. Exprimer y_n en fonction de n.
   c. En utilisant les congruences modulo 5, étudier suivant les valeurs de l'entier naturel p le reste de la division euclidienne de 2^p par 5.
4. On note d_n le PGCD de x_n et y_n pour tout entier naturel n.
   a. Écrire un algorithme donnant d_n suivant les valeurs de n.
   Émettre des conjectures sur la valeur de d_n.
   b. Démontrer la conjecture émise en a.

Guide

1. Initialisation : $x_0 = 2^1 + 1 = 3$.
   • Hérédité : supposons que $x_n = 2^{n+1} + 1$.
   $x_{n+1} = 2x_n - 1 = 2(2^{n+1} + 1) - 1 = 2^{n+1+1} + 1$
   • donc .....
2. **a.** $x_2 = 2^3 + 1 = 9$, $x_3 = 2x_2 - 1 = 17$.
   $2x_2 - x_3 = 1$ donc ...
   b. $2x_n - x_{n+1} = 1$ donc ...
3. **a.** Par récurrence : $2x_0 - y_0 = 6 - 1 = 5$.
   Si $2x_n - y_n = 5$, alors $2x_{n+1} - y_{n+1} =$ ....., donc .....
   b. $y_n = 2x_n - 5 = 2^{n+2} - 3$
   c. $2^2 \equiv -1$ [5], donc $2^4 \equiv 1$ [5]. On démontre que $2^{4k+r} \equiv 2^r$ [5].
4. On conjecture que $d_n = 5$ si $n = 4k + 1$ et 1 sinon
   a. $2x_n - y_n = 5$ donc d_n le pgcd de x_n et y_n divise 5, donc $d_n = 1$ ou $d_n = 5$.
   b. 5 divise x_n si $n + 1 = 4k + 2$, soit $n = 4k + 1$.
   5 divise y_n si $n + 2 = 4k + 3$, soit $n = 4k + 1$, donc...

QCM - Vrai ou faux BAC

125 **Vrai ou Faux (Justifier)**

a. Le PGCD de 2004 et 4 002 est 6.

b. PGCD($3n^3 - 11n$; $n + 3$) = PGCD(48 ; $n + 3$).

c. 847 et 342 sont premiers entre eux.

d. Il existe des entiers naturels n tels que n et $2n + 1$ ne soient pas premiers entre eux.

e. Soit n un entier naturel.
PGCD($n + 3$; $2n + 1$) = 5

f. On appelle S l'ensemble des couples(x ; y) d'entiers relatifs solutions de l'équation $3x-5y = 2$.
« L'ensemble S est l'ensemble des couples ($5k - 1$; $3k - 1$) où k est un entier relatif. »

g. a et b sont deux entiers relatifs, n et p deux entiers naturels premiers entre eux.
$a \equiv b$ (p) si et seulement si $na \equiv nb$ (p).

h. Dans le plan muni d'un repère, (D) est la droite d'équation $11x - 5y = 14$.
Les points de (D) à coordonnées entières sont les points de coordonnées $(5k + 14 ; 11k + 28)$ où $k \in \mathbb{Z}$.

i. Si un entier naturel n est congru à 1 modulo 7 alors le PGCD de $3n + 4$ et de $4n + 3$ est égal à 7.
Soient a et b deux entiers naturels.

j. Soient a et b deux entiers naturels. S'il existe deux entiers relatifs u et v tels que
$au + bv = 2$ alors le PGCD de a et b est égal à 2.

k. Si dans la division de n par 3 le reste est 2 et par 5, le reste est 1, alors $n - 11$ est divisible par 15.

l. Il n'existe aucun entier relatif x tel que $\begin{cases} x \equiv 2\ [4] \\ x \equiv 5\ [5] \end{cases}$.

126 **QCM (Choisir la ou les bonnes réponses)**

1. On se propose de résoudre l'équation (E) :
$24x + 34y = 2$, où x et y sont des entiers relatifs.

a. Les solutions de (E) sont toutes de la forme :
$(x ; y) = (34k - 7 ; 5 - 24k)$, $k \in \mathbb{Z}$.

b. Les solutions de (E) sont toutes de la forme :
$(x ; y) = (17k - 7 ; 5 - 12k)$, $k \in \mathbb{Z}$.

c. Les solutions de (E) sont toutes de la forme :
$(x ; y) = (-7k ; 5k)$, $k \in \mathbb{Z}$.

2. On définit a_n et b_n tels que $(1 + \sqrt{6})^n = a_n + \sqrt{6}\ b_n$

a. $a_6 = 1$ et $b_6 = 216$

b. Pour tout n, 5 divise $a_n + b_n$.

c. a_n et b_n sont premiers entre eux.

3. Soit n un entier naturel.
On pose $N = 9n + 1$ et $M = 9n - 1$.

a. M et N sont premiers entre eux.

b. si n est impair, M et N sont premiers entre eux.

c. Si n est pair, MN est divisible par 4.

4. Soit n un entier naturel. On pose $A(n) = n^4 + 1$.

a. $A(n)$ est pair.

b. $A(n)$ est premier avec n.

c. $A(n)$ est premier avec 3.

5. Le système d'inconnue x entier relatif : $\begin{cases} x \equiv 1\ [12] \\ x \equiv 7\ [18] \end{cases}$.

a. n'a pas de solution.

b. a pour solution $x = 1 + 12k$, k entier relatif.

c. a pour solution $x = 25 + 36k$.

Exercice BAC

127 **PARTIE A** **Restitution organisée des connaissances**

Énoncer le théorème de Bézout et le théorème de Gauss.

1. En utilisant le théorème de Bézout, démontrer le théorème de Gauss.

2. Soient p et q deux entiers naturels tels que p et q sont premiers entre eux.
Déduire du théorème de Gauss que, si a est un entier relatif, tel que $a \equiv 0\ [p]$ et $a \equiv 0\ [q]$, alors $a \equiv 0\ [pq]$.

PARTIE B

On se propose de déterminer l'ensemble S des entiers relatifs n vérifiant le système :

$$n \equiv 9\ [17] \text{ et } n \equiv 3\ [5]$$

1. a. Écrire un algorithme permettant de trouver une solution de S.

b. Quelle conjecture faire sur les solutions de S ?

2. Recherche d'un élément de S. On désigne par $(u ; v)$ un couple d'entiers relatifs tel que $17u + 5v = 1$.

a. Justifier l'existence d'un tel couple $(u ; v)$.

b. On pose $n_0 = 3 \times 17u + 9 \times 5v$.
Démontrer que n_0 appartient à S

c. Donner un exemple d'entier n_0 appartenant à S.

3. Caractérisation des éléments de S.

a. Soit n un entier relatif appartenant à S.
Démontrer que $n - n_0 \equiv 0\ [85]$.

b. En déduire qu'un entier relatif n appartient à S si et seulement si $n = 43 + 85k$ où k est un entier relatif.

128 Le théorème des restes chinois

Soient a et b deux entiers naturels et m et n deux entiers relatifs. On cherche les entiers relatifs x tels que : $\begin{cases} x \equiv n\,[a] \\ x \equiv m\,[b] \end{cases}$.

Cas 1 : $m = n$. On cherche donc x tel que $(x - n) \equiv 0$ [a] et $(x - n) \equiv 0$ [b].

1. Soit x une solution, et d = PGCD(a ; b), $a = da'$, $b = db'$. Montrer qu'il existe (k, k') tel que $ka' = k'b'$

2. En utilisant le théorème de Gauss, montrer que $x \equiv n[\mu]$, où $\mu = da'b' = ab' = a'b$.

3. Réciproquement, vérifier que si $x \equiv n[\mu]$, alors x est solution.

4. Conclure.

Exemple : Résoudre $\begin{cases} x \equiv -1\,[4] \\ x \equiv -1\,[6] \end{cases}$.

Cas 2 : $m \neq n$, a et b premiers entre eux.

1. Soit x une solution.

a. Montrer qu'il existe un couple (k, k') d'entiers relatifs tels que $ak - bk' = m - n$.

b. Montrer qu'il existe un couple (u, v) d'entiers relatifs tels que $au + bv = 1$.

2. Soit $x_0 = n + (m - n)au$.

a. Montrer que $x_0 = mau + nbv$

b. Montrer que x_0 est solution.

c. Montrer que x est solution si et seulement si $x \equiv x_0$ [a] et $x \equiv x_0$ [b]

d. En déduire que x est solution si et seulement si $x \equiv x_0$ [ab].

Exemple : Résoudre $\begin{cases} x \equiv 2\,[5] \\ x \equiv 6\,[7] \end{cases}$.

Applications

a. Existe-t-il un entier naturel tel que si on le divise par 9 le reste est 5 et si on le divise par 21, le reste est 7 ? Si oui, le déterminer.

b. Existe-t-il un entier naturel tel que si on le divise par 54 le reste est 5 et si on le divise par 48, le reste est 23 ?

Aide

> On se ramènera au cas de nombres premiers entre eux.

129 Le chiffrement de Hill

Les codages monographiques résistent mal aux cryptanalystes, lesquels peuvent disposer de données sur les fréquences d'apparition des lettres d'une langue donnée. Pour pallier cette faiblesse on utilise un codage par blocs proposé par Hill dans les années 1930.

Pour coder FERMAT, on scinde en blocs de deux lettres, FE RM AT que l'on transforme en équivalent numérique : (5, 4) (17, 12) (0, 19).

Chaque couple de nombres (x, y) est codé en (z, t) par : $z \equiv ax + by$ [26], $0 \leqslant z \leqslant 25$ et $t \equiv cx + dy$ [26], $0 \leqslant t \leqslant 25$ avec a, b, c, d entiers relatifs puis en blocs de deux lettres.

1. Coder FERMAT avec $(a, b) = (5, 17)$ et $(c, d) = (4, 15)$.

2. Deux questions se posent :

- peut-on choisir (a, b), (c, d) quelconques ?
- comment décoder ?

Les deux questions sont liées.

On va montrer le résultat suivant : a, b, c, d étant des entiers relatifs et n un entier naturel, le système S $\begin{cases} ax + by \equiv z\,[n] \\ cx + dy \equiv t\,[n] \end{cases}$ a une unique solution si et seulement si $\Delta = ad - bc$ est premier avec n.

a. Montrer que S équivaut à S' : $\begin{cases} \Delta x \equiv dz - bt\ [n] \\ \Delta y \equiv at - cz\ [n] \end{cases}$.

b. Montrer que Δ est premier n si et seulement si il existe un couple d'entiers relatifs (u, v) tel que $\Delta u + vn = 1$. On admet alors qu'il existe un unique nombre noté Δ' tel que $\Delta\Delta' \equiv 1$ [n] et $1 \leqslant \Delta' \leqslant n$.

Ce nombre est appelé inverse de Δ modulo n.

c. Montrer alors que $x \equiv \Delta'\,(dz - bt)$ $[n]$, $0 \leqslant x \leqslant n$.

Que vaut alors y ?

3. On pose $(a, b) = (5, 17)$ et $(c, d) = (4, 15)$, $n = 26$.

a. Calculer Δ et déterminer Δ'.

b. Décoder alors FI QM FP OA JG HK

On pourra compléter, puis utiliser l'algorithme :

```
entrer z, t                    TI 83
  a = 5, b = 17, c = 4,        ; prompt Z, T
  d = 15                       : 5 → A, 17 → B
  Δ' =                         : … → Δ'
  x = Mod(Δ' (dz - bt),        : (Δ' (dz - bt) → E
  [26],                        : E-Ent(E/26)*26 → X
```

130 Les triplets pythagoriciens

Un triplet (x, y, z) d'entiers naturels non nuls tels que $x^2 + y^2 = z^2$ est appelé un triplet pythagoricien noté TP.

1. Triplets irréductibles. Vérifier que :

a. (a, b, c) est un TP si et seulement si, pour tout entier naturel n, (na, nb, nc) est un TP.

b. Si deux des trois nombres ont un diviseur commun d alors d divise le troisième.

c. Si deux des trois nombres sont premiers entre eux alors a, b et c sont premiers entre eux deux à deux. En déduire que l'on peut se limiter à la recherche de TP (a, b, c) où les entiers sont premiers entre eux 2 à 2. Un tel triplet pythagoricien est appelé triplet pythagoricien irréductible noté (TPI).

2. Triplets irréductibles rangés. Soit (a, b, c) un TPI.

a. Montrer qu'il y a au moins deux nombres impairs.

b. Montrer qu'il y a au moins un nombre pair.

c. Montrer que si c est pair alors $c^2 \equiv 2$ [4]. En déduire que c est impair.

d. En déduire que l'on peut se limiter à la recherche de TPI (a, b, c) tel que a et c sont impairs et b est pair. Un tel TP sera dit irréductible et rangé. (TPIR)

3. Détermination de tous les TPIR.

a. Soit (a, b, c) un TPIR.

i. Montrer que l'équation équivaut à

$$\left(\frac{b}{2}\right)^2 = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right) \text{ où } \frac{b}{2}, \frac{c+a}{2}, \frac{c-a}{2}$$

sont des entiers naturels.

ii. Montrer que $\frac{c+a}{2}$ et $\frac{c-a}{2}$ sont premiers entre eux.

iii. En déduire qu'il existe deux entiers u et v tels que $u^2 = \frac{c+a}{2}$ et $v^2 = \frac{c-a}{2}$. (On admettra le résultat suivant qui sera démontré dans le chapitre 3 : si x, y, z sont des entiers naturels tels que PGCD$(x ; y) = 1$ et $z^2 = xy$ alors il existe deux entiers naturels u et v tels que $x = u^2$ et $y = v^2$).

iv. Montrer qu'alors, $c = u^2 + v^2$ et $a = u^2 - v^2$ et $b = 2uv$ où u et v sont premiers entre eux et de parités différentes .

b. En déduire alors que (a, b, c) est un triplet pythagoricien irréductible rangé si et seulement si il existe deux entiers premiers entre eux et de parités différentes u et v tels que $0 < v < u$ et $a = 2uv$, $b = u^2 - v^2$ et $c = u^2 + v^2$.

4. Voici le début d'un programme implanté sur TI83.

a. Justifier chacune des entrées.

b. Terminer le programme afin qu'il donne les nombre et les triplets tels que c soit inférieur à un nombre donné n.

```
PROGRAM:TRIPLET
:Prompt N
:1→X
:EffListe L1,L2,
L3
:For(U,1,√(N))
:For(V,1,U-1)
:If pgcd(U,V)=1
et partDéc((U+V)
/2)≠0 et (U²+V²≤
N)
:Then
:U²-V²→L1(X)
:2*U*V→L2(X)
:U²+V²→L3(X)
```

131 **Le critère d'Eisenstein**

On considère la fonction polynôme f de degré n à coefficients entiers relatifs définie par :

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, avec $a_n \neq 0$.

On cherche à trouver des racines rationnelles.

1. Montrer que si $a_0 = 0$, alors 0 est racine de f.

2. On suppose que $a_0 \neq 0$.

Soit $\frac{p}{q}$ un rationnel irréductible tel que $f(\frac{p}{q}) = 0$.

a. Montrer que

$a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 p\, q^{n-1} + a_0 q^n = 0$.

b. En déduire que

$a_n p^n = q(\, a_{n-1}p^{n-1} + \ldots + a_1 p\, q^{n-2} + a_0 q^{n-1})$

c. Montrer que q est premier avec p^n.

d. En déduire que q divise a_n. Montrer de même que p divise a_0.

3. Application 1. Soit $f(x) = 2x^7 + ax^3 - 3$. Sachant que f admet une racine rationnelle, quelles peuvent être les valeurs de a ?

4. Application 2. On veut trouver les racines de $f(x) = 4x^3 - 7x^2 - 12x + 21$.

a. Trouver une racine rationnelle a.

b. Trouver une fonction du second degré g telle que $f(x) = (x - a)g(x)$.

c. Trouver toutes les racines de f.

Défis

132 L'équation $x^7 + 3x + 3$ a-t-elle des racines rationnelles ?

133 Les côtés d'un terrain triangulaire ont pour mesure, en mètres, 132, 156 et 204. On veut planter des arbres sur son périmètre de façon qu'il y ait un arbre à chaque sommet du triangle et que les arbres soient également espacés. Quel est le nombre minimal d'arbres que l'on pourra planter si on veut que la distance entre deux arbres soit exprimée par un nombre entier de mètres ?

134 Trois navires partent d'un même port, l'un tous les huit jours, l'autre tous les 10 jours, le dernier tous les quinze jours. Tous quittent le port un 11 mai. Quelle est la date du prochain départ commun ?

Communiquer à l'écrit ou à l'oral

À propos de cryptographie

Au début, on utilisa des substitutions mono-alphabétiques : substitution d'une lettre par une autre lettre en respectant les deux conditions suivantes :

- deux lettres différentes sont codées par des lettres différentes
- la même lettre est toujours codée de la même façon.

Mais une analyse des fréquences des lettres dans une langue permet de déchiffrer le message.

Le chiffrement de Hill a permis un temps de retarder le cassage des codes.

1. Dans le cas d'un codage affine, du type $n' \equiv an + b$ [26], expliquer comment faire pour casser le code, si on ne connaît ni a ni b.

2. Dans le cas du chiffrement de Hill, on code deux lettres ou plus en même temps. (voir exercice 129).
Expliquer comment une même lettre peut-être codée de deux façons différentes. Comment pourrait-on tenter de casser le code ?

Accompagnement personnalisé

Soutien

AP 1 Analyse critique de copies

Objectifs :
- *Revoir l'utilisation du PGCD.*
- *Avoir une attitude critique vis-à-vis des documents.*

1. On considère l'énoncé suivant : on désigne par p un nombre entier naturel. On considère pour tout entier naturel non nul n le nombre $A_n = 2^n + p$. On note d_n le PGCD de A_n et A_{n+1}. Montrer que d_n divise 2^n.

Réponse 1

$A_n = 2^n + p$. $A_{n+1} = 2^{n+1} + p$.
$d_n = PGCD(A_n, A_{n+1})$.
Donc d_n divise A_n et d_n divise A_{n+1}
Or $A_n = 2^n + p$, donc d_n divise 2^n et d_n divise p, donc d_n divise 2^n.

Réponse 2

$PGCD(2^n + p, 2^{n+1} + p) = PGCD(2^n, 2^{n+1}) = 2^n$.

Réponse 3

d_n divise $2^n + p$ et toute combinaison linéaire, donc d_n divise 2^n et d_n divise p.

Voici, à gauche, trois réponses d'élèves. Que penser de ces raisonnements ?
Quelle remarque le professeur pourrait-il porter sur ces copies ?

Voici, à droite, d'autres raisonnements pour cette question :

a. Pour que d_n divise A_n, il faut que d_n divise 2^n et d_n divise p donc d_n divise 2^n.

b. d_n divise A_n et A_{n+1} donc d_n divise $A_{n+1} - A_n = 2^n(2 - 1) = 2^n$

c. $d_n = PGCD(A_n, A_{n+1}) = PCGD(2^n, A)$, donc d_n divise 2^n.

d. D'après le théorème de Bezout, on sait que si $d = PGCD(a, b)$, alors $au + bv = d$. En prenant $u = 1$, $v = -1$, on a : $A_{n+1} - A_n = 2^n(2 - 1) = 2^n$, donc $d_n = 2^n$ donc d_n divise 2^n.

2. Voici la suite ;
a. Déterminer la parité de A_n en fonction de celle de p.
b. Déterminer la parité de d_n en fonction de celle de p.
c. Déterminer $PGCD(2^{2011} + 2011, 2^{2012} + 2011)$
Et des réponses :
a. 2^n étant pair, A_n a même parité que p.
b. d_n a même parité que A_n donc que p.
c. $n = p = 2011$ donc d est impair.
Les réponses sont-elles exactes ? Sont-elles bien rédigées ? Sont-elles complètes ? Terminer avec soin la rédaction de cet exercice.

- Parmi les quatre raisonnements ci-dessus, trouver les raisonnements faux.
- Trouver les propriétés que l'élève a cru pouvoir utiliser.
- Repérer les raisonnements exacts.
- Citer les propriétés que l'élève aurait pu rajouter.
- Écrire un raisonnement correct et complet.

Découvrir un métier

AP 2 Chercheur en mathématiques

Objectif :
- *Aider à l'orientation.*

Les différentes fonctions que se partagent les chercheurs sont : conduire une réflexion rigoureuse sur une problématique identifiée, entreprendre, selon le domaine de recherche, les expérimentations et les missions nécessaires, construire, au niveau national et international, un réseau d'échange des savoirs entre les chercheurs d'une même communauté, former à la recherche et par la recherche les jeunes chercheurs et de futurs cadres supérieurs de l'industrie, publier les résultats de ses travaux de recherche, participer à leur transfert vers le secteur industriel, contribuer à la diffusion des résultats de la recherche dans la société et développer la culture scientifique et technique et participer à l'administration de la recherche.



Cédric Villani, médaille Fields 2010

1. Quel est le niveau d'études requis pour devenir chercheur ?
2. Où peut exercer un chercheur en mathématiques ?
3. Beaucoup de chercheurs sont aussi enseignants. Pourquoi ?
4. Qu'est ce que la médaille Fields ?

Approfondir

AP 3 Un théorème dû à Euler

Objectif :
- *Découvrir un théorème important pour coder des messages.*

Soit n un entier naturel. On définit la fonction φ de $\mathbb{N}$ dans $\mathbb{N}$ appelée fonction indicatrice d'Euler.
$\varphi(n)$ désigne le nombre de nombres entiers naturels non nuls premiers avec n et inférieur à n.
Soit a un entier naturel premier avec n.

Considérons $s_1 < s_2 < \ldots < s_{\varphi(n)}$ les entiers inférieurs à n et premiers avec n, puis les produits as_1, as_2..., $a\,s_{\varphi(n)}$ et les restes r_1, r_2..., $r_{\varphi(n)}$ de ceux-ci modulo (n). On a donc $as_i \equiv r_i\ [n]$

1. Soit S l'ensemble $\{s_1, s_2..., s_{\varphi(n)}\}$. Montrer que $s_1 = 1$ et $s_{\varphi(n)} = n - 1$.

2. Soit i un entier naturel tel que $1 \leqslant i \leqslant \varphi(n)$.
a. Montrer que n divise $as_i - r_i$.
b. Soit d un diviseur de n tel que d divise r_i. Montrer que $d = 1$.
c. En déduire que r_i est premier avec n et est élément de S.

3. Soit i et j deux entiers naturels tels que $1 \leqslant i < j \leqslant \varphi(n)$ tels que $r_i = r_j$.
a. Montrer que n divise $s_i - s_i$ et que $(n - 1) \leqslant s_i - s_i \leqslant n - 1$.
b. En déduire $s_i = s_i$.
c. En déduire que les r_i sont distincts, et sont égaux dans leur ensemble, à l'ordre près, aux s_i pour $1 \leqslant i \leqslant \varphi(n)$.

4. a. En déduire que $as_1 \times as_2 \times \ldots \times a\,s_{\varphi(n)} \equiv s_1 \times s_2 \times \ldots \times s_{\varphi(n)}\ [n]$.
b. Montrer n divise $(a^{\varphi(n)} - 1)\ s_1 \times s_2 \times \ldots \times s_{\varphi(n)}$
c. Montrer que n est premier avec $s_1 \times s_2 \times \ldots \times s_{\varphi(n)}$.
En déduire que n divise $(a^{\varphi(n)} - 1)$

5. Montrer que si a un entier naturel premier avec n, $a^{\varphi(n)} \equiv 1\ [n]$
Ceci est un des nombreux théorèmes dus à Euler.

AP 4 Une application : un codage par exponentiation

Objectif :
- *Découvrir une autre méthode de codage.*

1. Sur un tableur, écrire les congruences modulo 26 des puissances successives des entiers de 2 à 25.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	n/k	2	3	4	5	6	7	8	9	10	11	12	13
2	1	2	3	4	5	6	7	8	9	10	11	12	13
3	2	4	9	16	25	10	23	23	3	22	17	14	13
4	3	8	1	12	21	8	5	18	1	12	5	12	13
5	4	16	3	22	1	22	9	14	9	16	3	14	13
6	5	6	9	10	5	2	11	8	3	4	7	12	13
7	6	12	1	14	25	12	25	12	1	14	25	14	13
8	7	24	3	4	21	20	19	18	9	10	15	12	13
9	8	22	9	16	1	16	3	14	3	22	9	14	13
10	9	18	1	12	5	18	21	8	1	12	21	12	13
11	10	10	3	22	25	4	17	12	9	16	23	14	13
12	11	20	9	10	21	24	15	18	3	4	19	12	13
13	12	14	1	14	1	14	1	14	1	14	1	14	13
14	13	2	3	4	5	6	7	8	9	10	11	12	13

Ainsi la cellule G4 renvoie la congruence modulo 26 de 7^3.
a. Montrer que les nombres premiers avec 26 sont impairs et non multiples de 13. En déduire $\varphi(26)$.
b. Expliquer les colonnes M et L.
c. Expliquer la ligne 13. Que constatez-vous à la ligne 14 ?
d. À l'aide du tableur, vérifier que n^{12k+1} est congru à n modulo 26. On admettra ce résultat pour la suite.
e. D'après le tableau , conjecturer l'existence d'entier k tel que pour n entier de [2, 25], les congruences modulo 26 de n^k soient toutes distinctes ?

2. a. On pose $k = 7$. Montrer qu'il existe (u, v) entiers naturels tel que $7u = 1 + 12v$.
b. Déterminer la valeur de u comprise entre 2 et 11.
c. Montrer que pour tout n de [0, 25], $(n^7)^u \equiv n\ [26]$. En déduire que :
i. si $n^7 \equiv m^7\ [26]$, alors $n \equiv m\ [26]$.
ii. Si $a \equiv n^7\ [26]$, alors $a^u \equiv n\ [26]$.

3. Lara et Aymeric communiquent par message secret de la façon suivante : Lara transforme chaque lettre de son message en nombre de 0 à 25 suivant l'ordre alphabétique, puis élève chaque nombre obtenu à la puissance 7, prend les restes dans la division par 26, transforme ce reste en lettre. Comment Aymeric, qui connaît le code fait-il pour déchiffrer les messages ?

3 Nombres premiers

Vérifier ses acquis

1 Nombres premiers

a. Parmi les 20 premiers entiers naturels, lesquels sont premiers ?
b. Les nombres pairs peuvent-ils être premiers ?

2 Diviseurs et multiples

1. Trouver des diviseurs évidents aux nombres suivants : 24 ; 132 ; 111 ; 225 ; 1 331.
2. a. Écrire la liste des multiples de 9 inférieurs à 100.
b. Écrire la liste des multiples de 12 inférieurs à 100.
c. En déduire les multiples communs à 9 et 12 inférieurs à 100. Quel en est le plus petit ? On le note m.
d. Déterminer d, le PGCD de 9 et 12.
e. Que dire de md ?

3 Décomposition

1. Décomposer en produit de nombres premiers les nombres suivants : 10×32 ; 25×36 ; 75×120.
2. On pose $a = 2^5 \times 3^3 \times 5^2$ et $b = 2^4 \times 3^2 \times 5$. Montrer que b divise a et donner le quotient de a par b.
3. On pose $a = 2^2 \times 3^3$ et $b = 2 \times 3^4$.
a. Déterminer les diviseurs de a. Quel est leur nombre ?
b. Déterminer les diviseurs de b. Quel est leur nombre ?
c. Déterminer les diviseurs communs à a et b. Quel est le plus grand ?
4. On pose $a = 2^2 \times 3^3$ et $b = 2 \times 3^4$.
a. Quelle est la forme des multiples de a ?
b. Quelle est la forme des multiples de b ?
c. Quelle est la forme des multiples communs à a et b ? Quel en est le plus petit ?
5. Vrai ou Faux
Soit $a = 25 \times 33 \times 52 \times 7$ et $b = 24 \times 34 \times 5 \times 11$.
a. $26 \times 33 \times 52 \times 11$ est un multiple de a.
b. $22 \times 34 \times 5$ est un diviseur de b.
c. $25 \times 34 \times 52 \times 7 \times 11 \times 13$ est un multiple commun à a et b.
d. $2 \times 3 \times 5 \times 7$ est un diviseur commun à a et b.

4 Fractions

a. Rendre irréductibles les fractions $\frac{12}{16}$; $\frac{144}{132}$; $\frac{3\,250}{1275}$.
b. Additionner les fractions suivantes : (On donnera les résultats sous forme de fraction irréductible.)

$$a = \frac{1}{4} + \frac{1}{6} \; ; \quad b = \frac{3}{10} + \frac{5}{6} \; ; \quad c = \frac{1}{4} - \frac{5}{6}.$$

5 Congruences

1. Vrai ou faux
a. si $a \equiv b$ [pq], alors $a \equiv b$ [q].
b. si $a \equiv b$ [q], alors $a \equiv b$ [pq].
c. si $a \equiv 2$ [7], alors $a^2 \equiv 4$ [7].
d. si $a^2 \equiv 4$ [7], alors $a \equiv 2$ [7].
e. si $a^2 \equiv 4$ [49], alors $a \equiv 2$ [7].
2. QCM (Choisir la ou les bonnes réponses)
a. Si $a \equiv 2$ [5] et $a \equiv 2$ [7], alors
i. $a \equiv 2$ [35]. ii. $a \equiv 4$ [35]. iii. $a^2 \equiv 4$ [35].
b. Si $a \equiv 2$ [4] et $a \equiv 2$ [6], alors
i. $a \equiv 4$ [24]. ii. $a \equiv 2$ [12]. iii. $a^2 \equiv 4$ [24].

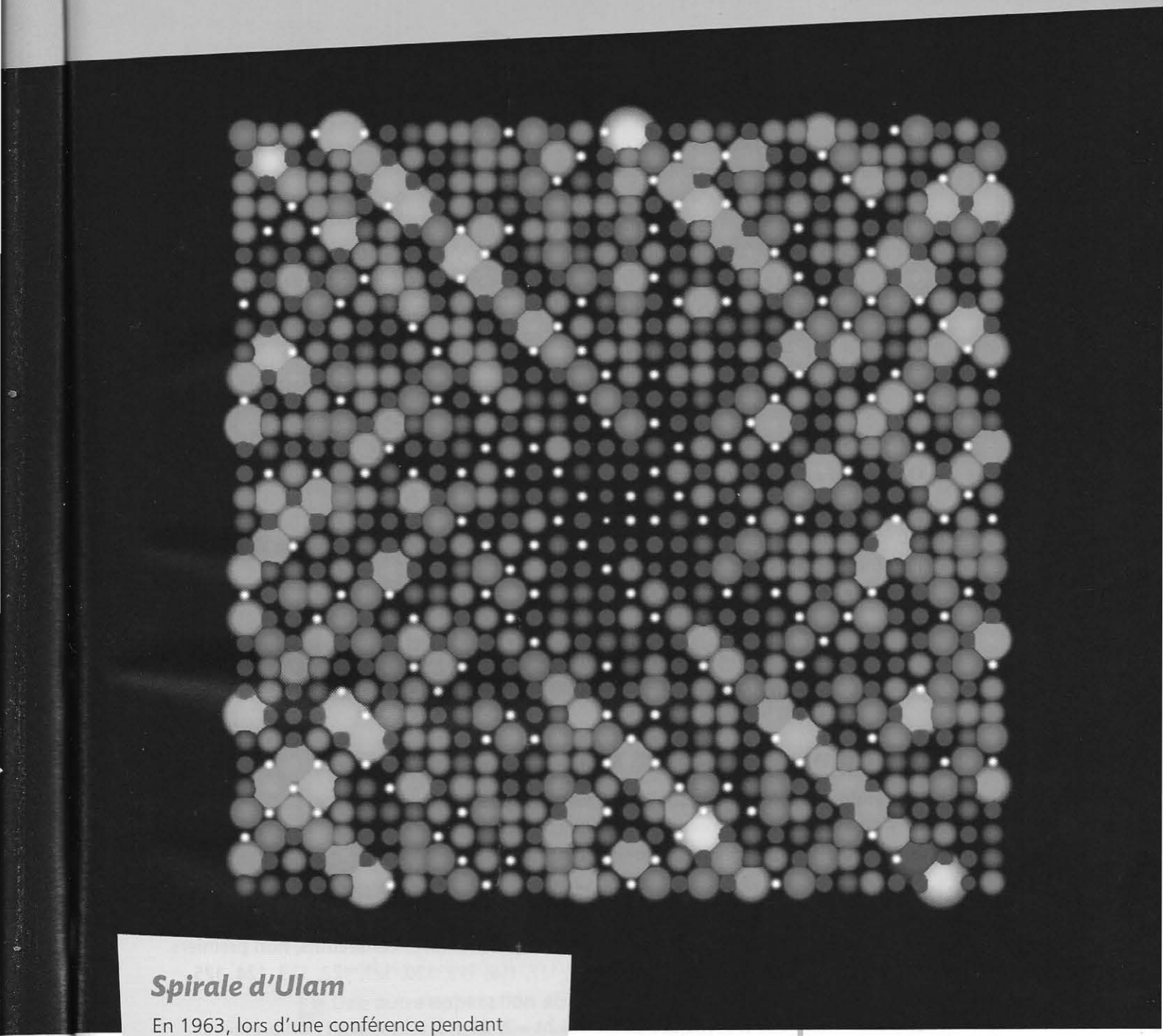
6 Théorèmes de Bézout et de Gauss

1. Vrai ou Faux a, b, c, u et v sont des entiers.
a. Si a divise b et est premier avec bc, alors a divise c.
b. Si a et b sont premiers entre eux, alors pour tout couple $(u ; v)$, $au + bv = 1$.
c. a et b sont premiers entre eux si et seulement si il existe un couple $(u ; v)$ tel que $au + bv = 1$.
d. Si a divise bc et est premier avec b, alors a divise c.
2. n est un entier naturel. Les nombres suivants sont-ils premiers entre eux ?
a. n et $2n + 1$. **b.** $4n + 3$ et $3n + 2$.
c. $5n + 2$ et $4n + 3$. **d.** $5n + 2$ et $4n + 1$.
3. Les équations suivantes ont-elles des solutions entières ?
a. $3x - 5y = 1$. **b.** $4x + 6y = 1$.
c. $3x + 2y = 19$. **d.** $6x + 9y = 3$.

Algorithmique

4. Écrire un algorithme permettant de trouver des coefficients de Bézout $(u ; v)$ tels que $au + bv = 1$, avec a et b premiers entre eux.

5. Déterminer une solution particulière entière des équations suivantes :
a. $7x + 4y = 1$; **b.** $7x - 5y = 1$;
c. $7x + 4y = 3$; **d.** $7x - 5y = 8$.



La spirale d'Ulam généralisée montrant 1 024 nombres entiers générée par Jean-François Colonna.

Spirale d'Ulam

En 1963, lors d'une conférence pendant laquelle il s'ennuie, le mathématicien polonais Stanislaw Ulam dessine une grille où il place les nombres entiers en commençant par le 1 au centre puis selon une spirale tournant dans le sens inverse des aiguilles d'une montre. En noircissant les nombres premiers, il s'aperçoit que ces derniers tendaient à s'aligner selon des diagonales. Persuadé que ces dessins n'aboutiraient à rien, Ulam abandonna ses investigations sur la répartition des nombres premiers.

? ***Une autre façon de mettre en évidence des alignements obliques est de tracer au-dessus de chaque nombre, un disque de diamètre égal à son nombre de diviseurs. Quel sera alors le diamètre du disque représentant les nombres premiers ?***

Activités d'introduction

Activité 1 Crible d'Ératosthène

Objectifs
Revoir : la définition de nombres premiers.
Découvrir : le crible d'Ératosthène.

Un peu d'histoire...
Ératosthène (276-194) av. J.-C. était un mathématicien grec contemporain d'Archimède. Il mit au point une table des nombres premiers inférieurs à un nombre N donné.

Un entier naturel p est premier s'il admet exactement deux diviseurs, 1 et lui-même. 1 est donc non premier. Si un nombre a au moins trois diviseurs, il est dit composé.
On rentre dans un tableau tous les nombres de 1 à N (ici, $N = 100$).
On va éliminer, en les barrant, tous les nombres composés. 1 est non premier, donc barré. 2 est premier, mais tous ses multiples sont composés. On les barre donc.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21									30
31									40
41									50
51									60
61									70
71									80
81									90
91									100

1. Expliquer pourquoi 3 est premier.
2. Recopier la grille et la remplir en éliminant tous les multiples de 3. Pourquoi le premier multiple de 3 à barrer est-il 3^2 ?
3. Quel est le suivant non barré ? Pourquoi est-il premier ?
4. Quand s'arrêter pour être sûr que tous les nombres restants dans le tableau soient premiers ?
5. Pour trouver tous les nombres premiers inférieurs à 400, quelle doit être la dimension du tableau à construire ? Où s'arrêter ?
6. Refaire le tableau pour trouver les nombres premiers inférieurs à 400.

Activité 2 Les nombres premiers se raréfient-ils ?

1. Reprendre le tableau de l'activité précédente, question 6.
   a. Y a-t-il des nombres premiers impairs consécutifs ?
   b. Quelle est la plus grande séquence sans nombre premier ?
2. **Question : Existe-t-il des intervalles de longueur n donnée sans aucun nombre premier ?**
   a. Vérifier que {24, 25, 26, 27, 28} est formé de 5 nombres consécutifs, non premiers.
   b. Vérifier que l'ensemble {114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126 } est formé de 13 nombres consécutifs, non premiers.
   c. $24 = 1 \times 2 \times 3 \times 4$. Expliquez pourquoi $24 + 2$, $24 + 3$, $24 + 4$ sont non premiers.
   d. De manière générale, on pose $n\ ! = 1.2.3.\ldots\ldots n$, le produit des n entiers consécutifs, inférieurs ou égaux à n. Montrer que pour tout entier k compris entre 2 et $n + 1$, $(n + 1)\ ! + k$ n'est pas un nombre premier. On a ainsi construit un ensemble de n nombres consécutifs composés.

Objectif
Découvrir : la répartition des nombres premiers.

3. **Mais existe-t-il un nombre premier plus grand que tous les autres ?**
   a. Que dire de $n\ ! + 1$?
   b. En utilisant la propriété que tout entier supérieur ou égal à deux admet un diviseur premier, quelle inégalité a-t-on entre n et un diviseur premier de $n\ ! + 1$? Que peut-on en conclure ?

Commentaire
Un mathématicien russe, Tchebichev (1821-1894), a montré que, quelque soit n, il y a au moins un nombre premier entre n et $2n$. Ce résultat est connu sous le nom de « Postulat de Bertrand ».

Activité 3 Des nombres premiers particuliers

Objectif
Découvrir: des nombres premiers particuliers.

Les mathématiciens ont tenté de trouver des critères de primalité. Par exemple, les nombres de Mersenne.

1 Soit a un entier supérieur ou égal à 2.
a. $a \geqslant 3$. Montrer en utilisant soit les congruences, soit l'identité suivante : $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$, que, quelque soit $n \geqslant 2$, a^{n-1} n'est pas premier.
b. Que dire si $a = 2$?

Un peu d'histoire...
« Les mathématiciens ont tenté en vain jusqu'à ce jour de découvrir une régularité dans la suite des nombres premiers et nous avons de bonnes raisons de croire qu'il y a là un mystère que l'esprit humain ne pénètrera jamais. »
Léonard Euler (1707-1783).



2 Les nombres de la forme $M_n = 2^n - 1$ ont été étudiés par Mersenne et ont pris son nom.
a. Déterminer les 12 premiers nombres de Mersenne.
b. Parmi ceux-ci, lesquels sont premiers ? (On pourra utiliser un logiciel adapté : Xcas par exemple).
c. Montrer, en utilisant l'identité rappelée au 1., que si n est composé ($n = km$), alors M_n est divisible par $2^k - 1$. Que peut-on en déduire ?
d. i. Vérifier que M_{11} admet deux diviseurs premiers de la forme $22k + 1$.
ii. Si p est premier, M_p est il premier ?

Activité 4 Divisibilité d'un produit et nombre premier

Objectif
Découvrir: des propriétés et des applications des nombres premiers.

1 **Une propriété des nombres premiers**
a. Quels sont les entiers naturels inférieurs à 7, premiers avec 7 ? Quels sont les autres nombres premiers avec 7 ?
b. Avec quels nombres p premier est-il premier ?

2 **Une application du théorème de Gauss**
a. Rappeler le théorème de Gauss.
b. Soient a et b deux entiers naturels et $n = ab$. On suppose que n admet un diviseur premier p. Montrer que si p ne divise pas a, alors il divise b.
c. En déduire que si un nombre premier p divise un produit de nombres premiers, il est l'un d'eux.

Commentaire
Ce résultat se généralise : Un nombre premier divisant un produit d'entiers, divise au moins l'un d'eux.

3 **Une autre application du théorème de Gauss**
Soient p et q deux diviseurs premiers distincts d'un entier naturel n.
a. Montrer qu'ils sont premiers entre eux.
b. Montrer qu'il existe deux entiers naturels u et v tels que $n = up = qv$.
c. Montrer que q divise u. En déduire que pq divise n.

Commentaire
Un nombre divisible par deux nombres premiers distincts l'est par leur produit.

4 **Un exemple : les coefficients binomiaux**
a. Donner les valeurs des coefficients binomiaux $\binom{n}{k}$ pour $n \leqslant 6$ et $1 \leqslant k \leqslant n-1$.
Dans quel cas n divise-t-il $\binom{n}{k}$ pour tout k tel que $1 \leqslant k \leqslant n-1$?
b. Soit p un nombre premier. On rappelle que si $p \geqslant k$, $k!\binom{p}{k} = p(p-1)\ldots(p-k+1)$.
Montrer que si $1 \leqslant k \leqslant p-1$, p est premier avec $k!$ En déduire que p divise-t-il $\binom{p}{k}$.

Activités d'introduction

Activité 5 Pratique de la décomposition d'un entier en produits de facteurs premiers

Objectifs
Revoir : la décomposition en facteurs premiers et les diviseurs.
Découvrir : la recherche du nombre de diviseurs.

1 L'idée est de diviser un nombre successivement par tous ses diviseurs premiers, en commençant par le plus petit.
On considère le nombre 1 274.
1 274 est pair et $1\,274 = 2 \times 637$.
Il n'est divisible ni par 3, ni par 5. Essayons par 7.
$637 = 7 \times 91$ et $91 = 7 \times 13$.

1 274	2
637	7
91	7
13	13
1	

a. Donner alors la décomposition de 1 274 en produit de puissances de facteurs premiers.
b. Quel est le plus petit entier qui, multiplié par 1 274, donne un carré ?

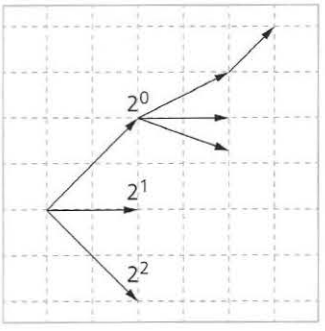
2 Dans certains cas, en utilisant les caractères de divisibilité, on peut aller beaucoup plus vite.
Soit $N = 198\,900$.
a. N est clairement le produit de deux nombres premiers entre eux. Lesquels ?
b. En déduire la décomposition de N en facteurs premiers.

3 **Application à la recherche de diviseurs**
a. Soit $n = 2^7$.
i. Quelle est la forme générale des diviseurs de n ?
ii. Quel est le nombre de diviseurs de n ?
iii. Quelle est la somme de tous les diviseurs de n ?
b. Soit p un nombre premier et k un entier naturel. Reprendre les questions du **1.** avec $n = p^k$.
c. Montrer que $864 = 2^5 \times 3^3$.
i. soit d un diviseur de 864. Montrer qu'il existe α et β deux entiers tels que $0 \leqslant \alpha \leqslant 5$ et $0 \leqslant \beta \leqslant 3$ et tels que $d = 2^\alpha \times 5^\beta$.
ii. Recopier et compléter le tableau ci-dessous.

$\times$	2^0	2^1	2^2	2^3	2^4	2^5
5^0	1					32
5^1						
5^2						
5^3	125					864

Quel est le nombre total de diviseurs de 864 ?
iii. Si $n = 2^\alpha \times 5^\beta$, quel est le nombre de diviseurs de n ?

4 **a.** Décomposer $N = 24\,500$ en produit de puissance de facteurs premiers.
b. Quelle est la forme générale des diviseurs de N ?
c. Quel est le nombre de diviseurs ?
d. Parmi tous ces diviseurs, quelles sont les paires de diviseurs premiers entre eux ?
e. Construire un arbre de diviseurs et retrouver tous les diviseurs.



Activité 6 Le système RSA

Objectif
Découvrir : un système de codage à clé publique.

Principe

Le système RSA est un système de codage à clé publique, c'est-à-dire connue de tous.



Principe du code RSA

Alice a plusieurs correspondants, dont Bob, et elle souhaite être la seule à connaître le contenu des messages envoyés par ses différents correspondants. Dans un premier temps, nous nous limitons à l'envoi d'un nombre de Bob à Alice : Bob code ce nombre et Alice le déchiffre.

Alice choisit deux entiers n et c (on verra comment ultérieurement) et elle les rend publics en les communiquant à tous ses correspondants ou même en les mettant sur son site web : (RSA, n, c). C'est la clé publique.

1 **a.** Bob, sur le site web d'Alice, trouve (RSA, 33, 7) ; il souhaite envoyer le nombre $a = 2$ à Alice. a doit être choisi inférieur ou égal à 32.

Le codage : Bob forme un nombre b, (en général compris entre 1 et n, ici entre 1 et 33) congru à 2^c modulo n. Quel nombre va-t-il former dans ce cas ?

b. Alice reçoit ce nombre b envoyé par Bob.

Le déchiffrage : Il suffit qu'Alice possède un entier d, évidemment lui tenu secret, tel que a soit congru à b^d modulo n. a est donc l'entier compris entre 1 et n, congru à b^d modulo n. Essayer avec $d = 3$.

c. Bob souhaite envoyer cette fois 5 ; recommencer la procédure, que constatez-vous ?

2 Comment Alice a-t-elle procédé ?

a. Alice a choisi un entier $n = pq$ produit de deux nombres premiers différents ; lesquels ici ?

b. Alice a choisi en outre un autre entier c, $2 \leqslant c < (p - 1)(q - 1)$, premier avec $(p - 1)(q - 1)$; lequel ?

c. Alice communique à tous (clef publique) le couple (n, c) ; toute personne sait alors envoyer à Alice un nombre codé par le procédé de **1a**.

d. Pour décoder, Alice utilise un nombre d, secret, (c'est la clef privée), qui vérifie cd est congru à 1 modulo $(p - 1)(q - 1)$. Vérifier cette propriété dans le cas particulier de **1**.

Dans le TP2 p. 89, on démontrera pourquoi ces choix permettent à Alice de déchiffrer le nombre envoyé par Bob et on expliquera comment ce procédé permet alors de transmettre un message.

Commentaire

Le système de cryptographie RSA est considéré comme le code public le plus sûr.
Cette méthode a été créée en 1977 par Rivest, Shamir et Adleman, d'où le nom de RSA.
Il est utilisé dans le monde entier et sert aujourd'hui à des protections de toutes sortes notamment dans les cartes bancaires.
Sa sécurité est assurée par deux faits :

- les tests de primalité, qui sont très performants, permettent de trouver deux nombres premiers p et q très grands et ainsi de prendre $n = pq$ très grand. Prendre un nombre c est facile ;
- au contraire, il est très difficile de factoriser un nombre et la connaissance de n et de c ne permet pas de retrouver p et q et donc le nombre d indispensable pour décoder.

Actuellement, le plus grand nombre premier est un nombre de Mersenne, avec $p = 43\,112\,609$, qui a 12 978 189 chiffres en écriture décimale. Il fut découvert en 2008.

A Définition et premières propriétés

Dans ce chapitre, nous n'envisageons que des entiers naturels non nul.

1 Premières définitions

Définition 1

Un entier naturel p est premier s'il admet exactement deux diviseurs, 1 et lui-même. Un nombre ayant au moins trois diviseurs est dit composé.

Note : Les nombres pairs, excepté 2, sont tous divisibles par 2, donc ils sont composés.

EXEMPLES : • 1 n'admet qu'un seul diviseur, 1, donc 1 n'est pas premier.
• 2 admet pour diviseur 1 et 2 ; 2 est donc premier.

2 Test de primalité

Propriété 1

Tout entier naturel n supérieur ou égal à 2 admet au moins 1 diviseur premier.

Note : $p = n$ si, et seulement si, n est premier.

DÉMONSTRATION : On considère l'ensemble des diviseurs de n supérieurs ou égaux à 2. Cet ensemble est non vide car il contient n. Il admet donc un plus petit élément p, nécessairement premier.

Propriété 2

Si n est supérieur ou égal à 2 et n'est pas premier, il admet au moins un diviseur premier p tel que $p \leqslant \sqrt{n}$.

DÉMONSTRATION : Soit n non premier et p le plus petit diviseur premier vérifiant donc $2 \leqslant p < n$, puisque n est non premier.
p divise n, donc il existe un entier naturel q tel que $n = pq$. q est un diviseur propre de n, c'est-à-dire différent de n, donc $q \geqslant p$ et $n \geqslant p^2$. Ainsi, $p \leqslant \sqrt{n}$.

Propriété 3

Test de primalité. Si un entier naturel n n'est divisible par aucun nombre premier inférieur à sa racine carrée, il est premier.

EXEMPLES : 5 est impair, donc non divisible par 2 et $3^2 > 5$, donc 5 est premier.

3 Propriétés des nombres premiers

Propriété 4

Soient p un nombre premier et n un entier naturel. Alors p divise n ou p premier avec n. En particulier, un nombre premier p est premier avec tout nombre qui lui est strictement inférieur.

Propriété 5

Si p premier divise $a \times b$, alors p divise a ou p divise b.

DÉMONSTRATION : Cf. exercice 9 p. 90.

Conséquences : 1. si p premier divise un produit, il divise au moins un des facteurs.
2. si p premier divise un produit de nombres premiers, il est l'un d'eux.

Propriété 6

L'ensemble des nombres premiers est infini.

DÉMONSTRATION : Cf. exercice 33 p. 91.

Savoir-faire 1 Composé ou premier ?

→ Exercice corrigé 22 p. 91
→ Exercices d'application 23 à 32 p. 91

Énoncé

1. Justifier que les nombres suivants sont composés :
a. 14 751.
b. $6k + 2$ tout entier naturel k non nul.
c. $4^n - 1$ pour tout entier naturel supérieur ou égal à 2.
d. $10^{2\,011} + 1$.
2. 2 011 est-il premier ?

Méthode

Utiliser :
1. a. les caractères de divisibilité vus au chapitre 1 ;
b. la factorisation ;
c. l'identité :
$(a^n - 1) = (a - 1)(a^{n-1} + \ldots\ldots + a + 1)$;
d. les congruences.
2. Test de primalité.

Solution

1. a. La somme des chiffres de 14 751 est 18, il est donc divisible par 9, donc composé.
b. $6k + 2 = 2(3k + 1)$, donc si $k > 0$, $3k + 1 >$. Ainsi, $6k + 2$ est composé.
c. $4^n - 1 = (4 - 1)(4^{n-1} + \ldots\ldots + 4 + 1) = 3(4^{n-1} + \ldots\ldots + 4 + 1)$. Si $n \geqslant 2$, $4^{n-1} + \ldots\ldots + 4 + 1 > 5$, donc $4^n - 1$ est composé.
On peut aussi utiliser les congruences modulo 3, car $4 \equiv 1[3]$. Pour tout n, $4^n \equiv 1[3]$, donc 3 divise $4^n - 1$, qui est composé si $4^n - 1 \geqslant 4$, à savoir $n \geqslant 2$.
d. $10 \equiv -1\ [11]$, donc par compatibilité des congruences avec les puissances, $10^{2\,011} \equiv (-1)^{2\,011}\ [11]$.
Or $(-1)^{2\,011} = -1$, donc $10^{2\,011} + 1$ est divisible par 11, donc composé.

2. 2 011 n'est divisible ni par 2, ni par 3, ni par 5, ni par 11, par les critères de divisibilité.
$2\,011 = 7 \times 287 + 2 = 13 \times 154 + 9 = 17 \times 118 + 5 = 19 \times 105 + 16 = 23 \times 87 + 10$
$= 29 \times 69 + 10 = 31 \times 64 + 27 = 37 \times 54 + 13 = 41 \times 49 + 2 = 43 \times 46 + 33.$
Aucun reste n'est nul. De plus $44 < \sqrt{2\,011} < 45$. 2 011 n'admet aucun diviseur premier inférieur à sa racine carrée. 2 011 est donc premier.

Savoir-faire 2 Utilisation de la notion de nombre premier

→ Exercice corrigé 34 p. 91
→ Exercices d'application 35 à 41 p. 91

Énoncé

a. Soient a et b deux nombres entiers naturels tels que $p = 2a + 3b$ soit un nombre premier. Montrer que a et b sont premiers entre eux.
b. Soit p un nombre premier. Trouver tous les couples d'entiers naturels $(a ; b)$ tels que $a^2 - b^2 = p$.

Solution

a. Soit d un diviseur commun à a et b. d divise alors toute combinaison linéaire de a et b donc $2a + 3b$, donc d divise p.
Or p n'a que 2 diviseurs 1 et p et $a < p$ donc $d < p$. On en déduit que $d = 1$ et que a et b sont premiers entre eux.
b. $a^2 - b^2 = (a - b)(a + b)$.
Or p premier n'admet qu'une seule décomposition dans N : $p = 1 \times p$.
D'autre part, si $(a ; b)$ est solution, alors $a > b$ et $a - b < a + b$.
On en déduit que a et b sont solutions du système : $\begin{cases} a - b = 1 \\ a + b = p \end{cases} \Leftrightarrow \begin{cases} 2a = p + 1 \\ 2b = p - 1 \end{cases}$.
Si $p = 2$, le système n'a pas de solution.
Si $p > 2$, alors p est impair et $p - 1$ et $p + 1$ sont pairs.
Le seul couple solution est $\left(\frac{p+1}{2}, \frac{p-1}{2}\right)$.

B Décomposition en facteurs premiers

1 Décomposition d'un entier en produit de facteurs premiers

Propriété 7

Tout entier supérieur ou égal à deux est un produit de nombres premiers.
Cette écriture porte le nom de « décomposition en facteurs premiers ».

Démonstration : Soit n un entier supérieur ou égal à 2.
Soit P_n la proposition : Tout entier k avec $2 \leqslant k \leqslant n$ admet une décomposition en facteurs premiers. P_2 est vraie : 2 est premier. Supposons P_n vraie.
$n + 1$ admet un diviseur premier p_1 ; $p_1 \geqslant 2$ et donc $n + 1 = p_1 \times n_1$, avec $2 \leqslant n_1 \leqslant n$.
Par P_n, n_1 admet une décomposition en facteurs premiers donc $P_n + 1$ est vraie

Remarque : les entiers p_i ne sont pas nécessairement distincts. En regroupant, la décomposition s'écrit alors : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots\ldots \times p_s^{\alpha_s}$, avec $1 < p_1 < \ldots\ldots\ldots < p_s$, premiers distincts et α_i entier, $\alpha_i \geqslant 1$
Désormais on écrira une décomposition sous cette forme.

Propriété 8

Cette décomposition est unique, à l'ordre des nombres premiers près.

Démonstration : Supposons que $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots\ldots \times p_s^{\alpha_s} = q_1^{\beta_1} \times q_2^{\beta_2} \times \ldots\ldots\ldots \times q_r^{\beta_r}$ avec $1 < q_1 < \ldots\ldots\ldots < q_r$
p_1 divise $q_1^{\beta_1} \times q_2^{\beta_2} \times \ldots\ldots\ldots \times q_r^{\beta_r}$ donc par le théorème 5, il existe k tel que $p_1 = q_k \geqslant q_1$ et de même, il existe l tel que $q_1 = p_l \geqslant p_1$ donc $p_1 = q_1$. La démonstration se termine alors par une récurrence analogue à la précédente.

2 Applications de la décomposition

Propriété 9

Soient a et b deux entiers supérieurs ou égaux à 1.
Si $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots\ldots \times p_s^{\alpha_s}$, $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots\ldots\ldots \times p_s^{\beta_s}$ ou $p_1, \ldots, p_s$ sont des nombres premiers distincts et α_i et β_i entiers des entiers positifs ou nuls, alors b divise a si, et seulement si, pour tout i, $0 \leqslant \beta_i \leqslant \alpha_i$.

Démonstration : Voir exercice 85 p. 95.

Conséquences : Si n, entier naturel supérieur ou égal à 2 se décompose en $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots\ldots \times p_s^{\alpha_s}$, alors tous les diviseurs positifs de n sont de la forme $d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots\ldots\ldots \times p_s^{\beta_s}$, avec β_i entier, $0 \leqslant \beta_i \leqslant \alpha_i$
et n admet $(\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_s + 1)$ diviseurs supérieurs ou égaux à 1.

Propriété 10

PGCD de deux entiers.
Soient $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots\ldots \times p_s^{\alpha_s}$, $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots\ldots\ldots \times p_s^{\beta_s}$ où $p_1, \ldots, p_s$ sont des nombres premiers distincts et α_i et β_i entiers des entiers positifs ou nuls.
Alors PGCD$(a, b) = p_1^{\gamma_1} \times p_2^{\gamma_2} \times \ldots\ldots\ldots \times p_s^{\gamma_s}$ avec $\gamma_i = \min(\alpha_i, \beta_i)$.

Savoir-faire 3 Utiliser le théorème de Gauss avec des nombres premiers

→ Exercice corrigé 42 p. 92
→ Exercices d'application 43 à 46 p. 92

Énoncé

1. a. Soit p un nombre premier. Montrer que $ab \equiv 0\ [p]$ équivaut à $a \equiv 0\ [p]$ ou $b \equiv 0\ [p]$
b. En déduire que pour tout entier n premier avec p, $na \equiv nb\ [p]$ équivaut à $a \equiv b\ [p]$
2. Soit p un nombre premier et $A_p = \{1, 2, \ldots, p-1\}$
Montrer que pour tout a de Ep, l'équation $ax \equiv 1\ [p]$ a une unique solution dans A_p.

Méthode

La division n'existe pas dans les congruences et on ne peut pas utiliser de raisonnement par équivalence.

Solution

1. a. $a.b \equiv 0\ [p]$ signifie que p divise ab. Or p premier, donc p divise a ou p divise b donc $a \equiv 0\ [p]$ ou $b \equiv 0\ [p]$.
Réciproquement : si $a \equiv 0\ [p]$ ou $b \equiv 0\ [p]$, par produit, $a.b \equiv 0\ [p]$.
b. Si $a \equiv b$ [p], alors par produit, $n.a \equiv n.b$ [p]
Réciproquement, si $n.a \equiv n.b\ [p]$, par somme, $n.a - nb \equiv 0\ [p]$, d'où,
$n(a-b) \equiv 0\ [p]$. Or p ne divise par n donc p divise $a-b$ donc $a \equiv b\ [p]$.
2. p est premier avec a donc, d'après le théorème de Bézout, l'équation $ax + py = 1$ a des solutions et il existe un entier x_0 tel que $ax_0 \equiv 1\ [p]$. Soit r le reste dans la division de x_0 par p.
$x_0 \equiv r\ [p]$ donc $ax_0 \equiv ar\ [p]$ donc $ar \equiv 1\ [p]$ et avec r non nul (sinon p diviserait ax_0 donc 1) élément de A_p.
Supposons qu'il existe r' élément de Ap tel que $ar' \equiv 1\ [p]$. Dans ce cas, $ar \equiv ar'\ [p]$
D'après 1., $r \equiv r'\ [p]$ donc p divise $r - r'$.
Or $-(p-1) \leqslant r - r' \leqslant p - 1$ donc $r - r' = 0$ et l'unicité est démontrée.

Savoir-faire 4 Les applications de la décomposition

→ Exercice corrigé 55 p. 92
→ Exercices d'application 56 à 59 p. 92

Énoncé

1. Trouver tous les diviseurs de 120.
2. a. Décomposer en facteurs premiers $a = 17\,640$ et $b = 4\,116$.
b. Déterminer le plus petit entier c tel que bc soit un carré parfait.
c. Déterminer PGCD(a, b).
d. Simplifier la fraction $q = \frac{a}{b}$ et calculer $S = \frac{1}{a} + \frac{1}{b}$.

Méthode

1. Utiliser la formule pour trouver le nombre de diviseurs. Ainsi on est sûr de ne pas en oublier.
2. pour simplifier une fraction, on divise numérateur et dénominateur par leur PGCD.
Pour additionner deux fractions, on trouve un dénominateur commun.

Solution

1. $120 = 10 \times 12 = 2 \times 5 \times 4 \times 3 = 2^3 \times 3 \times 5$. 120 a donc $4 \times 2 \times 2 = 16$ diviseurs.
Les diviseurs de 120 sont : 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30,40, 60, 120
2. a. La décomposition en facteurs premiers de a et b donne :
$a = 2^3 \times 3^2 \times 5 \times 7^2$ et $b = 2^2 \times 3 \times 7^3$.
b. Un carré parfait a tous ses exposants pairs, donc si $c = 3 \times 7$,
alors $bc = 2^2 \times 3^2 \times 7^4 = (2 \times 3 \times 7^2)^2$.
c. $d = \text{PGCD}(a, b) = 2^2 \times 3 \times 7^2 = 588$.
d. Soient a' et b' tels que $a = da'$, $b = db'$. $a' = 2 \times 3 \times 5 = 30$, $b' = 7$
donc $q = \frac{a}{b} = \frac{a'}{b'} = \frac{30}{7}$.
$s = \frac{1}{a} + \frac{1}{b} = \frac{1}{da'} + \frac{1}{db'} = \frac{b'}{da'b'} + \frac{a'}{da'b'} = \frac{b'+a'}{da'b'} = \frac{37}{123\,480}$.

TP Algorithmique 1 Nombres premiers ?



Objectif :
- *Utiliser le tableur et programmer sur la calculatrice un algorithme.*

1 Approche du problème

a. Rappeler les caractères de divisibilité par 2 et par 3.

b. Montrer que si p est premier, $p \geqslant 5$, il est de la forme $6k - 1$ ou $6k + 1$.

c. Soit n un nombre entier, $n \geqslant 5$. Montrer que pour dire s'il est premier ou non, il suffit de le diviser par 2, par 3, puis successivement par les entiers de la forme $6k - 1$ ou $6k + 1$.

2 Avec un tableur

On veut tester si 399 601 est premier.

k	$6k-1$	$6k+1$	399601	632
	2	3	1	1
1	5	7	1	6
2	11	13	4	7
3	17	19	16	12
4	23	25	22	1
5	29	31	10	11
6	35	37	6	1
7	41	43	15	2

Pour tester la divisibilité par 2 et 3, en B2 et C2, on entre 2 et 3.

a. Quelles formules en B3, C3 pour générer les entiers naturels de la forme $6k - 1$ et $6k + 1$?

b. En D1, on rentre le nombre N à tester et en E1 la partie entière de sa racine carrée. Quelle formule entrer en D2 et pour obtenir le reste dans la division de N par les nombres de la colonne B ?

c. Si N est divisible par un nombre des colonnes B ou C, comment sera le reste de la colonne E ? Conclure.

3 Avec un algorithme et des logiciels de calcul formel

```
Demander N
Initialiser T à 1
Tantque T² ⩽ N faire
   Si a/n = E(a/n)
   Afficher n et a/n
   Remplacer T par T + 1
Fin
```

a. Que fait cet algorithme ?

b. Implanter le programme sur une calculatrice.

c. 12319 est il premier ?

Avec la calculatrice TInspire ou TI 89, entrer isprime (n)

Pour tester si un nombre est premier avec les logiciels :

Scilab	Premier(n)
Xcas	Isprime(n)
Maxima	Primep(n)
Derive	PRIME ?(n)

4 De la répartition des nombres premiers

a. On note $\pi(N)$ le nombre de nombres premiers inférieurs à un nombre donné.

i. Déterminer à l'aide du crible d'Ératosthène $\pi(N)$, pour N = 10, N = 100.

ii. Dans ces deux cas, calculer la densité de répartition $\frac{\pi(N)}{N}$.

iii. Modifier l'algorithme précédent pour qu'il donne $\pi(N)$, puis $\frac{\pi(N)}{N}$.

b. La table suivante donne les valeurs de $\pi(N)$ pour des valeurs de N.

N	10	10^2	10^3	10^4	10^6	10^8	10^{10}	10^{20}
$\pi(N)$		25	168	1 229	78 498	50 847 534	455 052 512	2 220 819 602 560 918 840

Calculer dans chacun des cas $\frac{\pi(N)}{N}$, puis $\frac{\ln(N)\pi(N)}{N}$.

Que constate-t-on ?

TP Algorithmique 2 Nombres parfaits



Objectif :
- *Chercher les diviseurs d'un entier naturel sur un problème historique.*

On appelle nombre parfait un nombre entier n égal à la somme de ses diviseurs propres, c'est-à-dire autre que lui-même, ce qui revient à dire que si $s(n)$ désigne la somme des diviseurs positifs de n, alors $s(n) = 2n$.
Exemple : $6 = 1 \times 6 = 2 \times 3$. Ses diviseurs propres sont 1, 2, 3 dont la somme fait 6 donc 6 est parfait.

1 Vérifier que à la main que 28 est parfait.

2 Ci-contre figure un algorithme.
a. Que fait-il ?
b. Comment le modifier pour :
i. Dire si un nombre donné est parfait ?
ii. Trouver les premiers nombres parfaits inférieurs à 10 000 ?

```
Variables : N, D, X entiers, N≥1., L1 liste
Début
Entrer N, Effacer liste L1,
   X=1, D=1
Tantque √N ≥ D faire :
   Si partie décimale de (N/D)=0
      L1(X)=D
      Si N=D² alors
         X=X+1
         L1(X)=N/D
      FinSi
   X=X+1
   FinSi
   D=D+1
FinTantque
Tri croissant de L1
Afficher L1
```

3 On trouve que 496 et 8 128 sont parfaits.
a. Vérifier que pour chacun de ces nombres N, il existe un entier n tel que $N = 2^{n-1}(2^n - 1)$.

4 **a.** Soit n un entier naturel non nul. Déterminer les diviseurs de 2^{n-1}.
b. On suppose que $p = 2^n - 1$ est premier. Quels sont ses diviseurs ?
c. En déduire les diviseurs de $N = 2^{n-1}(2^n - 1)$.
d. Démontrer que N est parfait.

5 **Une propriété des nombres parfaits : division harmonique**
On dit qu'un entier naturel non nul N est en division harmonique si le quotient du nombre de diviseurs de N par la somme des inverses des diviseurs de N est un entier naturel.
Par exemple : 6 admet 4 diviseurs qui sont 1 ; 2 ; 3 et 6.
La somme des inverses des diviseurs de 6 vaut: $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 2$.
Le quotient $\frac{4}{2} = 2$ est un entier. 6 est donc en division harmonique.
a. En utilisant et adaptant l'algorithme précédent, dire si les nombres 32 et 140 sont en division harmonique.
b. Faire calculer la somme des inverses des diviseurs de n, pour les quatre premiers nombres parfaits. Que peut-on conjecturer ?
c. Soit p un nombre premier. Montrer que p n'est pas en division harmonique.
d. On suppose que $p_n = 2^n - 1$ est premier. On pose $a_n = 2^{n-1}p_n$.
i. Donner la liste des diviseurs de a_n en fonction de p_n.
ii. Que peut-on conclure si la somme des inverses des diviseurs de a_n vaut 2 ?

Commentaire

Cette démonstration est due à Euclide, mais il n'a pas étudié la réciproque.
Euler s'est intéressé aux nombres parfaits pairs et il a montré qu'ils étaient de la forme étudiée par Euclide.
Quand aux nombres parfaits impairs, on n'a pas à ce jour prouvé leur existence.

Remarque : La recherche des nombres parfaits est à relier à la recherche des nombres de Mersenne premiers.

TP TICE 1 Un test de non primalité



Objectif :
- *Découvrir un théorème important et des tests.*

1 Soit m un nombre entier naturel et A_m l'ensemble des entiers naturels compris entre 1 et $m - 1$. On veut étudier si pour tout n élément de A_m, $n^m - n$ est divisible par m. On appelle Q_m cette proposition.

a. Q_m est-elle vraie pour $m = 2$ et $m = 3$?

b. Q_4 est-elle vraie ?

c. On pose $m = 5$. Déterminer A_5. À l'aide d'un tableur, construire le tableau donnant les congruences modulo 5 des puissances de a. Pour construire le tableau, on utilise la fonction MOD du tableur en remarquant que $n^{k+1} = n.n^k$. Vérifier que pour tout n de A_5, $n^5 \equiv n$ [5].

$n =$	1	2	3	4
$k = 1$	1	2	3	4
2	1	4	4	1
3	1	3		
4	1	1		
5	1	2		

d. Refaire la même chose pour m de 6 à 11. Pour quelles valeurs de m, Q_m est-elle vraie ?

2 Dans la suite, p est un nombre premier. On veut montrer que pour tout entier naturel n, n divise $n^p - n$.
On appelle P_n cette proposition.

a. Montrer que P_0 est vraie.

b. On suppose que P_n est vraie.
En utilisant la formule dite du binôme $(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$, montrer que $(n + 1)^p - (n + 1) = n^p - n + \sum_{k=0}^{p-1} \binom{p}{k} n^k$.

c. Démontrer (voir Activité 4) que pour $1 \leqslant k \leqslant p - 1$, p divise $\binom{p}{k}$. Conclure.

Commentaire
Ce résultat est connu sous le nom de « petit théorème de Fermat ».

3 Un test de non primalité

a. Soit m un entier naturel. En utilisant la question 2, montrer que s'il existe n tel que m ne divise pas $n^m - n$, alors m n'est pas premier.

b. Calculer 2^{340} mod (341) ? Peut-on conclure que 341 est premier ?

c. En utilisant un tableur, calculer les restes successifs dans la division par 58 483 de $2^{58\,483}$. 58 483 est-il premier ?

Commentaire
Ce test est connu sous le nom de test de Fermat. Si m ne divise pas $2^m - 2$, m n'est pas premier. En pratique on a recours à l'exponentiation rapide (voir AP3). Il permet de dire si un nombre n'est pas premier, mais on ne sait pas quels sont alors ses diviseurs.

4 Les nombres de Carmichael

On veut répondre à la question : un nombre m tel que pour tout entier n, $n^m \equiv n$ [m] est il premier ?
Étude d'un exemple : $m = 561$.

a. Décomposer 561 en facteurs premiers.

b. Vérifier que 560 est multiple de 2, de 16 et de 10.

c. soit a un entier naturel premier avec 561. On pose $b = a^{561} - a = a(a^{560} - 1)$.
Vérifier $(a^{560} - 1)$ est divisible par $(a^2 - 1)$, par $(a^{10} - 1)$ et par $(a^{16} - 1)$.

d. i. Montrer en utilisant **2.** que $(a^2 - 1)$ est divisible par 3, $(a^{10} - 1)$ par 11 et $(a^{16} - 1)$ par 17.
ii. En déduire que b est divisible par 561.
iii. Étudier le cas où a n'est pas premier avec 561.

Commentaire
Le petit théorème de Fermat ne constitue pas un test de primalité.

TP TICE 2 Le système RSA

Objectif :
- *Comprendre le système RSA.*

On se propose d'expliquer la théorie du système RSA abordée dans l'activité 6.
Le principe est celui d'un codage asymétrique, où la fonction de codage P est publique, P(M) = N, mais la fonction de décodage, S telle que S(N) = M est secrète.
Ces deux fonctions vérifient S(P(M) = P(S(M)) = M.

1 La construction de P et S repose sur le petit théorème de Fermat

Soient p et q deux nombres premiers différents. On forme $n = pq$ et $m = (p - 1)(q - 1)$.

a. Soit a un entier inférieur ou égal à $n - 1$. On veut montrer que pour tout entier naturel k, $a^{1+km} \equiv a\ [n]$

Premier cas : a est premier avec pq	**Deuxième cas** : p divise a
i. Montrer que $a^{(p-1)} \equiv 1\ [p]$, en déduire que $a^{(p-1)(q-1)} \equiv 1\ [p]$.	i. Montrer que $a^{1+km} \equiv a\ [p]$ pour tout entier naturel k.
ii. Montrer, en utilisant le théorème de Gauss que, $a^{(p-1)(q-1)} \equiv 1\ [pq]$	ii. Montrer que a est premier avec q.
iii. En déduire que quel que soit l'entier naturel k, $a^{1+km} \equiv a\ [n]$	iii. En déduire que $a^{1+km} \equiv a\ [q]$
	iv. Montrer enfin que $a^{1+km} \equiv a\ [n]$

b. i. Soit c premier avec m. Montrer, en utilisant le théorème de Bézout, qu'il existe un unique couple (d, k) d'entiers naturels tel que $cd - km = 1$ et $1 \leqslant d \leqslant m - 1$.
ii. En déduire que si a un entier naturel inférieur ou égal à $n - 1$, $a^{cd} \equiv a\ [n]$

2 Le système RSA

a. Bob veut envoyer le nombre M = 152 à Alice qui a publié RSA (12 319, 29). On rappelle que $n = 12\ 319$ et $c = 29$. Il va donc calculer $P(M) = N = 152^{29}\ [n]$, $N < n$.
Vérifier que N = 12 159.
Trois méthodes sont possibles :

A. Utiliser la calculatrice et la suite récurrence $u_{p+1} = \text{Mod}(u_p{*}a, n)$, où Mod (s, n) désigne le reste dans la division euclidienne de s par n.

B. Utiliser un tableur pour représenter la même suite. On entrera en celle A1 le nombre n, en cellule A2 le nombre a, en cellule A3, à nouveau le nombre a. Que doit-on rentrer en A4 pour obtenir par recopie les congruences modulo n des puissances de a ?

C. Utiliser l'algorithme ci-contre :

```
Entrer A, N, C
X = 1
Y = A
Tantque X < c faire
   Mod (AY, N) = Y
   X = X + 1
FinTantque
Afficher Y
```

b. Alice reçoit N. Pour publier son code, elle avait choisi deux nombres premiers p et q, formé $n = pq$, choisi c premier avec $(p - 1)(q - 1)$, puis trouvé d défini en 1.b.i.
i. À l'aide de la feuille de calcul du TP1, trouver p et q tel que $pq = 12\ 319$.
ii. À l'aide de l'algorithme d'Euclide (voir TP Algorithmique 2, chapitre 2), trouver d.

c. Alice forme alors $S(N) = N^d$. Expliquer comment elle peut retrouver M.

Commentaire

Parmi les applications du système RSA dans la vie courante, citons :
- La certification sur un ordinateur qui publie sa clé publique.
- L'authentification de la carte la carte bancaire, qui se passe entre la carte et le terminal. La clé publique est publiée par le groupement des banques.
- L'achat *via* Internet : L'internaute commande un objet en donnant des informations sur sa carte de crédit. Cette demande est cryptée à l'aide de la clé publique de la société, puis envoyée. Seule la société visée peut déchiffrer ce message, avec sa clé privée.

L'intérêt pour ce genre de code est d'avoir un nombre n produit de deux nombres premiers très grands de façon à ce que les calculateurs même les plus rapides ne puissent pas trouver en un temps suffisamment court les deux facteurs premiers nécessaires pour calculer d. Actuellement, les clés sont d'environs 256 octets, soit environ 616 chiffres.

Maîtriser le cours

Définition des nombres premiers

1 Vérifier que les nombres 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 sont premiers.

2 En utilisant les caractères de divisibilité, montrer que 111 et 111111 sont composés.

3 Soit n un entier naturel tel que $n = p \times q$, avec p et q entier naturels. n peut-il être premier ?

4 Soit n un entier naturel $n > 2$ et $N = (n - 2)(n^2 + 4)$. N peut-il être premier ?

5 Soient a et b deux entiers naturels. $a^2 - b^2$ peut-il être premier ?

6 317 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, ni par 11, ni par 13, ni par 17. Est-il premier ?

7 **a.** Déterminer le nombre d'entiers inférieurs ou égaux à 5 et premier avec 5.
b. Déterminer le nombre d'entiers inférieurs ou égaux à 25 et premier avec 25.

8 Montrer que l'équation $2012x + 5y = 1$ d'inconnues (x, y) a des solutions dans $\mathbb{Z}$.

9 Montrer que si p premier divise $a \times b$, alors p divise a ou p divise b.

10 **Vrai ou faux**
a. Les nombres premiers sont impairs.
b. Pour tout entier naturel n, n^2 est composé.
c. Si p est premier, $p + 2$ ne peut pas être premier.
d. Si p est premier, $p + 2$ est premier.
e. Si p et q sont premiers distincts, ils sont premiers entre eux.

11 **QCM** (Trouver la ou les réponses exactes)
a. $n^2 + 2n + 1$ est premier :
i. Pour certaines valeurs de n.
ii. Pour toutes les valeurs de n.
iii. Pour aucune valeur de n.
b. $n^2 - 2n + 3$ est premier :
i. Pour certaines valeurs de n.
ii. Pour toutes les valeurs de n.
iii. Pour aucune valeur de n.
c. Soit p premier, $p > 2$
i. p est impair ii. $p + 5$ est composé.
iii. $2p^2 + 1$ est premier.

Décomposition en facteurs premiers

12 On sait que $2x \equiv 0$ [11] et que $x < 100$.
Quelles sont les valeurs possibles de x ?

13 Soit p premier et $p > 2$.
On sait que $2x \equiv 0$ [p] et que $x < p^2$.
Quelles sont les valeurs possibles de x ?

14 Décomposer rapidement en facteurs premiers : 60, 90, 120 et 140.

15 Déterminer tous les diviseurs de 3^9.
Quelle est leur somme ?

16 Décomposer 72 en produit de facteurs premiers.
En déduire tous ses diviseurs.
Même question avec 600.

17 **a.** Déterminer tous les diviseurs de $a = 2^4 \times 3^2$ et $b = 3^2 \times 5^3$. En déduire PGCD(a, b) et PPCM (a, b).
b. Mêmes question avec $a = 2^3 \times 5^2 b = 3^2 \times 5^4$

18 Simplifier les fractions suivantes :

$$\frac{72}{60} ; \frac{2^3 \times 5^2}{2^5 \times 5 \times 7}.$$

19 Effectuer les sommes suivantes :

$$\frac{5}{60} + \frac{7}{42} ; \frac{3}{2^5 \times 5 \times 7} + \frac{5}{2^3 \times 3 \times 7^2}.$$

20 **Vrai ou faux** (sans calculatrice)
a. 35 divise 1 273.
b. 111 divise 11 111.
c. $17^2 \times 29^2$ est un carré.
d. $7^3 \times 29^6$ est un carré.

21 **QCM** (Trouver la ou les bonnes réponses)
a. p désigne un nombre premier.
i. Si p divise ab, alors p divise a ou p divise b.
ii. Si p divise $a + b$, alors p divise a et p divise b.
iii. Si p divise a ou p divise b, alors p divise $a + b$.
b. n désigne un entier naturel, p et q deux nombres premiers distincts.
i. $a \equiv 0$ [pq] si, et seulement si, $a \equiv 0$ [p] et $b \equiv 0$ [q].
ii. $a \equiv 0$ [nq] si, et seulement si, $a \equiv 0$ [n] et $b \equiv 0$ [q].
iii. si n divise p et n divise q, alors n divise pq.
c. soit $a = 156$.
i. a possède 3 diviseurs.
ii. a possède 12 diviseurs
iii. $a \times 13$ et un carré parfait.

Appliquer les capacités attendues

Définition des nombres premiers

Reconnaître des nombres composés et des nombres premiers [savoir-faire 1 p. 83]

22 Justifier que les nombres suivants sont composés :
a. 15790 ; **c.** 465325 ;
b. 21457894 ; **d.** 123456789.

23 **a.** Montrer que les nombres dont l'écriture décimale est terminée par 0, 2, 4, 5,6,8, sont composés.
b. En déduire que si un nombre supérieur à 5 est premier, son écriture décimale est terminée par 1, 3, 7, ou 9
c. Quel est le nombre maximal de nombres premiers dans une dizaine ?

24 Montrer que tout entier de la forme $4k$ ou $4k + 2$ est composé pour $k \geqslant 1$. En déduire que tout nombre premier impair est de la forme $4k + 1$ ou $4k + 3$.
La réciproque est-elle vraie ?

25 Montrer que tout nombre premier impair différent de 3 est de la forme $6k + 1$ ou $6k + 5$.

26 Soit n un entier naturel non nul.
a. Le nombre $N = 2n^2 + 3n$ peut-il être premier ?
b. Pour quelles valeurs de n le nombre $n^2 - 5n + 6$ est il premier ?

27 Montrer que $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$.
a. Pour quelles valeurs de n, le nombre $n^3 - 27$ est-il premier ?
b. Le nombre $n^6 - 27$ peut-il être premier ?

28 Montrer que si $a^2 - b^2$ est premier, alors a et b sont consécutifs. La réciproque est-elle vraie ?

29 **a.** En utilisant les congruences modulo 11, montrer que si n est impair et $n \geqslant 3$, $10^n + 1$ est composé.
b. Vérifier que $6^5 + 1$ est divisible par 11. En déduire des valeurs de n pour lesquelles $6^n + 1$ est composé.
c. $6^{2010} + 1$ est il premier ?

30 Dire si les nombres suivants sont premiers :
579, 911, 1 021, 1 597.

31 On dispose des chiffres 1, 1, 3 pour former des nombres de 3 chiffres.
a. Combien peut-on en former ?
b. Vérifier que ces nombres sont tous premiers.

32 On dispose des chiffres 1, 3, 7 pour former des nombres de 3 chiffres.
a. Combien peut-on en former ?
b. Ces nombres sont-ils tous premiers ?

33 **Une démonstration de l'infinitude des nombres premiers**
Supposons que l'ensemble E des nombres premiers soit fini et constitué de n éléments distincts notés $p_1 < \ldots\ldots < p_n$. Posons $N = p_1 \times \ldots\ldots \times p_n + 1$.
a. Justifier que N admet alors un diviseur premier d, donc dans E.
b. En déduire qu'il existe i tel que $d = p_i$.
c. Montrer que d divise $N - p_1 \times \ldots\ldots \times p_n$.
d. En déduire que l'ensemble E est infini.

Utiliser la notion de nombre premier [savoir-faire 2 p. 83]

34 Soient a et b entiers naturels supérieurs ou égaux à deux tels que $a + b = p$, avec p premier.
Montrer que a et b sont de parité différente.
Montrer que a et b sont premiers entre eux.

35 Les équations suivantes ont-elles des solutions ?
a. $27972x + 7y = 1$. **c.** $3x + 12345y = 1$.
b. $2x + 45679y = 2$.

36 Existe-t-il des entiers x tels que :
a. $2x \equiv 1$ [6] ? **c.** $2x \equiv 1$ [7] ?
b. $5x \equiv 2$ [11] ? **d.** $5x \equiv 1$ [6] ?

37 Trouver tous les couples (x, y) d'entiers naturels tels que :
a. $x^2 - y^2 = 7$. **c.** $x^2 - y^2 = 11$.
b. $x^2 - y^2 = 6$.

38 Montrer que 7 est premier avec 6 !.
8 est-il premier avec 7 ! ?

39 Soit p un nombre premier.
Montrer que p est premier avec $(p - 1)$!
Montrer que pour tout entier k tel que $1 \leqslant k \leqslant p - 1$, p est premier avec k !

40 Développer $(a + b)^3$.
Montrer que $(a + b)^3 \equiv a^3 + b^3$ [3].
Est-il vrai que $(a + b)^2 \equiv a^2 + b^2$ [3] ?
Est-il vrai que $(a + b)^4 \equiv a^4 + b^4$ [4] ?

41 Soient p et q deux nombres premiers distincts.
a. pq et $p + q$ sont-ils premiers entre eux ?
b. Écrire le rationnel $\frac{1}{p} + \frac{1}{q}$ sous forme d'une fraction irréductible.

Décomposition en facteurs premiers

Utiliser le théorème de Gauss
[savoir-faire 3 p. 85]

42 **a.** Montrer qu'il existe un unique entier x de [1, 4] tel que : $2x \equiv 1$ [5] .
b. En déduire que l'équation $2x \equiv 3$ [5] a une unique solution entière dans [1, 4].

43 **a.** Montrer qu'il existe un unique entier x de [1, 6] tel que : $3x \equiv 1$ [7].
b. En déduire que l'équation $3x \equiv 5$ [7] a une unique solution entière dans [1, 6].

44 Dresser la table de multiplication modulo 7.
Pour chaque nombre a de 1, à 6, trouver l'unique nombre b tel que $ab \equiv 1$ [7].
En déduire que 6 ! + 1 est divisible par 7.

45 Dresser la table de multiplication modulo 11.
Pour chaque nombre a de 1, à 10, trouver l'unique nombre b tel que $ab \equiv 1$ [11].
En déduire que 10 ! + 1 est divisible par 11.

46 Soit p un nombre premier impair et a un entier naturel compris entre 1 et $p - 1$.
Montrer que $a^2 \equiv 1$ [p] si, et seulement si, $a = 1$ ou $a = p - 1$.

Utiliser la décomposition en facteurs premiers [propriétés 7 et 8 p. 84]

47 Expliquer pourquoi les nombres suivants sont des carrés parfaits et donner leur racine carrée.
$a = 2^4 \times 3^6 \times 7^2$; $b = 3^2 \times 5^4 \times 7^6$.

48 Décomposer 132 en facteurs premiers.
Quel est le plus petit entier naturel a non nul tel que 132a soit un carré ?

49 Soit n un entier naturel.
Montrer que n est le carré d'un entier m si, et seulement si, tous les exposants de sa décomposition en facteurs premiers sont des multiples de 2.

50 **a.** Donner la décomposition en facteurs premiers de 2008.
b. Déterminer la plus petite valeur de l'entier naturel k pour laquelle k^6 est un multiple de 2008.

51 **a.** Quel est le plus petit entier possédant 3 diviseurs ?
b. Quels sont les entiers compris entre 10 et 20 qui possèdent 3 diviseurs ?

52 Un nombre s'écrit 4.10^n.
Existe-t-il une valeur de n pour laquelle il possède 27 diviseurs ?

53 **a.** Décomposer 144 en produit de facteurs premiers. En déduire la décomposition de 144 en produit de nombres premiers entre eux.
Même question avec les nombres suivants :
b. 1 095. **c.** 1 573. **d.** 512.

54 **a.** Soient p un nombre premier et n un entier naturel. Déterminer le nombre de diviseurs de p^n.
b. Déterminer le produit de ces diviseurs.

Appliquer la décomposition en facteurs premiers [savoir-faire 4 p. 85]

55 On pose $a = 2^3 \times 3^5 \times 7^2$ et $b = 3^2 \times 5^4 \times 7^6$.
a. Déterminer $d = \text{PGCD}(a, b)$.
b. Déterminer a' et b' tels que $a = da'$ et $b = db'$.
c. Calculer que $m = da'b'$.
d. Écrire la fraction $\frac{a}{b}$ sous forme irréductible.
e. Écrire $\frac{1}{a} + \frac{1}{b}$ sous forme irréductible.

56 Reprendre les questions de l'exercice 55 avec les nombres suivants :
a. $a = 2^3 \times 3 \times 7^2 \times 11$ et $b = 2 \times 3^2 \times 5^4 \times 7^6$.
b. $a = 810$ et $b = 435$.
c. $a = 600$ et $b = 270$.

57 Soient p et q deux nombres premiers distincts.
On pose $a = p^3 \times q^4$ et $b = p^2 \times q^5$.
a. Écrire la fraction $\frac{a}{b}$ sous forme irréductible.
b. Écrire $\frac{1}{a} + \frac{1}{b}$ sous forme irréductible.

58 Soient p et q deux nombres premiers distincts.
On pose $a = p^3 \times q^4$ et $b = p \times q^6$
a. Écrire la fraction $\frac{a}{b}$ sous forme irréductible.
b. Écrire $\frac{b}{a} + \frac{a}{b}$ sous forme irréductible.

59 Soient a et b deux entiers tels que $a + b = 1\,125$ et $a < b$. On note $d = \text{PGCD}(a, b)$.
a. Justifier qu'il existe n et m tels que $d = 3^n \times 5^m$.
b. Sachant que a et b ont 6 diviseurs communs et que $d < 50$, déterminer les valeurs possibles pour a et b.
c. Quelles conditions rajouter pour que le couple cherché soit unique ?

60 QCM

Pour chacune des propositions, donner la ou les bonnes réponses :

1. Si p et q sont deux nombres premiers distincts, alors :

a. $p + q$ est un nombre pair.
b. $p + q$ est un nombre premier.
c. p et $p + q$ sont premiers entre eux.

2. Soient a un entier naturel et p un nombre premier tel que p divise a^2. Alors :

a. p^2 divise a^2.
b. si a est premier, $p = a^2$.
c. p^2 divise a.

3. Soit p tel que p et $p + 2$ des nombres premiers supérieurs ou égaux à 5. Alors

a. $p + 1$ est pair.
b. $p(p + 2)$ est pair.
c. $p + 4$ est premier.

4. Si p premier, alors

a. p est impair.
b. $p^2 + 1$ est premier.
c. p^2 a six diviseurs dans $\mathbb{Z}$

5. $N = n^4 + 7n^2 + 10$

a. N est premier pour au moins une valeur de n.
b. N est premier pour toutes valeurs de n.
c. N n'est premier pour aucune valeurs de n.

Premier ou non premier ?

61 Dire si les nombres suivants sont premiers :

a. 2 699 ; 4 379 ; 21 863.
b. 12 ! + 7 ; 123 ! + 111 ; 5 ! + 7

62 Pour tout entier k, on note p_k le kième nombre premier, et on pose $P_k = p_1 . p_2 ... p_k + 1$.

a. Calculer P_1, P_2, P_3, P_4, P_5. Sont-ils premiers ?
b. P_k est il premier quel que soit k ?

63 **a.** Montrer que la somme de 3 entiers consécutifs n'est pas premier.

b. Soit k un entier naturel. On considère les 5 entiers naturels $k - 2$, $k - 1$, k, $k + 1$, $k + 2$. Que vaut leur somme ?

c. La somme de n, $n > 1$, nombres impairs consécutifs peut-elle être un nombre premier ?

64 1. **a.** $2^2 + 3^2 + 5^2$ est il un nombre premier ?
b. $5^2 + 7^2 + 11^2$ est il un nombre premier ?
c. Soit p un nombre premier supérieur ou égal à 5. Montrer que p^2 est congru à 1 modulo 3.
c. si, p, q, r sont des nombres premiers distincts supérieurs ou égaux à 5, $p^2 + q^2 + r^2$ est il un nombre premier ?

65 **a.** Montrer que $(n - 1)(n + 3) = n^2 + 2n - 3$.

b. En déduire que, quel que soit l'entier $n \geqslant 3$, le nombre $n^2 + 2n - 3$ n'est jamais premier.

66 Montrer quel que soit l'entier $n \geqslant 7$, le nombre $n^2 - 3n - 10$ n'est jamais premier.

67 On pose $u_1 = 1$, et pour tout entier naturel n, $u_{n+1} = 10u_n + 1$.



1. **a.** Vérifier que pour tout n, l'écriture décimale de u_n ne comporte que des 1.
b. Montrer que pour tout n, $u_n \equiv 1$ [2] et $u_n \equiv 1$ [5].
c. Montrer que u_n n'est jamais divisible par un nombre pair.

2. **a.** Construire à l'aide d'un tableur, un tableau donnant les restes dans la division par m des u_n, pour m impair variant de 3 à 21 et n de 1 à 20.

m/n	1	2	3	4	5	...	20
3	1	2	0	1	2	...	2
5	1	1	1	1	1	...	1
...	...	...	...	...	...	...	...
21	6	19	2	0	1	...	19

b. Quels sont les u_n qui apparaissent composés ?

3. **a.** Montrer que $9u_n = 10^n - 1$
b. Montrer que si n est pair, u_n est divisible par 11.
c. Montrer que si n est multiple de 3, u_n est divisible par 111.
d. Montrer que si n n'est pas premier, u_n n'est pas premier (on pourra utiliser l'identité rappelée dans l'activité 3).

68 **a.** Montrer, en utilisant les congruences que pour tout entier naturel k, $2^{2k+1} + 1$ est multiple de 3.
En déduire que si m est un entier naturel impair, $2^m + 1$ est composé
b. Montrer que si m admet un diviseur impair p, $2^m + 1$ est divisible par $2^q + 1$, où $m = pq$.
c. En déduire que si $2^k + 1$ est premier, alors $k = 2^m$.

Algorithmique

69 **Nombres de Fermat**

1. Fermat a étudié les nombres de la forme $F_n = 2^{2^n} + 1$.
a. Calculer F_0, F_1, F_2, F_3, F_4
b. Fermat a conjecturé que tous les nombres de cette forme étaient premiers.
En utilisant un algorithme, dire si ces 4 nombres sont premiers
Les choses se compliquent pour F_5. Fermat n'a pas pu dire s'il était premier ou non.

2. On démontre que les diviseurs premiers de F_5, s'ils existent, sont de la forme $k2^6 + 1$.
En utilisant un algorithme, montrer que F_5 n'est pas premier.

70 **Nombres de Fermat et infinitude**

1. **a.** Montrer que pour tout $k > 0$, $F_{n+k} - 1 = (F_n - 1)^{2^k}$.
b. En déduire que $F_{n+k} \equiv 2\ [F_n]$.
c. Montrer que si $m \neq n$, F_m et F_n sont premiers entre eux.
2. Soit p_n le plus petit diviseur premier de F_n et P l'ensemble des p_i pour i entier naturel.
a. Montrer que si $m \neq n$, $p_m \neq p_n$.
b. En déduire une autre preuve de l'infinitude des nombres premiers.

Un peu d'histoire...



Pierre de Fermat a vécu au XVII^e siècle. C'est un juriste et mathématicien français, surnommé « le prince des amateurs ». Il est en même temps un habile helléniste. Il s'est aussi intéressé aux sciences physiques ; on lui doit notamment le principe de Fermat en optique.

Des équations

71 **a.** Existe-t-il des couples (a, b) d'entiers naturels tels que $a^2 - b^2 = 4$?
b. Soit p un nombre premier impair, déterminer les couples (a, b) d'entiers naturels tels que $a^2 - b^2 = p^2$.

72 1. Les nombres a et b étant deux entiers naturels premiers vérifiant $a > b > 2$, trouver tous les couples $(x ; y)$ éléments de $\mathbb{N}^* \times \mathbb{N}^*$ tels que : $x^2 - y^2 = a^2b^2$.
2. Applications
a. Résoudre dans $\mathbb{N}^* \times \mathbb{N}$: $x^2 - y^2 = 196$
b. Résoudre dans $\mathbb{N}^* \times \mathbb{N}$: $x^2 - y^2 = 3\,025$.

Algorithmique

73 On veut résoudre dans $\mathbb{Z}$ l'équation (E) d'inconnue x : $x^2 - 2x + 6 \equiv 0$ (mod7).

1. **a.** Que fait cet algorithme ?
b. Utiliser cet algorithme sur la calculatrice pour trouver une solution positive à l'équation. Pourquoi sera-t-elle la plus petite ?

```
Entrer P,
X = 0, B = 1
TantQue B≠0
   X = X + 1
   B = f(X) mod P
FinTanque
Afficher X.
```

2. Déterminer a tel que
$4a \equiv 6$ (7) avec $1 \leqslant a \leqslant 6$.
b. Montrer que $(x - 5)(x - 4) \equiv x^2 - 2x + 6$ (mod 7).
c. En déduire les solutions de (E)
3. Utiliser la méthode précédente pour résoudre dans $\mathbb{Z}$ l'équation (E) d'inconnue x :
$x^2 - 3x + 1 \equiv 0$ (mod11).

74 On veut trouver les triplets d'entiers naturels a, b, c, tels que $3a = b^2$ et $5a = c^3$. Soient d = PGCD (b, c) et b' et c' tels que $b = db'$ et $c = dc'$.
a. Vérifier que b' et c' sont premiers entre eux.
b. Montrer que $5b'^2 = 3dc'^3$.
c. Montrer que c'^2 divise 5. En déduire que $c' = 1$.
d. Montrer que 3 divise b'. En déduire qu'il existe un entier naturel k tel que $d = 15k^2$.
e. Quels sont les triplets solutions ?



75 On considère l'équation $324x - 245y = 7$
1. **a.** Décomposer 324 et 245 en produit de facteurs premiers.
b. Montrer que pour toute solution $(x ; y)$, x est multiple de 7.
c. En utilisant un programme sur la calculatrice, déterminer une solution $(x_0 ; y_0)$ et en déduire toutes les solutions.
2. Soit δ le PGCD des éléments d'un couple $(x ; y)$ solution de l'équation ; quelles sont les valeurs possibles de δ ? Déterminer les solutions de l'équation telles que x et y soient premiers entre eux.

76 On considère les équations d'inconnues (x, y, z)
$z = x^2 + y^2$ (E_1) et $z = xy + 2x$ (E_2).
On cherche (x, y, z), avec x un nombre premier solution à la fois de (E_1) et de (E_2). Soit (x, y, z) un triplet solution.
1. **a.** Montrer que $y(x - y) = x(x - 2)$
b. Démontrer que si p premier divise ab, alors p divise a ou p divise b.
c. En déduire que x divise y.
2. On pose $y = kx$.
a. Montrer que x divise 2. Que peut-on en conclure ?
b. En déduire les valeurs possibles de k.
3. Déterminer alors les triplets solution.

Des diviseurs

77 Quels sont les nombres premiers qui divisent simultanément :
a. 1 980 et 760 ? **b.** 2 048 et 1 084 ?

78 **a.** Écrire la décomposition en facteurs premiers de $a = 504\,900$.
b. Écrire la décomposition en facteurs premiers de $b = 1\,188$.
c. Sans calculatrice, justifier que b divise a.

79 **a.** Écrire la décomposition en facteurs premiers de $a = 35000^{35000}$.
b. Écrire la décomposition en facteurs premiers de $b = 37\,515\,625$.
c. Sans calculatrice, justifier que b divise a.

80 Quelle est la forme de la décomposition en facteurs premiers d'un entier n qui admet 21 diviseurs ? Quel est le plus petit de ces nombres ?

81 Quelle est la forme de la décomposition en facteurs premiers d'un entier n qui admet un nombre p premier de diviseurs ? Quel est le plus petit de ces nombres ?

82 **a.** Montrer que tout nombre premier p différent de 2 est impair. En déduire si p premier impair, $p^2 - 1$ est multiple de 8.

b. En utilisant les congruences modulo 3, montrer que si $p > 3$, $p^2 - 1$ est multiple de 3

c. Montrer qu'un nombre est divisible par 24 si et seulement si il est divisible par 3 et par 8.

d. Montrer que pour tout nombre premier $p > 3$, $p^2 - 1$ est divisible par 24.

83 **Les nombres premiers jumeaux**

Deux nombres premiers sont jumeaux si leur différence est 2.

a. Montrer qu'ils sont alors impairs consécutifs.

b. Donner un exemple.

c. Montrer que leur somme (sauf pour 3, 5) est divisible par 12. (On pourra utiliser la technique de l'exercice 82)

d. Montrer que (sauf pour (3, 5)), ils sont de la forme $(6n - 1, 6n + 1)$.

Un peu d'histoire...

On ne sait toujours pas à ce jour, si les nombres jumeaux sont en nombres finis ou infinis.
Cependant, comme les nombres premiers, ils ont tendance à se raréfier.

84 On considère le nombre $N = 100$!.

a. Quels sont les nombres premiers intervenant dans la décomposition de N ?

b. Quel est le nombre premier qui a le plus grand exposant ?

c. Quel est l'exposant de 5 ?

d. Combien y a-t-il de zéros dans l'écriture décimale de N ?

85 Soient a et b tels que $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots \times p_s^{\alpha_s}$, $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots\ldots \times p_s^{\beta_s}$, où $p_1, \ldots, p_s$ sont des nombres premiers distincts et α_i et β_i entiers des entiers positifs ou nuls. Soit, pour tout i, $\gamma_i = \alpha_i - \beta_i$.

a. On suppose que $\gamma_i \geqslant 0$. Montrer que b divise a.

b. On suppose que b divise a. Soit m tel que $a = mb$. En utilisant l'unicité de la décomposition en facteurs premiers, montrer alors que $\gamma_i \geqslant 0$.

c. Quelle propriété du cours est ainsi démontrée ?

Utiliser les nombres premiers

86 On considère l'ensemble $A_7 = \{1 ; 2 ; 3 ; 4 ; 5 ; 6\}$

1. **a.** Recopier et compléter le tableau donnant les produits modulo 7 des éléments de A_7.

	1	2	3	4	5	6
1	1					
2		4				
3			2			
4				2		
5					4	
6						1

b. Vérifier que, pour tout élément a de A_7, il existe un élément y de A_7 tel que $ay \equiv 1$ [7].

c. Pour x entier relatif, démontrer que l'équation $3x \equiv 5$ (modulo 7) équivaut à $x \equiv 4$ [7].

2. Si a est un élément de A_7, montrer que les seuls entiers relatifs x solutions de l'équation $ax \equiv 0$ [7] sont les multiples de 7.

Algorithmique

87 Pour tout p premier, on désigne par A_p l'ensemble $\{1, 2, \ldots, p - 1\}$.

1. Que fait l'algorithme ci-contre ?

2. À l'aide de cet algorithme, résoudre dans A_{31} les équations : $2x \equiv 1$ [31] et $3x \equiv 1$ [31].

3. À l'aide des résultats précédents, résoudre dans $\mathbb{Z}$ l'équation $6x^2 - 5x + 1 \equiv 0$ [31].

```
Entrer P, A.
X = 0, B = 0
TantQue B≠1
   X = X + 1
   B = A × X mod P
FinTanque
Afficher X.
```

88 Soient a et b deux nombres premiers entre eux.
On veut montrer par deux méthodes différentes que $a + b$ et ab sont premiers entre eux.

1. En utilisant le théorème de Bézout.

a. Montrer qu'il existe deux entiers relatifs u et v tels que $(a + b)v + (u - v)$ a = 1. En déduire que a est premier avec $a + b$.

b. Montrer de même que b est premier avec $a + b$

c. Après avoir montré que si un nombre est premier avec deux nombres, il l'est avec leur produit, montrer que a + b et ab sont premiers entre eux.

2. En utilisant les diviseurs premiers.

a. Supposons que PGCD$(a + b ; ab)$ soit différent de 1. Justifier alors l'existence d'un diviseur premier p de $a + b$ et ab.

b. Montrer que d divise $a(a + b) - ab$. En déduire que d divise a.

c. Montrer de même que d divise b.

e. Conclure.

PGCD

89 Soient $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots \times p_s^{\alpha_s}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots\ldots \times p_s^{\beta_s}$, avec $\alpha_i \geqslant 0$, $\beta_i \geqslant 0$.
On pose $\delta_i = \max(\alpha_i, \beta_i)$ et $m = p_1^{\delta_1} \times p_2^{\delta_2} \times \ldots\ldots \times p_s^{\delta_s}$.
a. Montrer que m est un multiple commun de a et b. On admet que c'est le plus petit et on note $m = \text{PPCM}(a ; b)$.
b. Montrer que si $a = da'$ et $b = db'$, alors $m = da'b'$, où d désigne PGCD $(a ; b)$.
c. Application
On pose $a = 2^3 \times 3^5 \times 7^2$ et $b = 3^2 \times 5^4 \times 7^6$. Déterminer PPCM$(a ; b)$.
d. Trouver a et b tels que PPCM$(a ; b) = 210$ PGCD$(a ; b)$ et $b - a = \text{PGCD}(a ; b)$.

90 1. **a.** Décomposer 319 en produits de facteurs premiers.
b. En déduire les paires d'entiers naturels premiers entre eux ayant pour produit 319.
2. Démontrer que si x et y sont deux entiers naturels premiers entre eux, il en est de même pour $3x + 5y$ et $x + 2y$.
3. On veut résoudre dans $\mathbb{N}$ le système :
$\begin{cases} (3a + 5b)(a + 2b) = 1\,276, \\ ab = 2m \end{cases}$
où m désigne le plus petit multiple commun de a et b.
a. Soit $d = \text{PGCD}(a ; b)$, a' et b' tels que $a = da'$, $b = db'$. Vérifier que $md = ab$ et $m = da'b'$? En déduire que $d = 2$.
b. En déduire les solutions du système.

91 Déterminer tous les couples $(a ; b)$ d'entiers naturels tels que $m + 11d = 203$, m étant le PPCM (plus petit commun multiple) et d le PGCD de a et b.

92 1. Montrer que si p est premier et $p > 2$, il est congru à -1 ou à 1 modulo 4.
Le but de l'exercice est de répondre à la question : les nombres premiers congrus à -1 modulo 4 sont-ils en nombre fini ?
Soit E l'ensemble des nombres premiers congrus à -1 modulo 4. Supposons E fini, notons A le produit de ses éléments et B le nombre $4A - 1$.
2. Soit q un diviseur premier de B.
a. Montrer que $B \equiv -1$ [4].
b. Montrer que q n'est pas dans E. (On pourra raisonner par l'absurde).
3. **a.** Montrer qu'au moins un diviseur premier de B est congru à -1 modulo 4.
b. Conclure.

93 **a.** Soit p un entier naturel. Montrer que l'un des trois nombres p, $p + 10$ et $p + 20$, et l'un seulement est divisible par 3.
b. Les entiers naturels a, b et c sont dans cet ordre les trois premiers termes d'une suite arithmétique de raison 10. Déterminer ces trois nombres sachant qu'ils sont premiers.

Problèmes

94 Soit p un nombre premier donné. On se propose d'étudier l'existence de couples $(x ; y)$ d'entiers naturels strictement positifs vérifiant l'équation E : $x^2 + y^2 = p^2$
1. On pose p = 2.
Montrer que l'équation E est sans solution.
On suppose désormais $p > 2$ et que le couple $(x ; y)$ est solution de l'équation E.
2. Le but de cette question est de prouver que x et y sont premiers entre eux.
a. Montrer que x et y sont de parités différentes.
b. Montrer que x et y ne sont pas divisibles par p.
c. En déduire que x et y sont premiers entre eux.
3. On suppose maintenant que p est une somme de deux carrés non nuls, c'est-à-dire : $p = u^2 + v^2$ où u et v sont deux entiers naturels strictement positifs.
a. Vérifier qu'alors le couple $(|u^2 - v^2| ; 2uv)$ est solution de l'équation E.
b. Donner une solution de l'équation E, lorsque $p = 5$ puis lorsque $p = 13$.
4. On se propose enfin de vérifier sur deux exemples, que l'équation E est impossible lorsque p n'est pas somme de deux carrés.
a. $p = 3$ et $p = 7$ sont-ils somme de deux carrés ?
b. Démontrer que les équations $x^2 + y^2 = 9$ et $x^2 + y^2 = 49$ n'admettent pas de solution en entiers naturels strictement positifs.

95 On désigne par p un nombre entier premier supérieur ou égal à 7. Le but de l'exercice est de démontrer que l'entier naturel $n = p^4 - 1$ est divisible par 240, puis d'appliquer ce résultat.
1. Montrer que p est congru à -1 ou à 1 modulo 3.
En déduire que n est divisible par 3.
2. En remarquant que p est impair, prouver qu'il existe un entier naturel k tel que $p^2 - 1 = 4k(k + 1)$, puis que n est divisible par 16.
3. En considérant tous les restes possibles de la division euclidienne de p par 5, démontrer que 5 divise n.
4. **a.** Soient a, b et c trois entiers naturels.
Démontrer que si a divise c et b divise c, avec a et b premiers entre eux, alors ab divise c.
b. Déduire de ce qui précède que 240 divise n.
5. Existe-t-il quinze nombres premiers $p_1, p_2, \ldots, p_{15}$ supérieurs ou égaux à 7 tels que l'entier $A = p_1^4 + p_2^4 + \ldots + p_{15}^4$ soit un nombre premier ?

Devoir de synthèse

Revoir les bases suivantes :
cours A et B, savoir-faire 1 à 4.

[Le devoir est corrigé p. 173]

Premier sujet

96 **ROC**

1. Donner la définition de nombre premier.

2. Montrer que tout entier naturel n supérieur ou égal à 2, admet au moins 1 diviseur premier.

3. Montrer que $2 \times 3 \times 5 \times 7 + \times 11 + 1$ n'est divisible ni par 2, ni par 3, ni par 5, ni par 7 ni par 11. Est-il premier ?

Algorithmique

97 1. Que fait cet algorithme ?

```
Lire N (N impair et supérieur ou égal à 3)
T = 3
D = N
TantQue T ≤ √N faire
   Si partie décimale (N/T) = 0 alors
      D = T
      T = N²
   FinSi
   T = T+2
FinTantQue
Si N = D alors
   Afficher N « est premier »
   Sinon
   Afficher D « est un diviseur de N »
```

2. Le faire tourner sur la calculatrice et dire le résultat affiché pour N = 293 717.

98 Soient a et b deux entiers tels que $ab = 2\,592$ et $a < b$. On note $d = \text{PGCD}(a ; b)$.

a. Justifier qu'il existe n et m tels que $d^2 = 2^n \times 3^m$.

b. Sachant que a et b ont 6 diviseurs communs et que $d < 15$, déterminer les valeurs possibles pour a et b.

99 1. Montrer que tout nombre premier p supérieur strictement à 2 vérifie $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$

2. Soit p un nombre premier supérieur ou égal à 5.

a. Montrer que $p^2 - 1$ est divisible par 3.

b. Montrer que $p^2 - 1$ est divisible par 8.

c. Que peut-on en déduire ?

100 1. Décomposer en produit de facteurs premiers $a = 276$ et en déduire tous ses diviseurs positifs.

2. Décomposer en produit de facteurs premiers $b = 342$ et en déduire tous ses diviseurs positifs.

3. **a.** Déterminer $d = \text{PGCD}(a ; b)$.

b. Montrer que si $a = da'$ et $b = db'$, alors a' et b' sont premiers entre eux.

c. Calculer $m = da'b'$.

d. Simplifier $\frac{a}{b}$ et donner $\frac{1}{a} + \frac{1}{b}$ sous forme irréductible.

Deuxième sujet

101 Soit p un nombre premier.
On cherche tous les couples d'entiers naturels (x, y) tels que $x^2 - y^2 = p^2$.

1. Quels sont les diviseurs de p^2 ?

2. On pose $p = 2$.

a. Montrer que x et y ont même parité.

b. Déterminer les couples solution.

3. Dans cette question, $p \neq 2$.

a. Montrer que p est impair.

b. Déterminer toutes les solutions.

102 **a.** Le nombre $2^{11} - 1$ est-il premier ?
Expliquer exactement la démarche utilisée.

b. p et q étant deux entiers naturels non nuls, quel est le reste de la division par $2^p - 1$ du nombre 2^{pq} ?
(On pourra utiliser les congruences modulo $2^p - 1$.)
En déduire que $2^{pq} - 1$ est divisible par $2^p - 1$ et $2^q - 1$.

c. Démontrer que, si $2^n - 1$ est premier, alors n est premier.
La réciproque est-elle vraie ?

Algorithmique

103 Soit n un entier naturel.
On note $\varphi(n)$ le nombre d'entiers strictement positifs, inférieurs à n, premier avec n.

a. Déterminer $\varphi(n)$ pour $2 \leqslant n \leqslant 7$.

b. Compléter cet algorithme afin qu'il donne $\varphi(n)$:

```
Lire N
X = 1, A = 0
TantQue A < N-1 faire
   D = A, B = 0
   TanQue B≠1 faire
      D = D+1
      B = PGCD(D, N)
   FinTanQue
   L1(X) = D
   .....
```

Vérifier les résultats trouvés au **a.**

c. Soit p un nombre premier. Déterminer $\varphi(p)$.

d. Soient p et q deux nombres premiers distincts. Déterminer $\varphi(pq)$.

e. Soit p premier et n un entier naturel supérieur ou égal à 1. Montrer que $\varphi(p^n) = p^{n-1}(p - 1)$

f. Si $n = p^n q^m$ avec p et q premiers distincts, conjecturer $\varphi(n)$.
À l'aide de l'algorithme, calculer $\varphi(36)$ et vérifier votre conjecture.

Exercices guidés BAC

104 **1.** Montrer que 47 est premier.

2. Soit A l'ensemble des entiers naturels de l'intervalle [1 ; 46].
On considère l'équation (E) : $23x + 47y = 1$
où x et y sont des entiers relatifs.

a. Montrer que (E) a des solutions.

b. Donner une solution particulière (x_0, y_0) de (E).

c. Déterminer l'ensemble des couples (x, y) solutions de (E).

d. En déduire qu'il existe un unique entier x de A tel que $23x \equiv 1\ (47)$.

3. Soient a et b deux entiers relatifs.

a. Montrer que si $ab \equiv 0\ (47)$ alors $a \equiv 0\ (47)$ ou $b \equiv 0\ (47)$.

b. En déduire que si $a^2 \equiv 1\ (47)$ alors $a \equiv 1\ (47)$ ou $a \equiv -1\ (47)$.

4. **a.** Montrer que pour tout entier p de A, il existe un entier relatif q tel que $p \times q \equiv 1\ (47)$
Pour la suite, on admet que pour tout entier p de A, il existe un unique entier, noté inv(p), de A tel que $p \times \text{inv}(p) \equiv 1\ (47)$.

b. Déterminer inv(2) et inv(3).

c. Quels sont les entiers p de A qui vérifient $p = \text{inv}(p)$?

d. Montrer que $46! \equiv -1(47)$.

e. Proposer un algorithme qui permet de trouver inv(p) pour chaque entier p de A.

Guide

1. Trouver la partie entière de $\sqrt{47}$.
Effectuer des divisions euclidiennes.

2. **a.** 47 est premier, donc ...

b. Solution particulière évidente.

c. Théorème de Gauss, voir chapitre 2.

d. Parmi toutes les solutions, on détermine la seule de A par encadrement.

3. **a.** Cf. savoir-faire 3 : application du théorème de Gauss.

b. $a^2 \equiv 1\ (47)$ équivaut à $a^2 - 1 \equiv 0\ (47)$, puis a.

4. **a.** On procède comme en 2a, en remplaçant 23 par p.

b. $2 \times 24 = 48 = 47 + 1$, donc inv(2) = 24.
$3 \times 16 = 48 = 47 + 1$, donc inv(3) = 16

c. $p = \text{inv}(p)$ équivaut à $p^2 \equiv 1\ (47)$, puis 3b

d. $46 ! = 1 \times 2 \times 3 \times ... \times 16 \times ... \times 24 \times ... \times 46$
Chaque nombre excepté 1 et 46 ont un inverse dans A distinct de lui même. On regroupe les nombres par paires

e. On pourra par exemple faire calculer pour chaque nombre de A, le produit par chaque nombre de A modulo 47.

105 Soit (u_n) la suite définie pour tout entier naturel n non nul par :
$u_0 = 1$ et, pour tout entier naturel n, $u_{n+1} = 10u_n + 21$.

1. **a.** Calculer u_1, u_2 et u_3.

b. Quelle conjecture peut-on faire sur l'écriture décimale de u_n ?

2. **a.** Démontrer par récurrence que, pour tout entier naturel n, $3u_n = 10^{n+1} - 7$.

b. En déduire, pour tout entier naturel n, l'écriture décimale de u_n

3. **a.** Montrer que u_1 et u_2 sont des nombres premiers.

b. Écrire un algorithme permettant de tester si un nombre est premier. u_3 est il premier ?
On se propose maintenant d'étudier la divisibilité des termes de la suite (u_n) par certains nombres premiers.

4. **a.** Démontrer que, pour tout entier naturel n, u_n n'est divisible ni par 2, ni par 3, ni par 5.

b. Montrer que 7 ne divise pas 10^n pour tout entier naturel n.
En déduire que u_n n'est pas divisible par 7.

c. Démontrer que, pour tout entier naturel n, $3u_n \equiv 4 - (-1)^n$ (mod11). En déduire que, pour tout entier naturel n, u_n n'est pas divisible par 11.

d. À l'aide de la calculatrice, en précisant la démarche adoptée, vérifier les congruences : $10^9 \equiv 7(\text{mod}17)$ et $10^{16} \equiv 1(\text{mod}17)$.
En déduire que, pour tout entier naturel k, u_{16k+8} est divisible par 17.

Guide

1. **a.** $u_1 = 10u_0 + 21 = 31$, $u_2 = 10.31 + 21 = 331$

b. $u_n = 333.....1$, avec n fois le chiffre 3.

2. **a.** $3u_0 = 10 - 7$
si $3u_n = 10^{n+1} + 21$, $3u_{n+1} = 10.3\ u_n + 3.21 = ...$

b. $3u_n = 10^{n+1} - 7 = 10^{n+1} - 10 + 3$
$= 10(10^n - 1) + 3$
$9(10^n + 10^{n-1} + ... + 10) + 3$ donc $u_n = ...$

3. **a.** Voir savoir-faire 2.

b. VoirTP1. 3331 est premier.

4. **a.** Par caractère de divisibilité

b. $10 = 2 \times 5$ et 7 ne figure pas dans la décomposition de 10^n, donc préférer une démonstration par l'absurde : si 7 divise u_n, alors ...

c. $10 = 11 - 1$ donc $10 \equiv (-1)$ (mod 11)
si 11 divise un alors $3u_n \equiv 0$ (mod 11).
Or $3u_n \equiv 3$ (mod 11) ou $3u_n \equiv 5$ (mod 11)
donc ...
En mode suite, $u(0) = 1$ et
$u(n) = \text{Mod}(10\ u(n-1), 17)$ $u(9)$ et $u(16)$
$u16_{k+8} = 10^{16k+9} - 7 = 10^9\ (10^{16})^k - 7$

QCM - Vrai ou faux BAC

106 **Vrai ou Faux (Justifier)**

a. 2 013 est premier.

b. 2 011 est premier.

c. 60^2 est le plus petit multiple de 60 qui soit un carré parfait.

d. 120 a 13 diviseurs.

e. Si a et b sont premiers entre eux, leur décomposition n'ont aucun facteur premier commun.

f. Si p est premier, il est de la forme $4k + 1$ ou $4k + 3$

g. si p est premier est de la forme $4k + 1$ ou $4k + 3$, il est premier

h. Pour tout p premier tel que $p > 5$, $p^2 - 1$ est divisible par 24.

i. Pour tout p premier tel que $p > 3$, $p^2 + 11$ est divisible par 12

j. Pour tout entier naturel k ($2 \leqslant k \leqslant n$), le nombre $n! + k$ n'est pas un nombre premier.

107 **Vrai ou Faux (Justifier)**

a. Si p premier divise $a + b$, alors p divise a et p divise b.

b. Si p premier divise $a + b$, alors p divise a ou p divise b.

c. Si p premier divise $a + b$ et ab, alors p divise a et p divise b.

d. Si p premier divise ab, alors $p = a$ ou $p = b$.

e. Si p premier divise ab, alors p divise a ou p divise b.

108 **QCM (Trouver la ou les bonnes réponses)**

1. Soit $N = n^4 + 4$.

a. N n'est pas premier.

b. N est premier pour tout n.

c. N n'est pas premier pour $n > 2$.

2. Soit $N = 11111111111111111$.

a. N est divisible par 11.

b. N est divisible par 21.

c. N est divisible par 33.

3. Soient p un nombre premier impair et a et b deux entiers naturels tels que $a^2 - b^2 = p$.

a. $a \equiv b$ [p].

b. $a = b + 1$.

c. a et b ont même parité.

4. Soient a et b deux entiers naturels.

a. Si 7 divise ab, alors 7 divise a et 7 divise b.

b. Si 7 divise ab, alors 7 divise a ou 7 divise b.

c. si 7 divise $a + b$, alors 7 divise a et 7 divise b.

5. Soit x tel que $7x \equiv 3$ [11].

a. $x \equiv \frac{3}{7}$ [11].

b. $x \equiv 3$ [11].

c. $x \equiv 2$ [11].

Exercice BAC

109 **1. Restitution Organisée des Connaissances**

a. Énoncer le théorème de Gauss.

b. Montrer que si p premier divise un produit de deux entiers naturels ab, p divise a ou p divise b.

c. Soient p et q deux nombres premiers distincts. Montrer que si n est un multiple de p et de q, alors n est un multiple de pq.

2. On pose $p = 29$.

a. Vérifier que p est premier.

b. Montrer que quelque soit a de $A_{28} = \{1, 2, ..., 28\}$, l'équation $ax - 29y = 1$ admet au moins une solution sur $\mathbb{Z}$.

c. Déterminer des entiers u et v de A_{28} tels que $4u \equiv 1$ [29] et $7u \equiv 1$[29], en expliquant clairement la démarche.

d. En déduire les entiers relatifs x tels que : $28x^2 - 11x + 1 \equiv 0$ [29].

3.a. Vérifier que $n = 493$ est le produit de deux nombres premiers.

b. On pose $c = 3$ et $M = 331$.
Calculer $N \equiv M^c$ [493], $N < 899$.

c. On pose $q = 17$ et $m = (p - 1)(q - 1)$.
Montrer que l'équation (E) $3x + 448y = 1$ a des solutions dans $\mathbb{Z}$ et déterminer le couple (u, v) solution de (E) tel que $3u + 448v = 1$, $0 \leqslant u \leqslant 447$.

d. En utilisant un algorithme que l'on explicitera, montrer que $N^{299} \equiv M$ [493].

110 Des diviseurs des nombres de Mersenne

Soit p un nombre premier impair.

1. **a.** Soit k un entier naturel non nul tel que $2^k \equiv 1$ [p] et soit n un entier naturel. Montrer que, si k divise n, alors $2^n \equiv 1$ [p].
b. Soit b tel que $2^b \equiv 1$ [p], b étant le plus petit entier non nul vérifiant cette propriété. Montrer, en utilisant la division euclidienne de n par b, que si $2^n \equiv 1$ [p], alors b divise n.

2. Soit q un nombre premier impair et le nombre $A = 2^q - 1$. Soit p un facteur premier de A.
a. Justifier que : $2^q \equiv 1$ [p].
b. Montrer que p est impair.
c. Soit b tel que $2^b \equiv 1$ [p], b étant le plus petit entier non nul vérifiant cette propriété. Montrer que b divise q. En déduire que $b = q$.
d. On admet que $2^{p-1} \equiv 1$ [p].
Montrer que q divise $p - 1$, puis que $p \equiv 1$ [$2q$].

3. Soit $M_{17} = 2^{17} - 1$.
Voici la liste des nombres premiers inférieurs à 400 et qui sont de la forme $34m + 1$, avec m entier non nul : 103, 137, 239, 307. En déduire que M_{17} est premier.

Les diviseurs premiers des nombres de Mersenne $M_p = 2^p - 1$, avec p premier sont de la forme $2kp + 1$.

111 Somme et produit des diviseurs d'un entier

1. Soient p un nombre premier et n un entier naturel.
a. Quels sont les diviseurs de p^n ?
Quel est :
b. le nombre $d(p^n)$ des diviseurs de p^n ?
c. la somme $\sigma(p^n)$ des diviseurs de p^n ?
d. le produit $P(p^n)$ des diviseurs de p^n ?

2. Soient p et q deux nombres premiers distincts, a et b deux entiers naturels non nuls. On pose $n = p^a q^b$.
Montrer que $\sigma(n) = \sigma(p^a).\ \sigma(q^b)$.

3. **a.** Soit $n = 200$. Vérifier que $n^{d(n)} = P(n)^2$.
b. On pose $n = p^a q^b$.
Montrer que la formule du a) est encore valable.
c. On pose $p = 2$, $q = 5$. Déterminer n sachant que $P(b) = 20^{42}$.

112 Théorème de Wilson

1. Inverse modulo p
Soit p un nombre premier impair et
$A_p = \{1, 2, \ldots\ldots, p - 1\}$.
a. Montrer que pour tout a élément de A_p, l'équation $ax \equiv 1$ [p] a une unique solution dans A_p. Cette solution est appelée inverse de a modulo p.
b. Déterminer les éléments de A_P qui sont leurs propres inverses.
c. Montrer que si a, b, c sont dans A_p et $ab \equiv ac$ [p], alors $b = c$.
d. Montrer que $2 \times 3 \times \ldots \times p - 2 \equiv 1$ [p].

2. On veut démontrer le théorème de Wilson :
p est premier si, et seulement, si $(p - 1)\ ! + 1 \equiv 0$ [p].
a. À l'aide de 1, démontrer que si p est premier alors, $(p - 1)\ ! \equiv -1$ [p].
b. Supposons que $(p - 1)\ ! + 1 \equiv 0$ et p non premier. Montrer que cette condition est impossible.
c. Conclure.

113 Racine primitive

Soit p un nombre premier. On appelle racine primitive modulo p tout entier a de $A_p = \{1, 2, \ldots\ldots, p - 1\}$ tel que l'ensemble des restes dans la division par p des a^k pour k élément de A_p décrit A_p tout entier.

1. Exemple pour $p = 3$. $A_2 = \{1, 2\}$.
Montrer que 1 n'est pas racine primitive modulo 3, mais que 2 en est une.

2. Vérifier que seuls 2 et 3 sont racines primitives modulo 5. Trouver toutes les racines primitives modulo 7.

3. **a.** Montrer que pour $p > 3$, ni 1, ni $p - 1$ ne sont racines primitives modulo p.
b. On rappelle que pour tout a de A_p, $a^{p-1} \equiv 1$ [p].
Soit s le plus petit des entiers k tels que $a^k \equiv 1$ [p].
En effectuant la division euclidienne de $p - 1$ par s, montrer que s divise $p - 1$.
s est alors appelé ordre de a modulo p.
c. Montrer que s'il existe $s < p - 1$ tel que $a^s \equiv 1$[p], alors a ne peut pas être racine primitive modulo p.
On admet pour tout nombre premier p, il existe une racine primitive modulo p.

4. **a.** Soit p un nombre premier et g une racine primitive modulo p. Montrer que pour tout b de A_p, il existe un unique r de A_p tel que $g^r \equiv b$ [p]. r est appelé logarithme de base g modulo p de b, noté $l(b)$.
b. Soit a un entier naturel congru à k modulo $p - 1$.
Déterminer le reste dans la division de g^a par p ?
c. Écrire un algorithme permettant de trouver $l(b)$.
d. Application : $p = 53$, g = 40, $b = 20$. Trouver $l(b)$ en appliquant cet algorithme à la calculatrice.

114 Les nombres de Carmichael *(suite)*

On rappelle que pour tout a et tout p premier, non multiple de a, $a^{p-1} \equiv 1$ [p] et qu'un nombre de Carmichael (voir TP1 p. 88) est un nombre n non premier, $n > 1$ tel que, pour tout entier naturel a, $a^n \equiv a$[n].

1. Montrer que tout nombre c, produit de 3 entiers premiers impairs p_1, p_2, p_3, tel que pour tout i, $p_i - 1$ divise $c - 1$ est tel que, pour tout entier naturel a, $a^c \equiv a$ [c]. Vérifier que 1 015 est un nombre de la sorte.

2. On veut montrer que les nombres de Carmichael sont sans facteurs carrés, ce qui veut dire que les nombres premiers de sa décomposition en facteurs premiers ont tous pour exposant 1.
Soit p un diviseur premier de n.
a. Vérifier que $n > 3$.

b. Montrer que $np \equiv 0\ [p^2]$.
c. En déduire que $(p+1)^n \equiv 1\ [p^2]$.
d. Montrer que $(p+1)^n \equiv 1 + p\ [n]$.
e. Montrer que si p^2 divise n, $(p+1)^n \equiv 1 + p\ [p^2]$.
f. Que peut-on en conclure ?

115 Valuation p-adique

Soit p un nombre premier et a un entier naturel non nul. On appelle valuation p-adique de a notée $v_p(a)$ l'exposant de p dans la décomposition en facteurs premiers de a. Exemple : $a = 2^3 \times 3 \times 7^3$, $v_7(a) = 3$, $v_5(a) = 0$.

1. Écrire un algorithme donnant $v_p(a)$ pour tout nombre premier p et tout nombre a non nul.

2. **a.** Montrer que si $v_p(a) = k$, alors p^k divise a et p^{k+1} ne divise pas a.
b. Montrer $v_p(a)$ est le nombre de zéros qui termine l'écriture en base p de a.
c. Montrer que pour tout couple d'entiers naturels, $v_p(ab) = v_p(a) + v_p(b)$.

116 Des valeurs absolues sur l'ensemble $\mathbb{Q}$

1. On considère une fonction v définie sur $\mathbb{R}$, à valeur dans $\mathbb{R}^+$ vérifiant les propriétés suivantes :
* $v(x) \geqslant 0$ et $v(x) = 0$ si et seulement si $x = 0$
** $v(xy) = v(x).v(y)$
*** $v(x+y) \leqslant v(x) + v(y)$
Si de plus $v(x+y) \leqslant \text{Max}(v(x), v(y))$, la fonction v est dite ultra-métrique.
a. Vérifier que la fonction valeur absolue vérifie les propriétés *, **, ***.
b. Vérifier les propriétés suivantes :
i. $v(1) = v(-1) = 1$ donc $v(-x) = v(x)$
ii. Pour tout réel x non nul, $v\left(\frac{1}{x}\right) = \frac{1}{v(x)}$.
c. Montrer par récurrence que pour tout n entier naturel n, $v(n) \leqslant n$.

2. Soit n un entier naturel et p un nombre premier.
a. Montrer qu'il existe deux entiers naturels k et m tels que $n = p^k m$, avec $\text{PGCD}(m, p) = 1$ si $m \neq 0$
On pose $v(n) = p^{-k}$ si $m \neq 0$ et $v(0) = 0$.
b. Démontrer que v vérifie les propriétés **, ***.
c. Vérifier que $v(x+y) \leqslant \text{Max}(v(x), v(y))$.
d. Vérifier que pour tout n, $v(n) < 1$.
e. Montrer que si n est premier avec p, $v(n) = 1$.

3. Le but de cette partie est de trouver des fonctions v vérifiant les propriétés, *, **, *** sur l'ensemble des entiers naturels, et par les propriétés b) sur l'ensemble $\mathbb{Q}$ des nombres rationnels.
a. Vérifier que v_0 définie par $v_0(n) = 1$ pour tout n convient.
b. On suppose qu'il existe un entier naturel a, $a \geqslant 2$ tel que $v(a) = \omega$, avec $0 < \omega < 1$. On veut montrer que pour tout entier naturel n, $v(n) \leqslant 1$.
Supposons que qu'il existe n tel que $v(n) > 1$.
i. Montrer que pour tout entier naturel k, $v(n^k) = v(n)^k$.
En déduire que $\lim v(n^k) = +\infty$
ii. En utilisant la décomposition en base a de n^k, montrer qu'il existe un entier naturel s tel que
$v(n^k) \leqslant a(1 + \omega + \omega^2 + \ldots + \omega^s)$.
En déduire que pour tout k, $v(n^k) < \frac{a}{1-\omega}$.
iii. Conclure.
c. Par décomposition, $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots \times p_s^{\alpha_s}$.
Montrer qu'il existe un nombre premier p_i tel que $v(p_i) < 1$; dans la suite, on note $p = p_i$.
ii. Soit n fixé premier avec p. Montrer que pour tout entier naturel k, il existe deux entiers u_k et v_k tels que $n^k u_k + p^k v_k = 1$. Que vaut alors $v(n^k u_k + p^k v_k)$?
Montrer que si $v(n) < 1$, alors $\lim\limits_{k \to +\infty} v(n^k u_k + p^k v_k) = 0$ en déduire $v(n) = 1$.
iii. En déduire que si $n = p^k m$, avec $\text{PGCD}(m, p) = 1$ si $m \neq 0$, $v(n) = v(p)^k$.
d. Montrer enfin que si r est un rationnel tel que $r = p^k \frac{a}{b}$, avec $\text{PGCD}(a, p) = \text{PGCD}(b, p) = 1$, alors, $v(r) = v(p)^k$.

Commentaire

On démontre que si pour tout $n \geqslant 2$ on a $v(n) > 1$ on peut établir qu'il existe δ, $0 < \delta \leqslant 1$ tel que v soit la valeur absolue usuelle à la puissance δ.

Communiquer à l'écrit ou à l'oral

Dans son ordinateur, Sophie trouve les informations ci-contre.

1. Expliquer la signification des mots : Algorithme Chiffrement, Clé publique, Exposant.
2. **a.** Que signifie 256 octets ?
b. Pourquoi y a t-il des lettres ? Combien doit-il y avoir de caractères ?
c. Qu'est ce que la dimension de la clé ?

Autorité de certification.
Expire le mardi 6 mars 2012
Certificated Reed
.....
Infos de clé publique
Algorithme Chiffrement RSA (1 2 840 113549 1 1 1)
Clé publique 256 octets : AD 3D 61 6E 03 F3 90 3B
C0 41 0B 84 80 CD EC 2A A3 9D 6B BB 6E C2 42 84
F7 51 14 E1 A0 A8 2D 51 A3 51 F2 DE 23 F0 34 44
.....
Exposant 65337
Dimension de la clé 2048 bits

Accompagnement personnalisé

Soutien

AP 1 Des techniques pour : ....

Objectif :
- *Consolider les techniques de base de d'arithmétique.*

1 Trouver tous les diviseurs d'un nombre.
a. Si le nombre est petit, faire un calcul direct.
b. Utiliser la décomposition en facteurs premiers et faire un arbre de diviseurs.

2 Trouver le PGCD de deux nombres.
a. Utiliser l'algorithme d'Euclide :
b. Utiliser la propriété : si d divise a et d divise b, alors...
c. Utiliser la décomposition en facteurs premiers.

3 Résoudre des équations diophantiennes de la forme $ax + by = c$.
a. Si a ou b est premier, montrer que l'équation a des solutions.
b. Si ni a ni b ne sont premiers, à quelle condition l'équation a t'elle des solutions ?
c. Recherche d'une solution particulière :
i. Solution évidente :
ii. Recherche d'une solution de $ax + by = 1$ (avec PGCD(a, b) = 1), par l'algorithme d'Euclide puis multiplication par c.
iii. En utilisant des congruences.
d. Trouver la solution générale. Utiliser les théorèmes de Gauss pour trouver la solution générale.
e. Trouver des solutions dans un cas particulier.

4 Résoudre d'autres équations diophantiennes.
a. Par factorisation. b. Étude exhaustive des cas.
c. En utilisant les congruences :

1 a. Trouver les diviseurs de 72.
b. Trouver tous les diviseurs de 1008.

2 a. Trouver le PGCD de 1325 et 7532.
b. Trouver le PGCD de $n - 3$ et $2n + 1$.
c. Trouver le PGCD de $2^3.3^2.5$ et de $2^2.3^5.7$

3 b. L'équation $4x - 6y = 7$ a-t-elle des solutions ?
c. i. Trouver un couple solution de : $13x + 5y = 3$. (1)
ii. Trouver un couple solution de : $15x - 7y = 9$. (2)
iii. En utilisant les congruences modulo 10, montrer que si $71x + 5y = 363$, alors $x \equiv 3[5]$.
En déduire une solution particulière de l'équation 3.
d. Résoudre dans Z chacune des équations proposées.
e. Déterminer Tous couple d'entiers naturels (x, y) tel que : $91x + 10y = 412$. On suppose que (x, y) existe.
Montrer que $x \leqslant 4$.
En utilisant les congruences modulo 10, montrer que $x \equiv 2$ [10].
En déduire le seul couple solution.

4 a. Résoudre dans Z l'équation $x^2 - y^2 = 131$.
b. Résoudre dans Z l'équation $x^2 + y^2 = 113$.
c. Résoudre dans Z l'équation $3x^2 + 7y^2 = 100$.
i. En utilisant les congruences modulo 7, montrer que $3x^2 \equiv 2$ [7].
ii. En faisant une étude exhaustive, montrer que l'équation n'a pas de solutions.

Découvrir un métier

AP 2 Chef de projet recherche et développement ....

Objectif :
- *Aide à l'orientation : Se familiariser avec les métiers de l'arithmétique.*

La distribution par Internet de contenus multimédias (musique, films, télévision, etc.) posent de sérieux problèmes de sécurité aux producteurs de ces contenus (maisons de disques, studios de production, etc.). Le chef de projet Recherche & Développement, au sein des opérateurs de distribution, doit en permanence étudier et réaliser de nouveaux outils visant à protéger ces contenus. Techniquement, ces outils font largement appel à la cryptographie par chiffrement des données, authentification ou signature électronique.



1. Quels problèmes se posent dans la distribution par Internet ?
2. De quelle sécurité parle-t-on ?
3. Qu'est-ce que la protection logicielle ?

AP 3 De l'exponentiation rapide

Nous avons vu que pour coder avec RSA, on a souvent affaire à des très grands nombres et les procédés usuels sont coûteux en temps.
Soit n un entier strictement supérieur à 1, supposons que l'on sache calculer pour tout x appartenant à l'ensemble des réels, toutes les puissances x^k de x, pour tout k, tel que $1 \leqslant k \leqslant n-1$.

- Si n est pair alors $x^n = (x^2)^{\frac{n}{2}}$. il suffit alors de calculer $y^{\frac{n}{2}}$ avec $y = x^2$.
- Si n est impair et $n > 1$, alors $x^n = x\,(x^2)^{\frac{n-1}{2}}$. Il suffit de calculer $y^{\frac{n-1}{2}}$ avec $y = x^2$ et de multiplier par x le résultat.

On remarque que l'on divise à chaque fois l'exposant par 2 s'il est pair et s'il est impair on le divise par 2 après avoir oté 1. L'idée est donc d'utiliser la décomposition en base 2 de l'exposant.
Exemple : pour calculer a^{19} on décompose 19 en base 2. $19 = 16 + 2 + 1 = 2^4 + 2^1 + 1$. Son écriture en base 2 est $10011 = (x_4, \ldots\ldots, x_0)$

A. ❶ Justifier que $a^{19} = a.(a^{2^3+1})^2$
On considère l'algorithme suivant :

```
Au départ y = 1
pour i variant de 4 à 0 par pas de 1.
si x_i = 0, y = y^2
si x_i = 1, y = ay^2
Afficher y.
```

❷ Exécuter cet algorithme à la main et vérifier que l'on trouve bien a^{19}

B. On veut calculer $4\,372^{19}$ modulo 7 241

❶ Vérifier que l'algorithme suivant permettra ce calcul :

```
Au départ y = 1
pour i variant de 4 à 0 par pas de 1.
si x_i = 0, y = y^2 mod (7 241)
si x_i = 1, y = 4372y^2 mod (7 241)
Afficher y.
```

❷ Vérifier que l'on trouve 2 734

C. Avec l'exponentiation classique on aurait utilisé 19 opérations, avec celle-ci, on n'en utilise que 5.

❶ Vérifier que si c possède n chiffres en base 2, $2^{n-1} \leqslant c < 2^n$.

❷ En déduire qu'il faut $E(\frac{\ln c}{\ln 2}) + 1$ opérations par exponentiation rapide, contre c opérations par exponentiation classique.

AP 4 Des signatures par RSA

Principe : On a vu qu'avec la clé publique publiée par Alice, tout le monde peut lui envoyer un message qu'elle seule peut lire. Mais comment sait-elle que c'est vraiment Bob qui lui a envoyé ?
Bob envoie à Alice un message clair M et lui associe une signature s

Propriétés requises :
identification du signataire : La signature ne peut pas être contrefaite :
authentification du message : La signature n'est pas réutilisable et le message signé est inaltérable :
non repudiation : Bob ne peut pas nier avoir signé le message :

Cette fois-ci : Bob publie sa clé publique (n', c') et garde pour lui sa clé privé d'.
(Les notations sont les mêmes que dans le TP 4)

Bob envoie à Alice le message M et $s = S'(M)$, congru à $M^{d'}$ modulo n', $0 \leqslant s < n'$.
Seul celui qui connait d' peut produire la signature s.

❶ La clé publique de Bob est (22733, 17). Vérifier que sa clé privée est 13193. Il trouve $s = 15364$.

❷ Bob envoie (6645, 15364) à Alice.

❸ Alice calcule $M' = P'(s)$, congru à $s^{c'}$ modulo n', $0 \leqslant M' < n'$. Vérifier que $M' = M$. Quelle conclusion peut en tirer Alice ? Justifier.

❹ On veut calculer s en utilisant l'algorithme de l'AP3. Pour cela, il faut commencer par décomposer 13193 en base 2 sur la calculatrice en liste L_1 par exemple puis inverser l'ordre des chiffres en liste L_2, puis utiliser l'algorithme de l'AP3.

4 Matrices

Vérifier ses acquis

1 Produit scalaire

1. On considère les deux vecteurs $\vec{u} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ dans un espace de dimension 2.
Calculer le produit scalaire de ces deux vecteurs.

2. a. Donner deux vecteurs d'un espace de dimension 3 et calculer leur produit scalaire.

b. On note ces vecteurs $\vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$.
Écrire l'expression analytique permettant de calculer leur produit scalaire.

3. Parmi les formules suivantes, quelle est celle qui correspond à la forme condensée de la réponse **2.b** ?

a. $\sum_{i=1}^{3} u_i v_i$. **b.** $u_i v_i \sum_{i=1}^{3} 1$. **c.** $u_i \sum_{i=1}^{3} v_i$.

2 Norme d'un vecteur

1. Rappeler la définition de la norme d'un vecteur $\vec{u} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$.

2. Rappeler le lien entre norme et produit scalaire.

3 Colinéarité

1. Rappelez la définition de deux vecteurs colinéaires.

2. On se place en dimension 2 et on note $\vec{u} = \begin{pmatrix} x \\ y \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} x' \\ y' \end{pmatrix}$ ces deux vecteurs. Parmi les conditions suivantes, donner celle équivalente à la définition :

a. $xx' + yy' = 0$; **b.** $xx' - yy' = 0$;
c. $xy' + yx' = 0$; **d.** $xy' - yx' = 0$;
e. $xy + x'y' = 0$; **f.** $xy - x'y' = 0$.

3. On se place maintenant en dimension 3, et on note $\vec{u} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$ ces deux vecteurs.

a. *On suppose que toutes les coordonnées sont non nulles. Quelles relations peut-on alors écrire entre ces coordonnées ?*

b. On suppose qu'il existe une coordonnée nulle, par exemple $x = 0$. En déduire une condition nécessaire au fait que $\vec{u}$ et $\vec{v}$ sont colinéaires.

4. Dans chacun des cas suivants, si les vecteurs sont colinéaires, donner le coefficient k tel que $\vec{u} = k\vec{v}$.

a. $\vec{u} = \begin{pmatrix} 6 \\ -5 \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} -24 \\ 20 \end{pmatrix}$.

b. $\vec{u} = \begin{pmatrix} -1 \\ 3 \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} 5 \\ 15 \end{pmatrix}$.

c. $\vec{u} = \begin{pmatrix} 3 \\ 1 \\ -5 \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} -9 \\ -3 \\ 15 \end{pmatrix}$.

4 Somme de vecteurs

On donne les vecteurs $\vec{u} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ et $\vec{v} = \begin{pmatrix} 3 \\ -1 \end{pmatrix}$.

a. Calculer les coordonnées du vecteur $\vec{w} = -2\vec{u} + 3\vec{v}$.

b. On donne $\vec{t} = \begin{pmatrix} 0 \\ -7 \end{pmatrix}$. Déterminer les coefficients a et b tels que $\vec{t} = a\vec{u} + b\vec{v}$.

5 Systèmes linéaires 1

1. Le système $\begin{cases} x + y = a \\ -y = b \end{cases}$ est équivalent à :

a. $\begin{cases} x = a - b \\ y = -b \end{cases}$. **b.** $\begin{cases} x = a + b \\ y = -b \end{cases}$. **c.** $\begin{cases} x = b - a \\ y = -b \end{cases}$.

2. Le système $\begin{cases} x - y = a \\ y = -b \end{cases}$ est équivalent à :

a. $\begin{cases} x = a - b \\ y = -b \end{cases}$. **b.** $\begin{cases} x = a + b \\ y = -b \end{cases}$. **c.** $\begin{cases} x = b - a \\ y = -b \end{cases}$.

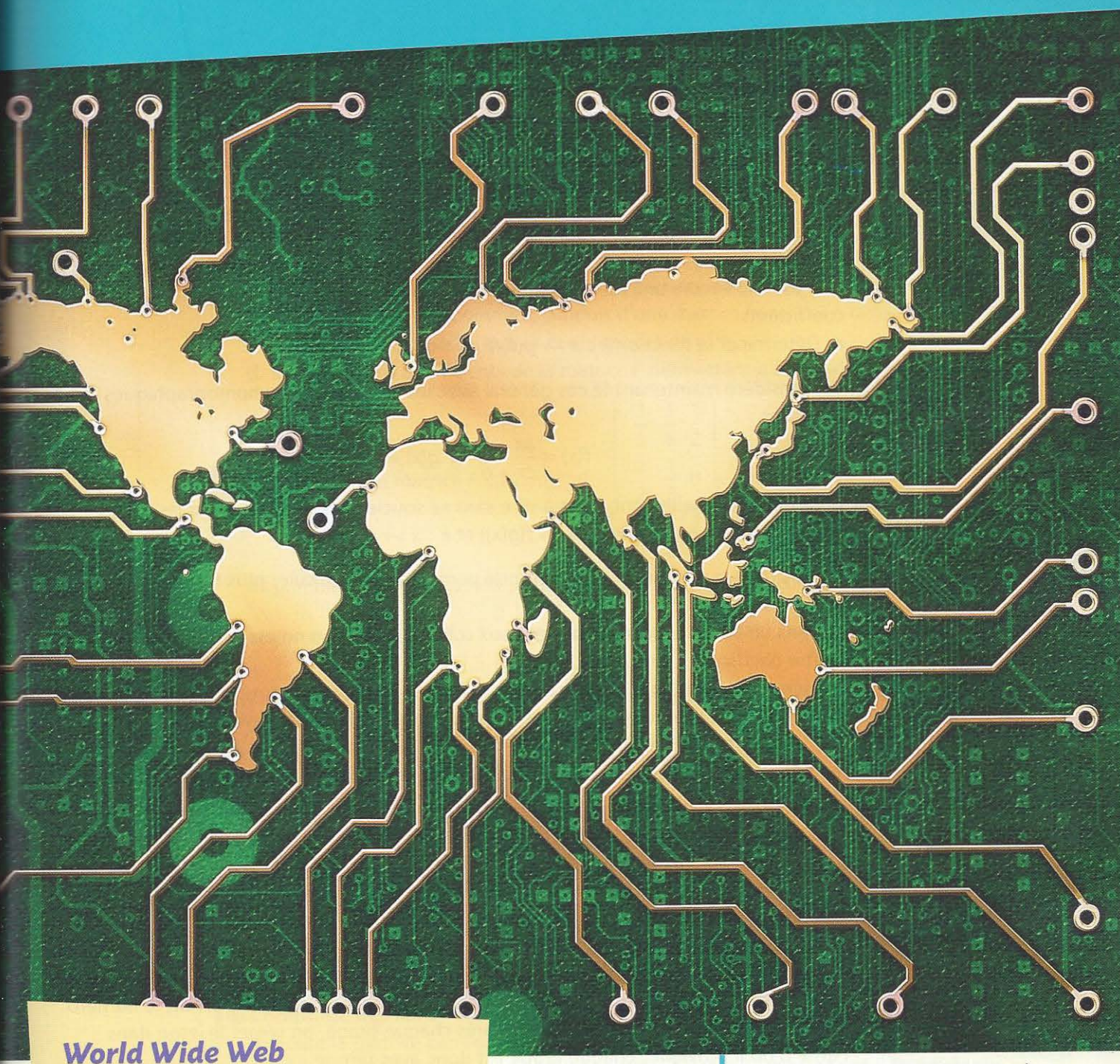
6 Systèmes linéaires 2

1. Résoudre les systèmes linéaires suivants :

a. $\begin{cases} 2x + y = 4 \\ -x - y = 6 \end{cases}$; **b.** $\begin{cases} 8x - 4y = 2 \\ -2x + y = -\frac{1}{2} \end{cases}$; **c.** $\begin{cases} x - 3y = -21 \\ -2x + 6y = -41 \end{cases}$.

2. a. Les deux vecteurs $\vec{u}_1 = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$ et $\vec{u}_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ extraits du 1er système sont-ils colinéaires ?

b. Même question pour les systèmes **b.** et **c.**



Représentation d'un monde mieux connecté dû, notamment, au développement et à la démocratisation d'Internet.

World Wide Web

Le *World Wide Web*, plus généralement appelé Web, ou Toile en français, est un système permettant de consulter des pages accessibles sur des sites. Chaque page permet de passer à d'autres pages à l'aide d'hyperliens.
Il ne faut pas confondre le Web et l'Internet : le Web n'est qu'une des applications de l'Internet qui permet l'utilisation d'autres services comme les messageries, électronique ou instantanée, le partage de fichiers, etc.

?

Lorsque l'on tape une expression, par exemple « World Wide Web », dans un moteur de recherche, dans quel ordre sont affichés les résultats ?

Quel est le nom de l'algorithme utilisé par Google permettant de classer les pages ?

Activités d'introduction

Activité 1 Un nouveau type de calcul

Objectifs
Revoir : calculer une fonction composée.
Découvrir : la notion de matrice ; le calcul matriciel.

1 On considère les deux fonctions homographiques suivantes :

$$f(x) = \frac{x-2}{-3x-5} \text{ et } g(x) = \frac{-5x+6}{7x+1}.$$

a. Vérifier que ces fonctions sont bien homographiques, puis déterminer manuellement la fonction $h : x \mapsto f(g(x))$.
b. h est-elle encore une fonction homographique ? Si oui, donner ses quatre coefficients.
c. Déterminer la fonction $k : x \mapsto g(f(x))$. A-t-on $h = k$?

2 On considère maintenant le cas général avec les deux fonctions homographiques suivantes :

$$f(x) = \frac{ax+b}{cx+d} \text{ et } g(x) = \frac{\alpha x+\beta}{\gamma x+\delta}.$$

Déterminer formellement, c'est-à-dire sans se soucier des conditions sur les coefficients, les fonctions $h : x \mapsto f(g(x))$ et $k : x \mapsto g(f(x))$.

3 On se propose de trouver une méthode permettant de calculer plus facilement ces coefficients.
a. Dans un tableau à deux lignes et deux colonnes, que l'on notera F, disposer les quatre coefficients de f.
b. Même consigne pour les fonctions g et h dans des tableaux notés G et H.
c. Compléter toutes les phrases possibles suivantes : « le coefficient à la …e ligne et … e colonne de H est obtenu comme la somme des produits des coefficients de la … e ..... de F par ceux de la … e ..... de G. » On note H = F × G ou encore FG.

4 **a.** Selon cette nouvelle méthode, calculer les coefficients de la fonction $k : x \mapsto g(f(x))$ et dresser le tableau correspondant K = GF.
b. A-t-on FG = GF ?

Activité 2 Une urne, puis une seconde

Objectifs
Revoir : formule des probabilités totales. Notation Σ.

On considère trois urnes numérotées de 1 à 3 et dans chaque urne des jetons portant les chiffres de 1 à 3. L'expérience consiste à tirer un jeton de l'urne portant le numéro du jeton tiré dans l'urne précédente. Après chaque tirage, on remet le jeton dans l'urne d'où il provient : chaque tirage est donc avec remise.
Lors du n-ième tirage, on note X_n la valeur du jeton tiré et donc le numéro de l'urne qui servira au $(n+1)$-ième tirage. On définit alors la suite de variables aléatoires $(X_n)_{n\in\mathbb{N}}$, que l'on initialise par la valeur X_0, qui est l'urne dans laquelle on piochera pour la première fois.
On ne s'intéressera dans ce chapitre qu'à l'issue du premier tirage (pour les tirages suivants, voir l'activité 1 p. 142), et le but est de répondre aux questions suivantes : étant donnée une valeur de X_0, quelle est la probabilité que $X_1 = 1$? que $X_1 = 2$? que $X_1 = 3$?

1 **a.** Pour tous i et j entre 1 et 3, on note p_{ij} la proportion de jetons portant le numéro i dans l'urne j. Exprimer p_{ij} sous la forme d'une probabilité conditionnelle portant sur les événements $(X_0 = \ldots)$ et $(X_1 = \ldots)$.

b. En remarquant que l'ensemble d'événements $\{(X_0 = 1) ; (X_0 = 2) ; (X_0 = 3)\}$ forme une partition de l'espace de probabilités, établir que pour tous i et j entre 1 et 3 :

$$P(X_1 = i) = \sum_{j=1}^{3} p_{ij} P(X_0 = j).$$

2 Pour tout entier naturel n, on pose $\mu^{(n)} = \begin{pmatrix} P(X_n = 1) \\ P(X_n = 2) \\ P(X_n = 3) \end{pmatrix}$.

a. Détailler la formule donnant la première coordonnée de $\mu^{(1)}$.
b. Écrire cette formule comme le produit d'une matrice ligne 1×3 à déterminer par $\mu^{(0)}$.
c. Faire de même pour les autres coordonnées de $\mu^{(1)}$.
d. En déduire les coefficients de la matrice P permettant d'écrire $\mu^{(1)} = P\mu^{(0)}$.

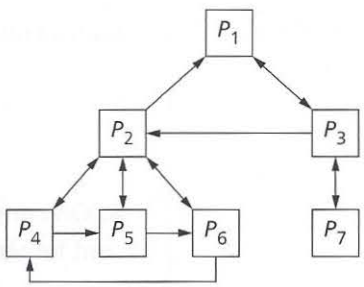
3 On considère la matrice P suivante : $P = \begin{pmatrix} \frac{1}{5} & \frac{1}{6} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{3} & 0 \\ \frac{3}{10} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$.

a. Combien y a-t-il de jetons portant chaque numéro dans chaque urne ?
b. On suppose que $\mu^{(0)} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$. Que cela signifie-t-il ?
c. Déterminer manuellement $\mu^{(1)}$ et vérifier à l'aide d'un logiciel de calcul formel.

Activité 3 Étude du principe du calcul de la pertinence d'une page Web

OBJECTIFS
Revoir : le produit ligne par colonne.
Découvrir : une utilisation concrète du calcul matriciel.

On considère un (petit) réseau, constitué de 7 pages Web. Chacune de ces pages émet des liens hypertextes vers d'autres pages du réseau. On peut représenter ce réseau par le graphe ci-contre, où les pages sont numérotées de P_1 à P_7 et chaque lien est représenté par un segment fléché.



1 **Comptage des liens**

a. Écrire la matrice carrée A de taille 7 que l'on complètera de la manière suivante : le coefficient à la i-ème ligne et j-ème colonne, noté a_{ij}, vaut 1 si la page P_i reçoit un lien de la page P_j ; 0 sinon.
b. Calculer les nombres suivants après avoir détaillé les formules :

$$\eta_3 = \sum_{i=1}^{7} a_{i3} \quad \text{et} \quad \mu_3 = \sum_{j=1}^{7} a_{3j}.$$

c. Que mesurent η_3 et μ_3 pour la page P_3 ?
d. D'après-vous, une page Web est-elle importante si elle émet ou reçoit beaucoup de liens ?
e. Une page Web étant donnée, quelle mesure peut-on facilement manipuler et comment ? Proposez un graphe permettant de donner de l'importance à la page P_3.
f. À l'aide des questions **d.** et **e.**, validez-vous ou invalidez-vous ce modèle de calcul de pertinence d'une page Web ?

2 Comptage pondéré

On va donc accorder une importance plus faible aux pages émettant beaucoup de liens, celles-ci étant moins spécifiques ; cette importance est inversement proportionnelle au nombre de liens émis. On pose $\eta = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_7 \end{pmatrix}$ et on définit maintenant l'importance μ_3 de la page P_3 par :

$$\mu_3 = \sum_{j=1}^{7} a_{3j} \frac{1}{\eta_j}.$$

a. Calculer η, puis μ_3.

b. Compléter la phrase suivante : « Le 3e coefficient de μ est obtenu comme le produit de la ...e ..... de la matrice A par le vecteur colonne $\begin{pmatrix} \frac{1}{\eta_1} \\ \vdots \\ \frac{1}{\eta_7} \end{pmatrix}$ ». Généraliser.

e. Ce modèle de mesure de pertinence est-il facilement manipulable ? Si oui, proposez un graphe permettant de donner de l'importance à la page P_3.

3 Comptage récursif

On va maintenant appliquer le principe suivant : « une page est importante si beaucoup d'autres pages importantes pointent vers elle ». L'importance de la page P_i est alors définie par :

$$\mu_i = \sum_{j=1}^{7} m_{ij} \mu_j,$$

où les coefficients de la matrice M sont définis de la manière suivante :

$$m_{ij} = \begin{cases} \frac{1}{\eta_j} \text{ si } P_i \text{ reçoit un lien de } P_j \\ 0 \text{ sinon} \end{cases}.$$

a. On considère une page P_i « vide » seulement émettrice de liens. Pour tout j, quelles sont les valeurs des coefficients m_{ij} ? En déduire son importance μ_i.

b. Cette page contribuera-t-elle au calcul de l'importance des autres pages ? Expliquer pourquoi.

c. Détailler la formule permettant de calculer μ_2.

d. Les coefficients de M apparaissant dans cette formule proviennent-ils d'une ligne ou colonne de M ?

e. Vérifier que ces coefficients sont égaux à $0 ; 0 ; \frac{1}{3} ; \frac{1}{2} ; \frac{1}{2} ; \frac{1}{2} ; 0$.

f. Compléter la seule des deux phrases suivantes qui est correcte (justifier) :
« le 2e coefficient de μ est obtenu comme le produit du vecteur ligne μ par la 2e ..... de la matrice M » ;
« le 2e coefficient de μ est obtenu comme le produit de la 2e ..... de la matrice M par le vecteur colonne μ ».

g. En déduire l'équation matricielle vérifiée par μ et vérifier (à la main ou à l'aide d'un logiciel) qu'une solution possible est : $\mu = \begin{pmatrix} 2 \\ 4 \\ 3 \\ 2 \\ 2 \\ 2 \\ 1 \end{pmatrix}$. En déduire la page la plus importante.

Activité 4 Résolution d'un système linéaire

Objectif
Découvrir : la notion de matrice inverse.

1 On considère le système de trois équations à trois inconnues suivant :

$$\begin{cases} x + y + z = 2 \\ 2x - y - 2z = -1 \\ x + 2y - z = -3 \end{cases} \Leftrightarrow \text{(E)}.$$

a. On pose $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $Y = \begin{pmatrix} 2 \\ -1 \\ -3 \end{pmatrix}$. Quelle est la matrice M qui permet d'écrire le système (E) sous la forme $MX = Y$?

Aide
On recherchera trois vecteurs ligne tels que leur produit avec X donne la première ligne du système, la deuxième, puis la troisième.

b. On pose $N = \begin{pmatrix} \frac{1}{2} & \frac{3}{10} & -\frac{1}{10} \\ 0 & -\frac{1}{5} & \frac{2}{5} \\ \frac{1}{2} & -\frac{1}{10} & \frac{-3}{10} \end{pmatrix}$. Calculer les produits MN et NM.

→ *Voir TP Algorithmique 2 p. 119 pour le calcul d'une matrice inverse*

c. Une telle matrice N est unique et est appelée la matrice inverse de M. On note alors $N = M^{-1}$. (On peut vérifier cet inverse à l'aide d'un logiciel de calcul formel). Démontrer que $X = M^{-1}Y$.

d. Calculer $M^{-1}Y$ afin de déterminer la solution du système (E).

2 On considère maintenant le système suivant $\begin{cases} x + y + z = 4 \\ 2x - y - 4z = 5 \\ -x + 2y + 5z = -1 \end{cases} \Leftrightarrow \text{(F)}.$

a. Écrire ce système sous forme matricielle. On notera M la matrice correspondante au système.

b. Demander à un logiciel ou à une calculatrice de calculer l'inverse de M. Pouvez-vous résoudre ce système selon la méthode précédente ?

c. Démontrer que si un triplet est solution de (F), alors il est aussi solution de $(F_1) \Leftrightarrow \begin{cases} x + y + z = 4 \\ y + 2z = 1 \end{cases}$.

Aide
On pourra combiner astucieusement les 2e et 3e lignes avec la 1re de (F) afin d'en faire disparaître la première inconnue.

d. En considérant les mêmes calculs « à l'envers », démontrer la réciproque.

e. En prenant z comme paramètre, en déduire que toutes les solutions de (F) sont $\begin{pmatrix} z+3 \\ 1-2z \\ z \end{pmatrix}$, $z \in \mathbb{R}$ et qu'une solution particulière est $\begin{pmatrix} 4 \\ -1 \\ 1 \end{pmatrix}$.

A Notion de matrice

1 Coefficients et taille d'une matrice

Définition 1

Une matrice est un tableau de nombres, ceux-ci étant appelés coefficients de la matrice. Si n et p représentent respectivement le nombre de lignes et de colonnes du tableau, on dit que la matrice est de taille $n \times p$. n et p sont appelés dimensions de la matrice. Le coefficient situé à la i-ème ligne et la j-ème colonne d'une matrice A se note a_{ij} ou, s'il peut y avoir ambiguïté, $a_{\{i,j\}}$.

Exemple : Dans la matrice A suivante de taille 2×3, on a par exemple : $a_{12} = 5$; $a_{22} = -7$.

$$A = \begin{pmatrix} -1 & 5 & -6 \\ 2 & -7 & 4 \end{pmatrix}.$$

Remarque : Usuellement, les coefficients sont pris dans l'ensemble des nombres réels, entiers naturels, relatifs, etc. mais on peut aussi choisir d'autres ensembles comme par exemple l'ensemble des restes de la division euclidienne par un entier naturel b, soit $\{0 ; 1 ; \ldots ; b - 1\}$, les nombres complexes, etc.

2 Matrices particulières

Définition 2

Une matrice ayant le même nombre n de lignes et de colonnes est appelée matrice carrée de taille $n \times n$ (ou plus simplement n).
Une matrice n'ayant qu'une seule ligne est appelée vecteur (ou matrice) ligne de taille $1 \times p$ (ou plus simplement p).
Une matrice n'ayant qu'une seule colonne est appelée vecteur (ou matrice) colonne de taille $n \times 1$ (ou plus simplement n).

Exemple : Les matrices A, B et C suivantes sont de tailles 3, 1×3 et 2×1. A est une matrice carrée, B un vecteur ligne et C un vecteur colonne.

$$A = \begin{pmatrix} -1 & 5 & -6 \\ 2 & -7 & 4 \\ -4 & 1 & 9 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 5 & -6 \end{pmatrix}, \quad C = \begin{pmatrix} 5 \\ -7 \end{pmatrix}.$$

Remarque : Une matrice nulle est une matrice dont tous les coefficients sont nuls.

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad O = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Remarque : La matrice unité de taille n, notée I_n, est la matrice carrée de taille n dont tous les coefficients sont nuls sauf ceux situés à la i-ème ligne et i-ème colonne et qui valent 1.

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ etc.}$$

Savoir-faire 1

Entrer une matrice dans une calculatrice ou un logiciel

→ *Exercice corrigé 11 p. 123*
→ *Exercices d'application 12 à 16 p. 123*

Énoncé

Entrer la matrice $A = \begin{pmatrix} 1 & -9 \\ -8 & 2 \\ 7 & -6 \end{pmatrix}$.

Solution

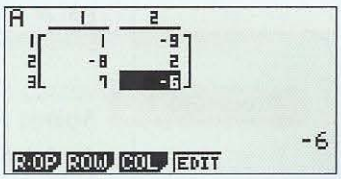
Avec une CASIO

① Menu, puis sélectionner 

② Choisir « >MAT », (F3), puis sélectionner la matrice dans laquelle stocker et appuyer sur DIM (F3) ou EXE

③ Entrer les dimensions puis valider en appuyant sur EXE

④ Entrer les coefficients pour obtenir le résultat suivant :



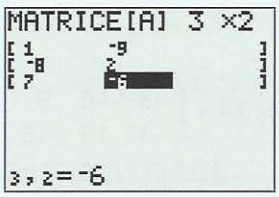
Avec une TI

① Accéder au menu matrice en appuyant sur la touche matrice

② Choisir le menu EDIT puis enter

③ Entrer les dimensions puis valider en appuyant sur enter

④ Entrer les coefficients pour obtenir le résultat suivant :

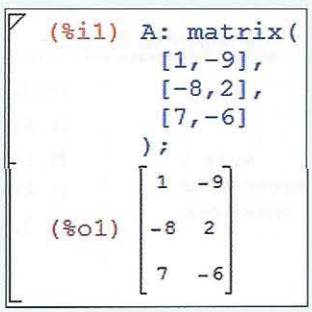


Avec Maxima

① Dans le menu « Algèbre », cliquer sur « Entrer une matrice… »

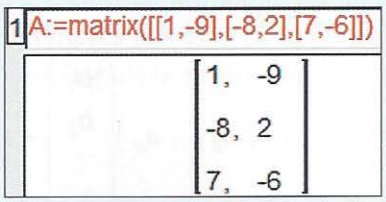
② Indiquer les dimensions puis le nom de la matrice.

③ Entrer les coefficients et valider la saisie pour obtenir le résultat suivant :



Avec Xcas

Dans la barre de saisie, on écrit « A:=matrix([[1,–9],[–8,2],[7,–6]]) » et on valide pour obtenir le résultat suivant :



En JavaScript

Une matrice est considérée comme un tableau de lignes. On écrit donc :

```
1 A = [[1,-9],[-8,2],[7,-6]];
```

B Opérations sur les matrices

1 Addition et multiplication par un réel

Définition 3

Soient A et B deux matrices de même taille. La somme de A et B, notée $A + B$, est une matrice ayant encore la même taille et dont chaque coefficient est la somme des coefficients de A et B situés à la même ligne et même colonne.

Exemple :

Si $A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & -6 \end{pmatrix}$ et $B = \begin{pmatrix} -3 & 5 & -7 \\ 2 & -4 & 6 \end{pmatrix}$, alors $A + B = \begin{pmatrix} -2 & 3 & -4 \\ -2 & 1 & 0 \end{pmatrix}$.

Propriété 1

Soient A, B, C et O quatre matrices de même taille, O étant la matrice nulle.

a. $A + B = B + A$.

b. $A + (B + C) = (A + B) + C$ et on note plus simplement $A + B + C$.

c. $A + O = O + A = A$.

Définition 4

Soient A une matrice et k un réel. Le produit de la matrice A par le réel k est la matrice, notée kA, de même taille que A dont chaque coefficient est le produit du coefficient de A situé à la même ligne et même colonne par k.

Exemple :

Si $A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & -6 \end{pmatrix}$, alors $3A = \begin{pmatrix} 3 & -6 & 9 \\ -12 & 15 & -18 \end{pmatrix}$; $-A = \begin{pmatrix} -1 & 2 & -3 \\ 4 & -5 & 6 \end{pmatrix}$.

Propriété 2

Soient A, B et O trois matrices de même taille, O étant la matrice nulle ; k et k' deux réels.

a. $k(A + B) = kA + kB$.

b. $(k + k')A = kA + k'A$.

c. $k(k')A = (kk')A$ et on note plus simplement $kk'A$.

d. $1A = A$; $(-1)A$ est notée $-A$; $A + (-A) = O$; $0A = O$.

Note :
– A est appelée matrice opposée de A.

2 Produit de deux matrices

Définition 5

Soient A un vecteur ligne de taille $1 \times n$ et B un vecteur colonne de taille $n \times 1$. Le produit de A par B, noté AB, est un nombre obtenu de la façon suivante :

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1b_1 + a_2b_2 + \dots + a_nb_n = \sum_{i=1}^{n} a_ib_i.$$

Remarque : En dimension 2 ou 3, on retrouve le produit scalaire de deux vecteurs que l'on connaît déjà.

Savoir-faire 2 Parcourir algorithmiquement tous les coefficients d'une matrice

→ Exercice corrigé 17 p. 123
→ Exercices d'application 18 à 22 p. 124

Énoncé

a. Définir la matrice A de taille 4×3 dont chaque coefficient a_{ij} est le produit du numéro de ligne par le numéro de colonne.
b. Définir la matrice identité de taille 5.

Solution

a.

```
Pour i = 1 à 4 faire
   Pour j = 1 à 3 faire
      aij = i*j ;
   FinPour
FinPour
```

→ Dans certains langages de programmation, la numérotation commence à 0.

Méthode

- On parcourt toutes les lignes.
- Dans chaque ligne, on parcourt toutes les colonnes.
- Pour modifier le coefficient présent dans cette ligne et cette colonne.

Remarque : On aurait très bien pu intervertir les deux boucles et parcourir toutes les colonnes, et dans chaque colonne, toutes les lignes.

b.

```
Pour i = 1 à 5 faire
   Pour j = 1 à 5 faire
      Si i==j, alors
         aij = 1 ;
      Sinon
         aij = 0 ;
      FinSi
   FinPour
FinPour
```

Savoir-faire 3 Additionner des matrices

→ Exercice corrigé 23 p. 124
→ Exercices d'application 14 à 28 p. 124

Énoncé

Soient $A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & -6 \end{pmatrix}$ et $B = \begin{pmatrix} 7 & -8 & 9 \\ -10 & 11 & -12 \end{pmatrix}$.

Calculer $A + 2B$ et stocker la somme dans C.

Solution

Avec une CASIO

On écrit Mat A + 2Mat B -> Mat C
On trouve la commande Mat dans OPTN, MAT (F2), Mat (F1)

Avec une TI

On écrit [A] + 2[B] -> [C]
On insère les noms des matrices depuis le menu matrice et en sélectionnant le bon nom dans la liste.

Avec Maxima / Xcas

On écrit C:A+2*B / C:=A+2B

En JavaScript

On écrit une double boucle comme dans la solution **a.** du savoir-faire 2 en utilisant l'affectation `cij = aij + 2bij` .

Définition 6

Soient A une matrice de taille $n \times p$ et B un vecteur colonne de taille $p \times 1$. Le produit de A par B, noté AB, est un vecteur colonne de taille $n \times 1$ dont chaque coefficient est obtenu comme le produit de chaque ligne de A par B.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & \ddots & & a_{2p} \\ \vdots & & \ddots & \\ a_{n1} & a_{n2} & \cdots & a_{np} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_p \end{pmatrix} = \begin{pmatrix} L_1 B \\ L_2 B \\ \vdots \\ L_n B \end{pmatrix} = \begin{pmatrix} a_{11}b_1 + \ldots + a_{1p}b_p \\ a_{21}b_1 + \ldots + a_{2p}b_p \\ \vdots \\ a_{n1}b_1 + \ldots + a_{np}b_p \end{pmatrix},$$

où L_i désigne la i-ème ligne de la matrice A.

Exemple :

Si $A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & -6 \end{pmatrix}$ et $B = \begin{pmatrix} 7 \\ -8 \\ 9 \end{pmatrix}$, alors $AB = \begin{pmatrix} 1\times 7 - 2\times(-8) + 3\times 9 \\ -4\times 7 + 5\times(-8) - 6\times 9 \end{pmatrix} = \begin{pmatrix} 50 \\ -122 \end{pmatrix}$.

Définition 7

Soient A un vecteur ligne de taille $1 \times n$ et B une matrice de taille $n \times p$. Le produit de A par B, noté AB, est un vecteur ligne, de taille $1 \times p$ dont chaque coefficient est obtenu comme le produit de A par chaque colonne de B.

Exemple :

Si $A = \begin{pmatrix} 1 & -2 & 3 \end{pmatrix}$ et $B = \begin{pmatrix} -4 & 5 \\ -6 & 7 \\ -8 & 9 \end{pmatrix}$, alors $AB = \begin{pmatrix} -4 + 12 - 24 & 5 - 14 + 27 \end{pmatrix} = \begin{pmatrix} -16 & 18 \end{pmatrix}$.

Définition 8

Soient A une matrice de taille $n \times p$ et B une matrice de taille $p \times q$. Le produit de A par B, noté AB, est une matrice de taille $n \times q$ dont le coefficient à la i-ème ligne et j-ème colonne est obtenu par le produit de la i-ème ligne de A par la j-ème colonne de B.

Note :
On ne peut calculer AB que si le nombre de colonnes de A est égal au nombre de lignes de B. Dans le cas où il est aussi possible de calculer BA, ce résultat n'est en général pas égal à AB.

Exemple :

Si $A = \begin{pmatrix} 1 & -2 & 3 \\ -4 & 5 & -6 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 2 & -3 \\ 4 & -5 & 6 \\ -7 & 8 & -9 \end{pmatrix}$, alors $AB = \begin{pmatrix} -30 & 36 & -42 \\ 66 & -81 & 96 \end{pmatrix}$.

On a obtenu -30 par le calcul suivant : $1 \times (-1) + (-2) \times 4 + 3 \times (-7)$.

Définition 9

Pour tout entier naturel, on appelle puissance n-ième d'une matrice carrée A, que l'on note A^n, le produit $\underbrace{A \times \ldots \times A}_{n \text{ fois}}$. Par convention, on a $A^0 = I$.

3 Propriétés du produit

Propriété 3

Soient A, B, C et I (matrice unité) des matrices dont les tailles permettent d'effectuer les opérations ci-dessous, ainsi qu'un réel k.

a. $A(BC) = (AB)C$.
b. $A(B + C) = AB + AC$.
c. $(A + B)C = AC + BC$.
d. $(kA)B = A(kB) = k(AB)$.
e. $IA = AI = A$.

Savoir-faire 4 Effectuer un produit de matrices

→ Exercice corrigé 29 p. 125
→ Exercices d'application 30 à 36 p. 125

Énoncé

Calculer le produit AB dans tous les cas suivants, lorsque cela est possible :

a. $A = (-2 \;\; 6 \;\; -5)$ et $B = \begin{pmatrix} 3 \\ 8 \\ -4 \end{pmatrix}$.

b. $A = (-2 \;\; 6 \;\; -5)$ et $B = \begin{pmatrix} 3 & -5 \\ 8 & 1 \\ -4 & -1 \end{pmatrix}$.

c. $A = (-2 \;\; 6 \;\; -5)$ et $B = \begin{pmatrix} 3 & -5 & -4 \\ 8 & 1 & -1 \end{pmatrix}$.

d. $A = \begin{pmatrix} -2 & 6 & -5 \\ 1 & 8 & -6 \\ -4 & 2 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} 3 \\ 8 \\ -4 \end{pmatrix}$.

e. $A = \begin{pmatrix} -2 & 6 & -5 \\ 1 & 8 & -6 \\ -4 & 2 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & -5 \\ 8 & 1 \\ -4 & -1 \end{pmatrix}$.

f. $A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ et $B = \begin{pmatrix} -3 & 2 \\ 2 & -1 \end{pmatrix}$.

Méthode

On commence par vérifier que le nombre de colonnes de A correspond au nombre de lignes de B et on détermine les dimensions de la matrice produit.
On peut vérifier les résultats à l'aide d'une calculatrice ou d'un logiciel à l'aide des instructions suivantes :

- Mat A × Mat B avec une CASIO ;
- [A]*[B] avec une TI ;
- A.B avec Maxima ;
- A*B avec Xcas.

Solution

a. Il s'agit du produit d'une matrice 1×3 par une matrice 3×1. La matrice produit sera donc de taille 1×1, et on a alors $AB = (-2 \times 3 + 6 \times 8 - 5 \times (-4)) = (62)$.

b. Il s'agit du produit d'une matrice 1×3 par une matrice 3×2. La matrice produit sera donc de taille 1×2 et on a alors $AB = (62 \;\; 21)$.

c. Il s'agit du produit d'une matrice 1×3 par une matrice 2×3. Ce produit est impossible car le nombre de colonnes de A n'est pas le même que celui de ligne de B. D'ailleurs, si l'on tente d'effectuer ce produit à l'aide d'un logiciel ou calculatrice, on obtient une erreur liée aux dimensions.

d. Il s'agit du produit d'une matrice 3×3 par une matrice 3×1. La matrice produit sera donc de taille 3×1 et on a alors $AB = \begin{pmatrix} 62 \\ 91 \\ 8 \end{pmatrix}$.

e. Il s'agit du produit d'une matrice 3×3 par une matrice 3×2. La matrice produit sera donc de taille 3×2 et on a alors $AB = \begin{pmatrix} 62 & 21 \\ 91 & 9 \\ 8 & 23 \end{pmatrix}$.

f. Il s'agit du produit d'une matrice 2×2 par une matrice 2×2. La matrice produit sera donc de taille 2×2 et on a alors $AB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

C Matrices inversibles

1 Définition et inverse des matrices de taille 2

Définition 10

Soit A une matrice carrée de taille n.
On appelle matrice inverse de A, lorsqu'elle existe, toute matrice carrée M de taille n, telle que $AM = MA = I_n$.

Propriété 4

Lorsqu'une matrice inverse existe, elle est unique et on la note A^{-1}.

Note : *Une matrice non carrée ne peut pas admettre d'inverse, à cause d'un problème de dimensions.*

Démonstration : Notons M et N, deux matrices inverses de A.
On a alors $M = MI_n = M(AN) = (MA)N = I_nN = N$.

Exemples :
On considère la matrice $A = \begin{pmatrix} 5 & 9 \\ 1 & 2 \end{pmatrix}$, alors on peut vérifier que $A^{-1} = \begin{pmatrix} 2 & -9 \\ -1 & 5 \end{pmatrix}$.

On considère la matrice $B = \begin{pmatrix} 6 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}$, alors on peut vérifier que $B^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ -5 & 30 & 1 \\ -1 & 6 & 0 \end{pmatrix}$.

Propriété 5

Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice carrée de taille 2.
A est inversible si, et seulement si, la quantité $ad - bc$ est différente de 0.

Démonstration : Introduisons la matrice $N = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$. On a alors $AN = NA = (ad - bc)I_2$.
Ainsi, si $ad - bc \neq 0$, alors A^{-1} existe et on a $A^{-1} = \dfrac{1}{ad - bc}N$. Réciproquement, si A^{-1} existe, alors $N = N(AA^{-1}) = (NA)A^{-1} = (ad - bc)A^{-1}$. N n'étant pas la matrice nulle, $ad - bc \neq 0$.

Remarque : On a en plus une formule donnant l'inverse d'une matrice de taille 2.

2 Résolution de systèmes linéaires

Définition 11

Tout système linéaire de n équations à p inconnues peut s'écrire sous une forme matricielle du type $MX = Y$, d'inconnue X, où M est une matrice de taille $n \times p$.

Exemple :
Le système $\begin{cases} 2x - 3y + z = -5 \\ -x - 4z = 2 \end{cases}$ peut s'écrire sous la forme $MX = Y$, avec

$M = \begin{pmatrix} 2 & -3 & 1 \\ -1 & 0 & -4 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $Y = \begin{pmatrix} -5 \\ 2 \end{pmatrix}$.

Propriété 6

On considère un système linéaire de n équations à n inconnues s'écrivant sous la forme $MX = Y$, où M est une matrice carrée de taille n. Si M est inversible, alors les solutions sont données par le vecteur colonne $X = M^{-1}Y$.

Savoir-faire 5 Déterminer l'inverse d'une matrice

→ Exercice corrigé 37 p. 125
→ Exercices d'application 38 à 43 p. 125

Énoncé

Déterminer l'inverse de la matrice $A = \begin{pmatrix} 5 & 9 \\ 1 & 2 \end{pmatrix}$ si cet inverse existe.

Méthode

Pour les matrices 2×2, on peut encore effectuer le travail à la main.
Pour les matrices de tailles supérieures, cette technique est trop coûteuse en temps. On préfère utiliser des logiciels qui utilisent un algorithme d'inversion. Un de ces algorithmes est étudié en TP.

Solution

À la main

On pose $A^{-1} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, et on effectue le produit

$AA^{-1} = \begin{pmatrix} 5a+9b & 5c+9d \\ a+2b & c+2d \end{pmatrix}$.

On résout alors le système $\begin{cases} 5a+9b=1 \\ 5c+9d=0 \\ a+2b=0 \\ c+2d=1 \end{cases} \Leftrightarrow \begin{cases} a=2 \\ b=-1 \\ c=-9 \\ d=5 \end{cases}$. L'inverse de A est donc bien la matrice donnée dans la partie cours ci-contre.

Avec une CASIO

On écrit Mat A^{-1}, en sélectionnant les touches :
OPTN MAT (F2) Mat (F1) A (ALPHA X,θ,T)$^{-1}$ (SHIFT))

Avec une TI

On écrit $[A]^{-1}$, en sélectionnant [A] depuis le menu matrice

Note :
Avec Maxima
On écrit « invert(A) ». On trouvera cette commande dans le menu Algèbre/Inverser la matrice.
Avec Xcas
On écrit « inv(A) ». On trouvera cette commande dans le menu CAS/Algèbre linéaire.

Savoir-faire 6 Résoudre un système linéaire

→ Exercice corrigé 44 p. 126
→ Exercices d'application 45 à 54 p. 126

Énoncé

Résoudre les systèmes (E) $\Leftrightarrow \begin{cases} 5x+9x=3 \\ x+2y=-2 \end{cases}$ et

(F) $\Leftrightarrow \begin{cases} -2x+6y-5z=0 \\ x+8y-6z=1 \\ -4x+2y-z=2 \end{cases}$.

Méthode

1. On écrit le système sous forme matricielle.
2. On inverse la matrice, lorsque cela est possible.
3. On résout le système en effectuant un calcul matriciel.

Solution

Le système (E) est équivalent à $A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$, où A est la matrice du savoir-faire 5. On a alors $\begin{pmatrix} x \\ y \end{pmatrix} = A^{-1}\begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 24 \\ -13 \end{pmatrix}$.

Le système (F) est équivalent à $B\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$, où $B = \begin{pmatrix} -2 & 6 & -5 \\ 1 & 8 & -6 \\ -4 & 2 & -1 \end{pmatrix}$. On a alors

$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = B^{-1}\begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} -\frac{1}{7} \\ \frac{13}{7} \\ \frac{16}{7} \end{pmatrix}$.

TP Algorithmique 1 Résolution d'un système 2x2



Objectifs :
- Travailler sur la colinéarité.
- Connaître le nombre de solutions d'un système 2x2.

Géométriquement, la résolution d'un système 2x2 correspond à la recherche du point d'intersection de deux droites dont on connaît les équations cartésiennes. On considère alors le système de deux équations à deux inconnues suivant :

$$\begin{cases} ax + cy = e \\ bx + dy = f \end{cases} \Leftrightarrow \text{(E)}.$$

On voudrait, sans avoir à résoudre le système, connaître le nombre de solution(s).

1 Considérations géométriques

Soient (d_1) et (d_2), les deux droites du plan correspondant aux équations cartésiennes du système (E). À quelle condition sur ces droites le système (E) a-t-il :

a. une unique solution ?

b. aucune solution ?

c. une infinité de solution ?

2 Traductions vectorielles

a. Donner des vecteurs directeurs $\vec{u_1}$ et $\vec{u_2}$ de (d_1) et (d_2).

b. Traduire les conditions établies à la question **1.** en terme de colinéarité de ces deux vecteurs.

c. Traduire analytiquement ces mêmes conditions.

3 Étude algébrique

Les conditions analytiques pour **1.b.** et **1.c.** étant identiques, poussons plus loin notre analyse.

a. Pourquoi peut-on supposer $a \neq 0$ ou $b \neq 0$?

Aide

Supposer la condition contraire, c'est-à-dire « a = 0 et b = 0 », puis considérer le système obtenu.

b. Quitte à échanger les deux équations, on suppose donc que $a \neq 0$. Remplacer L_2 par la combinaison linéaire $aL_2 - bL_1$ afin d'obtenir un système équivalent à (E) dans lequel on a éliminé l'inconnue x de la seconde équation.

c. Pourquoi était-il important de supposer $a \neq 0$?

d. Retrouver alors la condition établie en **2.c.** qui porte ici sur le coefficient de l'inconnue y pour que ce système admette une unique solution. En déduire les formules permettant de calculer les valeurs de y et de x.

e. Si cette condition n'est pas remplie, à quelle autre condition le système ne possède-t-il pas de solution ? Une infinité de solutions ? Dans ce dernier cas, que cela signifie-t-il sur les deux équations du système ?

4

Écrire un algorithme prenant en paramètre les six réels a, b, c, d, e, f et donnant le nombre de solution(s) du système (E) ainsi que leur valeur lorsque cela est possible.

5

Appliquer cet algorithme aux systèmes suivants :

a. $\begin{cases} -x + 2y = 15 \\ 5x - 10y = -4 \end{cases}$; **b.** $\begin{cases} 2x + 3y = 4 \\ 5x - 6y = 7 \end{cases}$;

c. $\begin{cases} 3x - y = 1 \\ -9x + 3y = -3 \end{cases}$.

TP Algorithmique 2 Calcul de l'inverse d'une matrice



Objectif :
- *Savoir comment est calculé l'inverse d'une matrice dans un logiciel.*

On propose de faire tester l'algorithme de Gauss-Jordan, permettant de calculer l'inverse d'une matrice.

1 On considère la matrice M suivante :

$$M = \begin{pmatrix} -1 & -2 & -3 \\ 5 & 3 & 6 \\ -8 & 2 & -1 \end{pmatrix}.$$

Déterminer son inverse (s'il existe) à l'aide d'un logiciel de calcul formel ou d'une calculatrice.

2 Pour déterminer algorithmiquement M^{-1}, on va considérer la matrice augmentée suivante :

$$A = \left(\begin{array}{ccc|ccc} -1 & -2 & -3 & 1 & 0 & 0 \\ 5 & 3 & 6 & 0 & 1 & 0 \\ -8 & 2 & -1 & 0 & 0 & 1 \end{array}\right).$$

a. Diviser la ligne L_1 par le coefficient a_{11}.

b. Remplacer la ligne L_2 par $L_2 - a_{21}L_1$.

c. Remplacer la ligne L_3 par $L_3 - \ldots L_1$ et vérifier que l'on obtient bien la matrice suivante :

$$A_1 = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & -1 & 0 & 0 \\ 0 & -7 & -9 & 5 & 1 & 0 \\ 0 & 18 & 23 & -8 & 0 & 1 \end{array}\right).$$

3 On recommence le procédé avec la ligne L_2.

a. Diviser la ligne L_2 par le coefficient ...

b. Remplacer la ligne L_1 par $L_1 - \ldots L_2$ et la ligne L_3 par $L_3 - \ldots L_2$.

4 Recommencer le procédé avec la ligne L_3. On obtient alors dans la partie gauche la matrice identité et dans la partie droite la matrice inverse de M.

5 Compléter l'algorithme suivant :

```
n = .....
Pour k allant de 1 à n par pas de 1, faire
   Si le coefficient a_kk = 0, échanger la ligne L_k avec une ligne L_i telle que a_ik ≠ 0.
   Si ce n'est pas possible, la matrice est non inversible.
   Diviser L_k par ....
   Pour toutes les lignes L_i autres que L_k, faire
      Remplacer L_i par ......
   FinPour
FinPour
Effectuer les inversions contraires de lignes que celles dans la boucle précédente.
```

6 Programmer cet algorithme sans tenir compte de l'échange des lignes (on le testera avec la matrice A donnée ci-dessus qui ne nécessite pas de tels échanges).

Aide

Pour modifier la totalité d'une ligne, on écrira une boucle portant sur l'indice des colonnes.
Pour modifier toutes les lignes sauf une d'indice donné, on utilisera un test conditionnel portant sur les indices de ces lignes.

TP TICE 1 Inversion géométrique d'une matrice 2x2



Objectif :
- *Retravailler les ensembles de points du type $\vec{u}.\vec{v} = k$.*

Soit $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, une matrice 2x2, où a, b, c et d sont quatre réels.

Si on considère que M est constituée des deux vecteurs colonnes $\vec{u}$ et $\vec{v}$, on voudrait construire géométriquement les vecteurs colonnes $\vec{s}$ et $\vec{t}$ définissant M^{-1}, si elle existe.

1 Analyse de la situation

Considérons plutôt la matrice M comme étant composée des deux vecteurs lignes $\vec{u_1}$ et $\vec{v_1}$.

a. Écrire les coefficients du produit MM^{-1} comme des produits scalaires en utilisant les vecteurs $\vec{u_1}$, $\vec{v_1}$, $\vec{s}$ et $\vec{t}$.

b. Sachant que le produit $MM^{-1} = I_2$, en déduire les conditions que doit satisfaire le vecteur $\vec{s}$, puis le vecteur $\vec{t}$.

2 Première construction

Il s'agit donc, étant donné deux vecteurs, de déterminer un troisième vecteur orthogonal au premier et dont le produit scalaire avec le second est égal à 1.

a. Notons $\vec{u_1}$ le premier vecteur. Déterminer l'ensemble des vecteurs $\vec{s}$ tels que $\vec{u_1}.\vec{s} = 1$.

Aide

Commencer par déterminer le vecteur $\vec{s}$ colinéaire à $\vec{u_1}$ vérifiant cette relation.

b. Notons $\vec{v_1}$ le second vecteur. Déterminer l'ensemble des vecteurs $\vec{s}$ tels que $\vec{v_1}.\vec{s} = 0$.

c. Étant donnés les deux vecteurs $\vec{u_1}$ et $\vec{v_1}$, en déduire une construction géométrique du vecteur $\vec{s}$ tel que $\vec{u_1}.\vec{s} = 1$ et $\vec{v_1}.\vec{s} = 0$.

3 Réalisation de la figure

a. Réaliser la construction donnée en **2.c.** avec un logiciel de géométrique dynamique puis créer une macro-construction prenant en objets initiaux les deux vecteurs $\vec{u_1}$ et $\vec{v_1}$ et renvoyant l'objet final $\vec{s}$.

Aide

Dans CaRMetal, une macro accepte facilement un vecteur seul en tant qu'objet initial.
Dans GeoGebra 4, on préfèrera utiliser l'origine et l'extrémité du vecteur.

b. Créer deux vecteurs $\vec{u}$ et $\vec{v}$ représentant les vecteurs colonnes de la matrice M.

c. Quelles sont les coordonnées des vecteurs $\vec{u_1}$ et $\vec{v_1}$ représentant les vecteurs lignes de M en fonction de celles de $\vec{u}$ et $\vec{v}$? Créer ces vecteurs.

d. Appliquer la macro créée en **a.** aux vecteurs $\vec{u_1}$ et $\vec{v_1}$ pour créer le vecteur $\vec{s}$ et aux vecteurs ... et ... pour créer le vecteur $\vec{t}$.

4 Vérification

Faire calculer au logiciel le produit matriciel $\begin{pmatrix} \vec{u} & \vec{v} \end{pmatrix}\begin{pmatrix} \vec{s} & \vec{t} \end{pmatrix}$ et vérifier qu'on obtient bien la matrice I_2.

5 Application

On désire résoudre l'équation $\begin{pmatrix} 5 & 9 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$.

a. Créer les trois vecteurs colonnes que comporte ce système.
b. Utiliser la macro-construction et les opérations matricielles à votre disposition pour résoudre ce système.

TP TICE 2 Valeurs propres, vecteurs propres



Objectif :
- *Faire un lien entre matrices et géométrie.*

Soit M une matrice carrée et u un vecteur colonne non nul. On dit que u est un vecteur propre de M, s'il existe un réel λ tel que $Mu = \lambda u$. On dit alors que λ est valeur propre de M, associée au vecteur propre u.

1 On considère la matrice D suivante : $D = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

a. Représenter cette matrice dans un logiciel de géométrie dynamique, puis un vecteur u d'origine O. Créer le vecteur $v = Du$ dont on prendra aussi l'origine en O.

Aide

Dans CarMetal, on créera les vecteurs colonnes de D puis on utilisera la macro prévue pour le produit.
Dans GeoGebra 4, on écrira $D = \{\{-1,0\},\{0,1\}\}$ puis on tapera le produit dans la barre de saisie.

b. Si u est un vecteur propre de D, que cela signifie-t-il concernant u et v ?
c. En manipulant le vecteur u, vérifier qu'il existe deux directions pour lesquelles u et v satisfont la condition trouvée à la question **b.**
d. Pour chacune de ces directions, quel est le scalaire λ tel que $v = \lambda u$? (On pourra prendre le vecteur u à coordonnées entières pour faciliter les lectures graphiques). Quel est le rapport avec D ?
e. Conjecturer un vecteur propre associé à chaque valeur propre et vérifier algébriquement.

2 On considère maintenant la matrice M suivante : $M = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$.

a. Vérifier que -1 et 1 sont valeurs propres de M et déterminer deux vecteurs propres associés, que l'on notera u_{-1} et u_1.
b. Soit $P = (u_{-1}\ u_1)$ la matrice composée des deux vecteurs propres, en colonne. Calculer $P^{-1}MP$ et observer la matrice produit.

3 Étude théorique

a. Écrire l'équation $Mu = \lambda u$ sous la forme $Au = 0$, où A est une matrice dépendant de λ.
b. Expliquer pourquoi l'on doit rechercher les valeurs de λ pour lesquelles A n'est pas inversible.
c. Démontrer que cela revient à résoudre l'équation $(-1 - \lambda)(1 - \lambda) = 0$ puis résoudre cette équation.
d. Pour chaque valeur de λ, en déduire un vecteur u_λ correspondant.

4 Lorsque cela est possible, effectuer le même travail, pratique et théorique avec les matrices suivantes :

a. $M = \begin{pmatrix} 5 & -3 \\ 6 & -4 \end{pmatrix}$. **b.** $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. **c.** $M = \begin{pmatrix} -0{,}5 & 1{,}5 \\ 1 & -1 \end{pmatrix}$.

Maîtriser le cours

Notion de matrice

1 **Vrai ou faux**

a. Une matrice de taille $n \times p$ possède p lignes et n colonnes.

b. Le coefficient d'une matrice A noté a_{ij} se situe à la i-ème ligne et la j-ème colonne.

c. Une matrice nulle est nécessairement carrée.

d. Une matrice unité est nécessairement carrée.

e. Une matrice ligne est aussi appelée vecteur ligne.

2 **QCM**

1. Soit A une matrice telle que pour tous i et j, $a_{ij} = 0$ sauf lorsque $i = j$, alors :

a. A est la matrice nulle ;

b. A est la matrice unité.

2. La taille d'une matrice ligne est notée :

a. $1 \times p$, où $p \in \mathbb{Z}$; **b.** $1 \times p$, où $p \in \mathbb{N}$;

c. $p \times 1$, où $p \in \mathbb{Z}$; **d.** $p \times 1$, où $p \in \mathbb{N}$.

3. Même question avec une matrice colonne.

Opérations sur les matrices

3 **Vrai ou faux**

a. On peut additionner deux matrices de tailles différentes.

b. On peut multiplier deux matrices de tailles différentes.

c. On peut multiplier deux matrices de n'importe quelles tailles.

4 **QCM**

1. Lorsqu'on peut additionner deux matrices, la matrice somme :

a. est encore de même taille ;

b. possède une taille différente.

2. Le produit d'une matrice ligne par une matrice colonne est :

a. une matrice de taille 1×1 ;

c. ne peut pas se calculer ;

b. un réel.

3. Pour que le produit AB soit calculable, il faut que :

a. le nombre de colonnes de A soit égal au nombre de colonnes de B ;

b. le nombre de colonnes de A soit égal au nombre de lignes de B ;

c. le nombre de lignes de A soit égal au nombre de colonnes de B ;

d. le nombre de lignes de A soit égal au nombre de lignes de B.

Logique

5 **Vrai ou faux**

a. Pour que le produit AB soit une matrice carrée, il faut que A et B soient des matrices carrées de même taille.

b. Pour que le produit AB soit une matrice carrée, il suffit que A et B soient des matrices carrées de même taille.

6 **QCM**

Le produit matriciel AB s'effectue en multipliant :

a. chaque ligne de A par chaque colonne de B ;

b. chaque colonne de A par chaque ligne de B ;

c. chaque colonne de A par chaque colonne de B.

Matrices inversibles

7 **Vrai ou faux**

a. L'inverse d'une matrice s'obtient en changeant les signes de tous les coefficients.

b. Toutes les matrices possèdent des inverses.

c. Une matrice et son inverse sont de même taille.

d. Il existe un seul inverse pour une matrice donnée.

8 **QCM**

Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. A est inversible si, et seulement si :

a. $ac - bd \neq 0$;

b. $ad - bc \neq 0$;

c. $ab - cd \neq 0$.

Logique

9 **Vrai ou faux**

a. Pour qu'une matrice admette un inverse, il suffit qu'elle soit carrée.

b. Pour qu'une matrice admette un inverse, il faut qu'elle soit carrée.

c. a. et b.

10 **QCM**

On considère un système linéaire de n équations à p inconnues.

1. La matrice associée à un tel système est de taille :

a. nxp ;

b. pxn.

2. Le vecteur représentant les inconnues d'un tel système est :

a. un vecteur ligne comportant p colonnes ;

b. un vecteur colonne comportant p lignes ;

c. un vecteur ligne comportant n colonnes ;

d. un vecteur colonne comportant n lignes.

Appliquer les capacités attendues

Notion de matrice

Manipuler une matrice dans une calculatrice ou un logiciel [savoir-faire 1 p. 111]

Pour les exercices **11** et **12**, entrer les matrices données dans une calculatrice ou dans un logiciel en utilisant la syntaxe appropriée.

11 **a.** $A = \begin{pmatrix} 1 & -2 & 3 & -4 \end{pmatrix}$.

b. $B = \begin{pmatrix} 4 \\ -5 \\ 6 \end{pmatrix}$.

c. $C = \begin{pmatrix} 12 & -15 \\ 7 & 2 \\ -1 & 4 \end{pmatrix}$.

d. $D = \begin{pmatrix} 1 & 2 & 3 & 4 \\ -5 & -6 & -7 & 8 \end{pmatrix}$.

12 **a.** $A = \begin{pmatrix} -1 & 2 & -3 \\ 10 & -11 & 12 \\ -7 & 8 & -9 \end{pmatrix}$.

b. $B = \begin{pmatrix} 10 & -11 & 12 & -13 & 14 \end{pmatrix}$.

c. $C = \begin{pmatrix} -7 \\ 8 \end{pmatrix}$.

d. $D = \begin{pmatrix} a & a^2 & a^3 \\ b & \frac{1}{b} & \frac{1}{b^2} \end{pmatrix}$.

13 Pour rentrer la matrice $M = \begin{pmatrix} 1 & -6 & 0 \\ 0 & 5 & -2 \end{pmatrix}$, un élève a écrit ceci dans le logiciel Maxima :

M : matrix([1,0],[−6,5],[0,−2]) ;

La matrice M ainsi définie est-elle correcte ? Si non, proposer une correction.

14 Les syntaxes ci-dessous sont issues de Maxima, XCas ou JavaScript.

1. Dans tous les cas, dire si elles sont correctes.

2. Si oui, donner les tailles des matrices ainsi définies.

a. A : matrix([4,6],[4,−2,−1]) (Maxima) ;

b. B = [[1,−2,3],[9,−8,7]] (JavaScript) ;

c. C := matrix([1];[−2];[5]) (XCas) ;

d. D := matrix([1,1],[−2,2],[3,3]) (XCas) ;

e. E = [[10,11,12]] (JavaScript).

15 On considère la matrice A suivante :

$$A = \begin{pmatrix} 1 & 17 & 3 & 0{,}2 \\ -21 & 7 & -6 & 0 \\ 12 & 10 & 4 & -1 \end{pmatrix}.$$

1. Quelles sont les réponses affichées par les calculatrices ou logiciels pour chacune des syntaxes suivantes :

a. A[1][1] (Maxima) ;

b. A[2,1] (XCas) ;

c. Mat A[3,4] (CASIO) ;

d. [A](2,3) (TI) ;

e. A[1][1] (JavaScript) ;

f. A[2] (Maxima) ;

g. Mat->List(Mat A,2) (CASIO) ;

h. A[3] (JavaScript) ;

i. A[0] (XCas) ;

j. Matr>liste([A],2,L_1):L_1 (TI) ;

k. col(A,2) (Maxima) ;

l. col(A,2) (XCas).

2. Que devient la matrice A si l'on exécute les instructions suivantes :

a. A[1][4]:2 (Maxima) ;

b. A[1,1]:=900 (XCas) ;

c. 6->Mat A[2,3] (CASIO) ;

d. 45->[A](2,4) (TI) ;

e. A[0][2]=100 (JavaScript) ;

f. A[1]:[1,1,1,1] (Maxima) ;

g. A[1]:=[1,1,1,1] (XCas) ;

h. List->Mat({1,2,3})->Mat A (CASIO) ;

i. A[1]=[1,1,1,1,1] (JavaScript) ;

j. Liste>matr({1,2,3},[A]) (TI).

16 On considère la même matrice A qu'à l'exercice 15.

1. Que permettent de connaître les syntaxes Maxima ou XCas suivantes :

a. « length(A) » ?

b. « length(A[1]) » ?

c. Donner au moins une autre possibilité pour obtenir le même résultat qu'à la question **b.**

2. *Voici une syntaxe CASIO : « Dim Mat A »*

a. Que permet-elle de savoir ?

b. En stockant ce résultat dans une liste, écrire une syntaxe permettant de récupérer uniquement le nombre de lignes de la matrice.

c. *Même question avec le nombre de colonnes.*

3. Mêmes question avec la syntaxe TI suivante : « dim([A]) »

TICE Parcourir algorithmiquement les coefficients d'une matrice [savoir-faire 2 p. 113]

17 Écrire un algorithme permettant de définir une matrice de taille 6×3 dont les coefficients sont égaux à la somme de leur position dans la matrice.

18 Dans une matrice carrée de dimension n, de coefficients a_{ij}, quels sont les coefficients vérifiant :

a. $i = j$; **b.** $i = j - 1$;

c. $i = j + 1$; **d.** $i + j = n$;

e. $i + j = n + 1$.

19 On considère l'algorithme suivant :

```
Saisir(n) ;
A est une matrice carrée de taille n ;
Pour i = 1 à n faire
   Pour j = 1 à n faire
      Si i+j == n, alors
         Aij = 1 ;
      Sinon
         Aij = 0 ;
      FinSi
   FinPour
FinPour
```

a. Faire tourner cet algorithme en prenant $n = 4$ et en déduire le type de matrice défini par cet algorithme.

b. Réécrire cet algorithme pour un langage de programmation ou un logiciel pour lequel la numérotation commence à 0.

20 Écrire un algorithme permettant de définir une matrice carrée de taille 6 dont tous les coefficients sont nuls sauf ceux situés sur les lignes juste au-dessus et juste en dessous de la diagonale, qui valent 1.

21 Écrire un algorithme qui reçoit en paramètre une matrice et qui permet de dire si c'est une matrice carrée.

Aide

On pourra stocker dans deux variables le nombre de lignes et de colonnes. Voir exercice 16.

22 Écrire un algorithme qui reçoit en paramètre une matrice et qui permet de dire si c'est une matrice unité.

Aide

On pourra d'abord tester si la matrice est carrée.

Opérations sur les matrices

Additionner des matrices [savoir-faire 3 p. 113]

Pour les exercices de 23 à 25, effectuer la somme des matrices A et B, lorsque cela est possible.

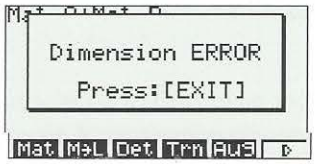
23 $A = \begin{pmatrix} -2 & 3 \\ 5 & -7 \end{pmatrix}$, $B = \begin{pmatrix} 3 & -3 \\ -5 & 8 \end{pmatrix}$

24 $A = \begin{pmatrix} 1 & -1 & 1 \\ -2 & 2 & -2 \end{pmatrix}$, $B = \begin{pmatrix} -2 & 2 & -2 \\ 1 & -1 & 1 \end{pmatrix}$.

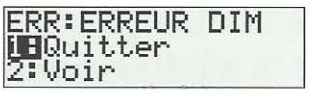
25 $A = \begin{pmatrix} 4 \\ 6 \\ 8 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 5 & 7 \end{pmatrix}$.

26 En voulant additionner deux matrices A et B, on a obtenu le résultat suivant :

Avec une CASIO :



Avec une TI :



Avec Maxima :

```
(%i3) A+B;
`fullmap' found arguments with incompatible structure.
-- an error. To debug this try: debugmode(true);
```

1. Expliquer ces captures d'écran.

2. **a.** Reproduire cette situation avec les calculatrices ou logiciels en choisissant correctement deux matrices A et B.

b. Faire de même dans XCas. Que se passe-t-il ? Interpréter.

Algorithmique

27 Écrire un algorithme permettant d'effectuer la somme de deux matrices A et B données en paramètres et qui affiche la matrice somme.

Aide

L'algorithme devra d'abord tester que la somme est possible et renvoyer un message d'erreur sinon.

28 On considère les matrices :

$$A = \begin{pmatrix} 7 & -10 \\ -5 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix}.$$

Calculer les valeurs des réels x et y tels que :

$$xA + yB = \begin{pmatrix} 11 & -50 \\ -20 & -7 \end{pmatrix}.$$

Effectuer un produit de matrices [savoir-faire 4 p. 115]

Pour les exercices 29 à 31, calculer le produit AB lorsque cela est possible et préciser la taille de la matrice produit.

29 **a.** $A = \begin{pmatrix} 3 & -7 \end{pmatrix}$ et $B = \begin{pmatrix} -7 \\ 3 \end{pmatrix}$.

b. $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 10 & -11 & 12 \end{pmatrix}$.

30 **a.** $A = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ et $B = \begin{pmatrix} \frac{1}{a} & \frac{1}{b} & \frac{1}{c} \end{pmatrix}$.

b. $A = \begin{pmatrix} a & b \\ 3 & 4 \\ 5 & c \end{pmatrix}$ et $B = \begin{pmatrix} \frac{1}{a} & \frac{1}{b} \\ 2 & -1 \end{pmatrix}$.

31 **a.** $A = \begin{pmatrix} -1 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 \\ 2 \\ a \end{pmatrix}$.

b. $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ et $B = \begin{pmatrix} -5 \\ -3 \end{pmatrix}$.

32 Dans chacun des cas suivants, calculer la ou les valeur(s) du coefficient réel a pour que l'égalité matricielle soit vraie.

a. $\begin{pmatrix} 0 & a \\ 3 & -4 \end{pmatrix} \times \begin{pmatrix} a^2 & -5 & 6 \\ -a & 0 & 0 \end{pmatrix} = \begin{pmatrix} -4 & 0 & 0 \\ 20 & -15 & 18 \end{pmatrix}$.

b. $\begin{pmatrix} a & 2 & -5 \end{pmatrix} \times \begin{pmatrix} -a & a \\ 3 & a+1 \\ 5 & 6 \end{pmatrix} = \begin{pmatrix} -119 & 52 \end{pmatrix}$.

33 On considère la matrice $A = \begin{pmatrix} 3 & 4 \\ -5 & x \end{pmatrix}$.

a. Calculer A^2.

b. Déterminer la valeur de x pour que $A^2 = \begin{pmatrix} -11 & 12 \\ -15 & -20 \end{pmatrix}$.

34 On considère les matrices :

$$A = \begin{pmatrix} 1 & -2 \\ y & 6 \\ 3 & x \end{pmatrix} \text{ et } B = \begin{pmatrix} y & 4 \\ 1 & x \end{pmatrix}.$$

Sans expliciter entièrement le produit AB, calculer les valeurs des réels x et y tels que : $AB = \begin{pmatrix} -1 & -4 \\ 7 & 28 \\ 7 & 28 \end{pmatrix}$.

35 Dans chacun des cas suivants, A est une matrice de taille $n \times p$ (on peut avoir $n = p$), et I est une matrice identité.

1. Préciser les tailles possibles des matrices B et I.

2. Développer les expressions données.

a. $A(B + I)$;

b. $(B + A)A^{-1}$;

c. $AB(B^{-1}A^{-1} - AB)$;

d. $B(I - A)$.

36 Factoriser les expressions suivantes :

a. $(A + I)^{-1}A + (A + I)^{-1}$;

b. $(A + I)^{-1} + A(A + I)^{-1}$;

c. $(A + I)^{-1} + A(I + A^{-1})$.

Matrices inversibles

Déterminer l'inverse d'une matrice

[savoir-faire 5 p. 117]

Pour les exercices de 37 à 40, déterminer l'inverse de la matrice A donnée et vérifier le résultat à l'aide d'un logiciel ou d'une calculatrice.

37 $A = \begin{pmatrix} 3 & 4 \\ -5 & 2 \end{pmatrix}$.

38 $A = \begin{pmatrix} 11 & 3 \\ 7 & 2 \end{pmatrix}$.

39 $A = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 2 & 0 \\ 3 & 0 & 1 \end{pmatrix}$.

40 $A = \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}$, où x est un réel quelconque.

41 Les matrices suivantes sont-elles inverses l'une de l'autre ?

a. $A = \begin{pmatrix} 6 & 5 \\ 7 & 6 \end{pmatrix}$ et $B = \begin{pmatrix} -5 & 6 \\ 6 & -7 \end{pmatrix}$.

b. $A = \begin{pmatrix} 155 & -13 \\ 12 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 13 \\ -12 & 155 \end{pmatrix}$.

c. $A = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$ et elle-même.

42 On considère les matrices suivantes :

$$M = \begin{pmatrix} \frac{3}{5} & 0 & -\frac{1}{5} \\ -\frac{3}{5} & \frac{1}{2} & -\frac{7}{10} \\ 0 & -\frac{1}{2} & \frac{9}{10} \end{pmatrix} \text{ et } N = \begin{pmatrix} \approx & \approx & \approx \\ -0{,}6 & 0{,}5 & -0{,}7 \\ 0 & -0{,}5 & 0{,}9 \end{pmatrix}.$$

1. Quel est le lien entre M et N ?

2. Voici une capture d'écran faite sous Maxima.

```
(%i3) N:float(M)$

(%i4) invert(M);
expt: undefined: 0 to a negative exponent.
 -- an error. To debug this try: debugmode(true);

(%i5) invert(N);
                [ 4.8 10^15   4.8 10^15   4.8 10^15  ]
                [                                    ]
(%o5)           [ 2.59 10^16  2.59 10^16  2.59 10^16 ]
                [                                    ]
                [ 1.44 10^16  1.44 10^16  1.44 10^16 ]
```

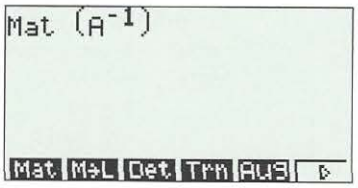
a. Que signifie float(M) ?

b. Commenter les résultats obtenus.

3. a. Essayer la syntaxe suivante « invert(ratsimp(N)); » et commenter le résultat obtenu.
b. Que signifie la commande « ratsimp » ?

4. Effectuer les mêmes manipulations avec le logiciel XCas mais en utilisant les commandes « evalf », « inv » et « float2rational ».

43 Commenter la capture d'écran suivante, provenant d'une calculatrice CASIO GRAPH 35+ :



Résoudre un système linéaire

[savoir-faire 6 p. 117]

Pour les exercices 44 à 49 :
a. Écrire le système sous la forme matricielle $AX = Y$.
b. Résoudre le système en utilisant l'inverse de la matrice A, lorsque cela est possible.

44 $\begin{cases} -4x + 3y = 2 \\ -x + y = 5 \end{cases}$.

45 $\begin{cases} 3x - 2y + z = 0 \\ -x - y = -1 \end{cases}$.

46 $\begin{cases} 2x + y = 7 \\ -y + z = -4 \\ x + z = 1 \end{cases}$.

47 $\begin{cases} x + y = z - 3 \\ 3x + y = x - z + 5 \end{cases}$.

48 $\begin{cases} 4x - 2y + z = 7 \\ x - y + z = 9 \\ -x + 5y + 2z = -10 \end{cases}$.

49 $\begin{cases} 7x - 2y = 3 \\ -7x + 2y = -1 \end{cases}$.

50 Voici une capture d'écran provenant du logiciel Maxima, montrant la résolution d'un système linéaire.

```
(%i1) linsolve([-x=-2*y+12, 7*x=3*y], [x,y]);
(%o1) [x=36/11, y=84/11]
```

a. Écrire ce système et donner sa matrice associée.
b. Vérifier le résultat par un calcul d'inverse de matrice.

51 Voici une capture d'écran provenant du logiciel Maxima, montrant la résolution d'un système linéaire.

```
(%i1) linsolve([2*x+5*y-8*z=24, -3*x+y-5*z=-2, x+y-z=6], [x,y,z]);
solve: dependent equations eliminated: (3)
(%o1) [x=2-%r1, y=2 %r1+4, z=%r1]
```

a. Donner la matrice associée à ce système. Est-elle inversible ?
b. Expliquer la réponse donnée par le logiciel.

52 Un élève a voulu connaître la forme générale des solutions du système linéaire suivant :

$$\begin{cases} ax + by = e \\ cx + dy = f \end{cases}.$$

Voici ce qu'il a entré dans Maxima :

```
(%i1) linsolve([a*x+b*y=e, c*x+d*y=f], [a,b]);
(%o1) []
```

a. Pourquoi le logiciel ne répond-il rien ?
b. Proposer une modification.

53 Voici une capture d'écran provenant du logiciel Maxima montrant la résolution d'un système linéaire.

```
(%i1) linsolve([2*x+3*y=4, -6*x-9*y=12], [x,y]);
(%o1) []
```

a. Pourquoi le logiciel ne répond-il rien ?
b. Proposer une modification, et une seule, pour que le logiciel puisse répondre quelque chose. Vérifier.

54 Voici une capture d'écran provenant du logiciel Maxima montrant la résolution d'un système :

```
(%i1) linsolve([x^2+y^2=13, x+y=-1], [x,y]);
(%o1) []
```

a. Pourquoi le logiciel ne répond-il rien ?
b. Dans le menu « Équations », chercher la commande permettant de résoudre un tel système (et le résoudre).



Manipulations de matrices

55 **Une question de taille**

On considère une matrice A de taille $n \times p$.

1. Soit N une matrice telle que le produit NA soit calculable. En déduire l'une des dimensions de N.
2. Soit M une matrice telle que le produit AM soit calculable. En déduire l'une des dimensions de M.
3. **a.** Soit P une matrice telle que les produits PA et AP soient calculables. Quelle est la taille de P. En déduire la taille de PA et AP.

b. On souhaite maintenant que $AP = PA$. Que peut-on en déduire sur A ?

c. Expliquer pourquoi on ne peut pas définir l'inverse d'une matrice non carrée.

56 **Identité remarquable ?**

On considère les matrices A et B, carrées de taille 2 :

$$A = \begin{pmatrix} 1 & 0 \\ -3 & 2 \end{pmatrix} \text{ et } B = \begin{pmatrix} 4 & -2 \\ 0 & 1 \end{pmatrix}.$$

1. Calculer puis comparer $(A+B)^2$ et $A^2 + 2AB + B^2$.
2. **a.** Développer $(A+B)^2$.

b. En déduire une condition nécessaire et suffisante pour qu'il y ait égalité, dans le cas général, entre les deux expressions données à la question 1.

c. Vérifier que les matrices A et B suivantes respectent bien cette condition et comparer à nouveau les deux expressions de la question **1.**

$$A = \begin{pmatrix} 1 & 0 \\ -3 & 2 \end{pmatrix}; \quad B = \begin{pmatrix} -1 & 0 \\ 15 & -6 \end{pmatrix}.$$

Logique

57 **Équation produit**

Soient A et B les deux matrices suivantes :

$$A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \quad B = \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}.$$

1. Calculer le produit AB.
2. On considère les deux propositions suivantes :

P : « l'un des facteurs est nul »

Q : « un produit de facteur est nul »

Dans $\mathbb{R}$, P est-elle :

a. nécessaire à Q ? ($Q \Rightarrow P$)

b. suffisante pour Q ? ($P \Rightarrow Q$)

c. équivalente à Q ? ($P \Leftrightarrow Q$)

3. Même question dans l'ensemble des matrices.

Algorithmique

58 On considère l'algorithme suivant permettant, pour deux matrices A et B données en paramètres et dans cet ordre, de calculer le produit AB, lorsque celui-ci est possible.

1. Compléter les lignes 3, 4 et 5 permettant de tester si le produit AB est possible ou non.
2. Compléter les lignes 8, 9 et 10 permettant de donner la taille de la matrice $C = AB$.

```
Saisir(A) ;
Saisir(B) ;
//à compléter
//à compléter
Si.....alors
   Afficher(« Erreur de dimension ») ;
Sinon
   n = nombre de.....de A ;
   q = nombre de.....de B ;
   C est une matrice de taille..... ;
   Pour i = 1 à n faire
      Pour j = 1 à q faire
         //calcul du coefficient c_ij
      FinPour
   FinPour
FinSi
```

3. **a.** Expliciter la formule permettant de calculer la valeur du coefficient c_{ij} en fonction des coefficients a_{ik} et b_{kj}.

b. Écrire une boucle permettant de calculer ce produit et le stocker dans la variable c_{ij}.

4. Complexité de l'algorithme

a. Combien de multiplications sont nécessaires au calcul de c_{ij} ? Combien d'additions ?

b. En déduire le nombre total d'opérations nécessaires au calcul de c_{ij}.

c. En déduire le nombre d'opérations nécessaires pour effecteur le produit AB.

d. Expliciter ce résultat lorsque les deux matrices sont carrées, de taille n.

59 **Inverse d'un produit**

Soient A et B deux matrices inversibles.

Démontrer que $(AB)^{-1} = B^{-1}A^{-1}$.

60 **Commutant d'une matrice de taille 2**

Soit A une matrice carrée de taille 2. On appelle commutant de A l'ensemble des matrices B de taille 2 telles que $AB = BA$.

Partie A

On veut montrer que si B est un polynôme de la matrice A, alors $AB = BA$.

1. Soit $B = A^k$, où k est un entier naturel. Démontrer par récurrence que pour tout entier naturel k : $AB = BA$.
2. Soit f une fonction polynômiale de degré n, $n \in \mathbb{N}$, c'est-à-dire donné par l'expression :

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

où les a_i sont des réels, $a_n \neq 0$.

On pose $B = f(A)$. Par une récurrence sur le degré de f, déduire de la question précédente que $AB = BA$.

Partie B

On considère la matrice diagonale suivante :

$$A = \begin{pmatrix} 3 & 0 \\ 0 & -7 \end{pmatrix}.$$

Le but est de démontrer la réciproque de la propriété énoncée dans la partie A.

1. Soit B une matrice telle que $AB = BA$. On note $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, où les b_{ij} sont des réels. Démontrer que $b_{12} = b_{21} = 0$.

2. **a.** Démontrer qu'il existe une fonction affine $f : x \mapsto mx + p$ telle que $f(3) = b_{11}$ et $f(-7) = b_{22}$.

b. En déduire que $B = f(A)$.

3. Reprendre l'exercice en généralisant la forme de la matrice A et donner une condition nécessaire sur les coefficients de A pour que la propriété soit vérifiée.

Partie C

On s'intéresse maintenant aux matrices A pour lesquelles il existe un matrice P inversible telles que : $P^{-1}AP = D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$, où d_1 et d_2 sont deux réels distincts. On veut démontrer la même propriété.

1. **a.** Soit B une matrice telle que $AB = BA$. En multipliant les deux membres de cette égalité, à gauche par P^{-1} et à droite par P, montrer que l'on obtient $DC - CD = 0$, avec $C = P^{-1}BP$.

b. On note $C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$, où les c_{ij} sont des réels.

En utilisant le résultat de la question **a.** démontrer que $c_{12} = c_{21} = 0$.

c. Démontrer qu'il existe une fonction affine $f : x \mapsto mx + p$ telle que $f(d_1) = c_{11}$ et $f(d_2) = c_{22}$.

d. En déduire que $C = f(D)$ puis que $B = f(A)$.

2. Application à un cas concret.

Soit $A = \begin{pmatrix} -102 & -140 \\ 75 & 103 \end{pmatrix}$.

a. À l'aide de la matrice $P = \begin{pmatrix} 7 & -4 \\ -5 & 3 \end{pmatrix}$, vérifier que A satisfait bien la condition donnée dans l'exercice.

b. Donner une matrice B commutant avec A.

Algorithmique

61 On considère l'algorithme suivant, écrit dans le module JavaScript de CarMetal :

```
1  A = [[1,2,3,4],[-5,-6,-7,-8],[9,10,11,12]];
2  n = A.length;
3  p = A[0].length;
4
5  for(i=0; i<n; i++){
6      a = A[i][0];
7      for(j=1; j<p; j++){
8          A[i][j-1] = A[i][j];
9      }
10     A[i][p-1] = a;
11     Println(A[i]);
12 }
```

1. Traduire cet algorithme en langage naturel.

2. **a.** Rappeler pourquoi les valeurs initiale et finale dans la boucle portant sur la variable i sont 0 et $n - 1$ et non pas de 1 et n.

b. Pourquoi la boucle portant sur la variable j commence-t-elle à 1 ?

3. **a.** Tester cet algorithme sur la matrice A donnée dans le code :

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ -5 & -6 & -7 & -8 \\ 9 & 10 & 11 & 12 \end{pmatrix}.$$

Que fait cet algorithme ?

b. Quel est le rôle de l'instruction « a = A[i][0] ; » à la ligne 7 ?

4. Adapter cet algorithme pour qu'il effectue l'opération contraire.

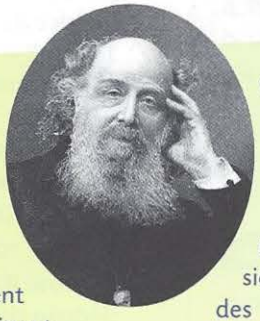
5. Adapter cet algorithme pour qu'il effectue le même type de transformation, mais sur les lignes.

62 Résoudre le système suivant en utilisant une matrice :

$$\begin{cases} 2x + 7y = 15 \\ -x + y = -7 \end{cases}.$$

Un peu d'histoire...

Notion de matrice



La notion de matrice est née par le biais de l'étude des coefficients de systèmes d'équations linéaires.

Leibniz, en 1693 et Cramer, en 1750 utilisent une notion étroitement liée, celle de déterminant, pour résoudre les systèmes linéaires. La première utilisation implicite de la notion de matrice a été faite par Joseph Louis Lagrange, qui désirait caractériser les extrema de fonctions de plusieurs variables. Dans la théorie actuelle, les matrices explicitement utilisées se nomment matrices définies positives ou négatives.

Gauss développa ensuite, vers 1800, une méthode permettant de résoudre les systèmes linéaires par combinaisons (linéaires) et utilisa une notation en tableau, proche de l'actuelle. Toutefois, même si le nom de Gauss est aujourd'hui associé à cette technique, des manuscrits chinois datant de plusieurs siècles auparavant expliquaient comment résoudre des systèmes 3x3. La première apparition de cette méthode a été publiée par Wilhelm Jordan (méthode de Gauss-Jordan, voir TP 2 p. 119)

Le terme de matrice, du latin "matrix" (reproductrice, femelle) a été introduit par James Joseph Sylvester en 1850 pour désigner un tableau de nombres, mais c'est avec les publications d'Arthur Cayley en 1855 que la notion prend tout son sens.

63 **Matrices de permutations de colonnes**

On reprend la matrice A de l'exercice 61.

On cherche s'il existe une matrice P qui puisse permuter vers la gauche les colonnes de A, c'est-à-dire telle que :

$$AP = \begin{pmatrix} 2 & 3 & 4 & 1 \\ -6 & -7 & -8 & -5 \\ 10 & 11 & 12 & 9 \end{pmatrix}.$$

1. Quelle doit être la taille de P ?
2. Recherche des coefficients de P.

a. Remplir la première colonne de P par des 0 ou des 1 de telle sorte que le résultat du produit de chaque ligne de A par la première colonne de P soit égal au deuxième coefficient de chaque ligne de A.

b. Faire de même pour les trois autres colonnes de P.

c. Vérifier le résultat en effectuant le produit AP à l'aide d'un logiciel ou d'une calculatrice.

3. **a.** Calculer P^2. En regardant la matrice obtenue, prédire le résultat de AP^2. Vérifier par le calcul.

b. Prédire le résultat de P^3. Vérifier par un calcul.

c. Même question pour P^4.

64 **Inverse d'une matrice 2×2**

Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice carrée de taille 2.

1. Démontrer que $(a + d)A - A^2 = (ad - bc)I_2$.
2. **a.** Factoriser le membre de gauche par A.

b. À quelle condition la matrice A admet-elle un inverse ?

c. Déterminer cet inverse.

65 On considère la matrice A suivante, dont on désire déterminer l'inverse :

$$A = \begin{pmatrix} 1 & -a & 0 & 0 \\ 0 & 1 & -a & 0 \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

a. Déterminer la matrice J telle que $A = I_4 - aJ$

b. Calculer J^2, J^3 et J^4 et en déduire que l'on peut écrire $I_4 = I_4 - a^4J^4$.

c. Factoriser cette expression par $I_4 - aJ$ et en déduire l'expression de A^{-1} en fonction de J, puis en fonction de a.

d. Vérifier ce résultat à l'aide d'un logiciel de calcul formel.

66 On considère la matrice A suivante, dont on désire déterminer l'inverse :

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 \end{pmatrix}.$$

a. Calculer (ou faire calculer) A^2 et A^3.

b. Déterminer les coefficients a et b tels que $A^3 = aA + bI_4$.

c. Après avoir factorisé cette égalité, en déduire l'inverse de A.

67 Soient A et B deux matrices carrées de tailles n telles que $AB = A + B$. On souhaite démontrer que $AB = BA$ (on dit que A et B commutent).

a. Développer $(I_n - A)(I_n - B)$ et en déduire, par des considérations d'inverses, que $(I_n - B)(I_n - A) = I_n$.

b. Développer alors le produit $(I_n - B)(I_n - A)$ et en déduire que $AB = BA$.

68 On considère les matrices P et Q suivantes :

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}; \quad Q = \frac{1}{4}(I_3 + P).$$

a. Calculer P^2, QP et PQ en fonction de P.

b. Calculer $(4I_3 - P)Q$ et $Q(4I_3 - P)$. Que peut-on en conclure ?

69 On désire trouver toutes les matrices A, carrées de taille 2 telles que $A^2 = A$. Soit A une telle matrice :

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

a. Calculer A^2 et démontrer que résoudre le problème donné revient à résoudre le système (S) suivant :

$$(S) \Leftrightarrow \begin{cases} a^2 + bc = a \\ b(a + d) = b \\ c(a + d) = c \\ d^2 + bc = d \end{cases}$$

b. Résoudre ce système en considérant deux cas : $b = 0$ ou $b \neq 0$.

Aide

Dans le cas $b = 0$, on considèrera quatre autres cas selon les valeurs de a et d.

Cryptage

70 **Cryptage de Hill**

Voici le principe pour un texte composé uniquement de lettres :

- on code chaque lettre par son rang dans l'alphabet, de 0 pour A, jusqu'à 25 pour Z ;
- on regroupe ces nombres par blocs de k caractères pour former des vecteurs lignes X à k colonnes (on prendra ici $k = 2$). S'il manque des nombres pour former le dernier vecteur, on complète arbitrairement ;
- on crypte chaque vecteur X à l'aide d'une matrice de codage A de taille k, modulo 26, et on obtient le vecteur ligne crypté $Y \equiv XA\ [26]$;
- le décodage s'effectue en utilisant la matrice inverse de A, modulo 26.

Aide

Une matrice modulo 26 est une matrice obtenue en réduisant modulo 26 tous les coefficients.

1. **a.** Pourquoi crypte-t-on modulo 26 ?
b. Quelle égalité, modulo 26, permet de décoder un vecteur ligne ?

2. Un exemple
a. On considère dans cette question le mot à crypter « CRYPTAGE ». Vérifier que les vecteurs X sont :
$X_1 = (2\ 17)$; $X_2 = (24\ 15)$; $X_3 = (19\ 0)$ et $X_4 = (6\ 4)$
b. On considère la matrice de cryptage $A = \begin{pmatrix} 3 & 2 \\ 7 & 11 \end{pmatrix}$.
Vérifier que les vecteurs Y modulo 26 sont :
$Y_1 = (21\ 9)$; $Y_2 = (-5\ 5)$; $Y_3 = (5\ 12)$ et $Y_4 = (20\ 4)$
et que le message crypté est donc : VJVFFMUE
c. Vérifier que la matrice $B = \begin{pmatrix} 17 & 4 \\ 1 & 7 \end{pmatrix}$ est bien l'inverse de A, modulo 26.
d. Vérifier que le décryptage fonctionne correctement.

3. On s'intéresse à la possibilité de décrypter un message, c'est-à-dire à l'existence d'une matrice inverse modulo 26. Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ une matrice carrée de taille 2, où a, b c, et d sont quatre entiers relatifs.
a. Entre quelles valeurs peut-on supposer les quatre entiers a, b, c et d ? Pourquoi ?
b. Rappeler la condition nécessaire et suffisante sur un nombre n et 26 pour laquelle on a $nu + 26v = 1$, où u et v sont deux entiers non nuls.
c. En déduire que sous cette condition, n admet un inverse modulo 26, et réciproquement, c'est-à-dire un nombre m tel que $nm \equiv mn \equiv 1$ [26]. A quoi m est-il égal dans notre cas ?
d. D'après la formule donnant l'inverse de A lorsqu'on la considère à coefficients entiers, déduire de ce qui précède une condition nécessaire et suffisante pour que A admette un inverse modulo 26.
e. Démontrer que si $a = 3$, $b = 18$, $c = 7$ et $d = 10$, alors A n'admet pas d'inverse modulo 26.
f. Démontrer que si $a = 12$, $b = 5$, $c = 9$ et $d = 21$, l'inverse de A modulo 26 est $A^{-1} = \begin{pmatrix} 5 & 9 \\ 5 & 14 \end{pmatrix}$.

4. Vérifier les résultats des questions **3.f.** et **3.g.** à l'aide d'un logiciel.

Aide

Dans Maxima, on définit le module depuis le menu Simplifier/Calcul modulaire et tous les calculs devront s'effectuer à l'aide de la commande « rat(...) »
Dans Xcas, on écrit le calcul souhaité suivi de « mod n » où n représente le module souhaité.

5. *Cryptage et décryptage d'un message*
Crypter un message (pas plus de 15 caractères) et demander à un camarade de le décrypter, après lui avoir fourni la matrice A.
On pourra s'aider d'un logiciel pour effectuer les calculs plus rapidement.

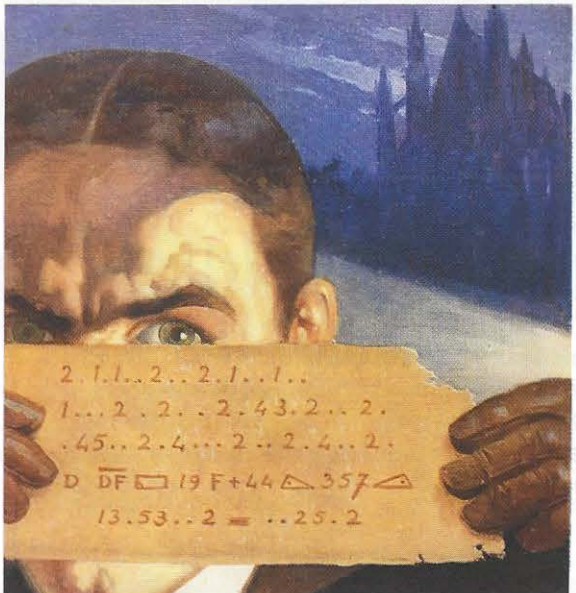
6. On s'intéresse dans cette question à la manière de construire une matrice A, inversible modulo 26.
a. Expliquer pourquoi l'on ne peut pas avoir a et b, ou a et c divisibles par 2 ou 13.
b. a étant un entier fixé, expliquer comment choisir b et c.

7. *Cryptanalyse*
Un espion a réussi à voler une machine de chiffrement qui utilise le principe de cryptage décrit dans cet exercice. La matrice de cryptage est inaccessible, mais on peut tout de même utiliser la machine.
a. Le commandement demande à l'espion de chiffrer « AB » et « YZ » et de retourner les résultats donnés par la machine. L'espion, ayant suivi dans sa jeunesse le cours de TS – spé maths, affirme alors, au péril de sa carrière, que ce choix n'est pas très judicieux. Expliquer pourquoi.

Aide

On pourra écrire sous forme matricielle les deux systèmes obtenus et vérifier que la matrice correspondant aux deux systèmes n'admet pas d'inverse modulo 26.

b. Le commandement, un peu agacé, demande à l'espion, puisqu'il est si malin, de proposer un meilleur choix. L'espion propose alors de chiffrer « BC » à la place de « AB » et de garder « YZ ». La machine donne alors les résultats « HI » et « MT ». Expliquer pourquoi cela va permettre de casser le code et donner la matrice de cryptage.
c. Dans le feu de l'action, l'espion a manqué de discernement car les deux systèmes à résoudre ne sont pas les plus simples possibles. En gardant le choix « AB », proposer un autre choix permettant de casser le code et vérifier que l'on obtient bien la même matrice qu'en **b.**



Graphes et matrices

71 Bonus – Malus

On considère le système de bonus/malus simplifié suivant :

- quatre classes de tarifications, de 1 (meilleur bonus) à 4 (pire malus) ;
- si l'assuré n'a pas de sinistre pendant une année, il passe de la classe i à la classe $\min(1, i-1)$;
- si l'assurée a au moins un sinistre responsable pendant l'année, il passe de la classe i à la classe $\max(4, i+1)$;

On note X la valeur de la classe actuelle et Y la valeur de la classe de l'année à venir.

1. On suppose que la probabilité de ne pas avoir d'accident pendant l'année est p. Quelle est la probabilité d'avoir au moins un accident pendant l'année ?

2. Représenter la situation par un graphe fléché, où chaque flèche, allant d'un état à un autre, sera accompagnée de la probabilité de passage entre les deux états.

3. Pour tout i entre 1 et 4, calculer $P(Y=i)$ en fonction de p et de $P(X=i)$.

4. a. On note $\mu_X = \begin{pmatrix} P(X=1) \\ P(X=2) \\ P(X=3) \\ P(X=4) \end{pmatrix}$ et de même pour μ_Y.

Déduire de la question **3.** la matrice P telle que $\mu_Y = P\mu_X$.

b. Que représente P_{11} ? P_{12} ? P_{13} ? P_{21} ?

c. Peut-on passer directement de l'état 4 à l'état 2 ?

d. Comment lire sur la matrice que l'on peut passer (indirectement) de l'état 4 à l'état 2 ?

5. Un jeune conducteur, c'est-à-dire une personne commençant à la classe 4, veut s'assurer.

a. Déterminer μ_X.

b. Calculer μ_Y.

72 Passer d'un état à un autre

On donne la matrice P suivante, représentant une situation de passage entre différents états, plus précisément, P_{ij} est la probabilité de passer de l'état j à l'état i :

$$P = \begin{pmatrix} 0{,}2 & 0 & 0{,}1 & 0{,}6 \\ 0{,}5 & 0{,}9 & 0{,}1 & 0 \\ 0 & 0 & 0 & 0{,}4 \\ 0{,}3 & 0{,}1 & 0{,}8 & 0 \end{pmatrix}.$$

1. Peut-on passer directement de l'état 4 à l'état 2 ? indirectement ?

2. a. Quel(s) est(sont) l'(les) état(s) que l'on peut atteindre directement depuis l'état 1 ? Quelle ligne / colonne doit-on regarder ?

b. Même question pour les états 2, 3 et 4.

3. a. Quel(s) est(sont) l'(les) état(s) qui mène(nt) directement à l'état 1 ? Quelle ligne/colonne doit-on regarder ?

b. Même question pour les états 2, 3 et 4.

c. Peut-on passer de l'état 1 à l'état 3 en passant par l'état 4 ?

4. a. Donner trois manières de passer de l'état 4 à l'état 2.

b. Donner trois manières de passer de l'état 4 à l'état 4.

5. a. On suppose que l'on part de l'état 1. Écrire le vecteur colonne de probabilité représentant cette situation.

b. Quelle est la probabilité que l'on se retrouve à l'état 1 après un changement d'état ?

c. Quelle est la probabilité que l'on se retrouve à l'état 1 après deux changements d'état ?

73

On considère un graphe fléché à trois états. Donner la matrice représentant la situation en suivant les informations suivantes :

- on passe de 1 à 3 avec la probabilité 0,9 ;
- on passe de 2 à 1 avec la probabilité 0,7 ;
- on passe de 3 à 2 avec la probabilité 0,5 ;
- on ne reste jamais sur un même état.

Rappel

P_{ij} est la probabilité de passer de l'état j à l'état i.

74 Jeu circulaire

Deux jeunes enfants jouent autour d'une cabine téléphonique. L'un des deux doit attraper l'autre. Pour corser le jeu, en arrivant à chaque coin de la cabine, il tourne dans un sens ou l'autre de façon aléatoire, mais équitablement répartie.



1. Après avoir numéroté les quatre coins de la cabine, représenter la situation par un graphe fléché.

2. a. Quelle sera la taille de la matrice représentant la situation.

b. Déterminer cette matrice.

Aide

On pourra reprendre le même principe qu'à l'exercice 71, ou plus directement, dire que P_{ij} est la probabilité de passage de l'état j à l'état i.

Systèmes linéaires

75 **1.** On considère le système linéaire suivant :

$$\begin{cases} 3x - 5y = 7 \\ -2x + y = -1 \end{cases}$$

a. Écrire ce système sous forme matricielle.
b. La matrice associée admet un inverse. Déterminer-le et résoudre ce système.
2. Mêmes questions avec le système suivant :

$$\begin{cases} x + y - z = 1 \\ 2x - 3y + z = -5 \\ 6x - 3z = 2 \end{cases}.$$

76 **1.** On considère le système linéaire suivant :

$$\begin{cases} 3x - 5y = 7 \\ 6x - 10y = 14 \end{cases}.$$

a. La matrice associée à ce système est-elle inversible ?
b. Montrer que l'équation L_2 est redondante par rapport à L_1.
c. En déduire que les solutions de ce système sont les couples $\left(x ; \dfrac{3x-7}{5}\right)$, $x \in \mathbb{R}$.

2. On considère le système linéaire suivant :

$$\begin{cases} x + y - z = 1 \\ 2x - 3y + z = -5 \\ x - 4y + 2z = -6 \end{cases}.$$

a. La matrice associée est-elle inversible ?
b. Montrer que L_3 est une combinaison linéaire de L_1 et L_2.
c. La ligne L_3 pouvant être éliminée, effectuer une combinaison linéaire entre L_2 et L_1 pour en éliminer l'inconnue x de L_2 et montrer que le système est équivalent au suivant :

$$\begin{cases} x + y - z = 1 \\ -5y + 3z = -7 \end{cases}.$$

d. En déduire que les solutions du système sont données par les triplets $\left(\dfrac{-2+2z}{5} ; \dfrac{7+3z}{5} ; z\right)$, $z \in \mathbb{R}$.
e. Vérifier à l'aide du logiciel Maxima ou XCas.

77 **Analyse critique d'une copie**

On considère le système suivant :

$$\begin{cases} -2x - y - z = -3 \\ 3x + 2y + z = 6 \\ x + y = 3 \end{cases}.$$

Voici deux résolutions, proposées par Marie et Pauline. Les résultats sont corrects, mais certains calculs maladroits. Les corriger.

Copie de Marie :

La matrice associée au système n'est pas inversible, donc on commence par éliminer la première inconnue des équations $\mathcal{L}_2$ et $\mathcal{L}_3$.
On remplace $\mathcal{L}_2$ par
$\mathcal{L}_2 + \dfrac{3}{2}\mathcal{L}_1 \Leftrightarrow \dfrac{y-z}{2} = \dfrac{3}{2} \Leftrightarrow y - z = 3.$
On remplace $\mathcal{L}_3$ par $2\mathcal{L}_3 + \mathcal{L}_1 \Leftrightarrow y - z = 3$.
On obtient donc le système :

$$\begin{cases} -2x - y - z = -3 \\ y - z = 3 \end{cases}$$

On choisit y comme paramètre, et on a donc :

$$\begin{cases} x = 3 - y \\ z = y - 3 \end{cases}$$

Les solutions sont donc données par les triplets : $(3 - y ; y ; y - 3)$, $y \in \mathbb{R}$.

Copie de Pauline :

La matrice associée au système n'est pas inversible, et on remarque que $\mathcal{L}_3 = \mathcal{L}_1 + \mathcal{L}_2$.
On peut donc éliminer une des équations du système, choisissons $\mathcal{L}_2$. On obtient donc :

$$\begin{cases} -2x - y - z = -3 \\ x + y = 3 \end{cases} \Leftrightarrow \begin{cases} -2x - y = -3 + z \\ x + y = 3 \end{cases}$$

On peut écrire ce système sous forme la forme matricielle :

$$\begin{pmatrix} -2 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -3 + z \\ 3 \end{pmatrix}$$

On inverse la matrice à l'aide d'une calculatrice et on a donc :

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} -3 + z \\ 3 \end{pmatrix} = \begin{pmatrix} -z \\ z + 3 \end{pmatrix},$$

Les solutions sont donc données par les triplets : $(-z ; z + 3 ; z)$, $z \in \mathbb{R}$.

78 Résoudre les systèmes linéaires suivants :

a. $\begin{cases} 3x - 2y + z = 8 \\ -x + 2y - 3z = -12 \\ x + 4y + z = 0 \end{cases}$; **b.** $\begin{cases} x - y + 2z = 0 \\ -2x + y - 3z = -1 \\ 3x + 2y + z = 5 \end{cases}$.

79 Même consigne qu'à l'exercice précédent.

a. $\begin{cases} x + y = 0 \\ 2x - 3y + 5z = 35 \\ 3x - 2y + 5z = 35 \end{cases}$; **b.** $\begin{cases} 2x + 7y - z = -27 \\ -4x - y - z = -6 \\ 6x + 6y + 6z = 27 \end{cases}$.

Devoir de synthèse

Revoir les bases suivantes :
cours de A à C, savoir-faire de 1 à 6.

[Le devoir est corrigé p. 173]

Chaque exercice peut être fait de manière indépendante.

80 QCM [5 points]

Soient A et B deux matrices, A est de taille 5×7.

1. Parmi les tailles suivantes, choisir celle(s) de B rendant possible le produit AB :

a. 5×7 ; **b.** 7×5 ; **c.** 7×7 ; **d.** 5×5.

2. Même question avec le produit BA.

3. Même question avec la somme $A + B$.

4. Soit A une matrice et B son inverse, alors

a. $AB = I$; **b.** $AB = O$; **c.** $AB = BA$.

5. L'inverse d'une matrice A est noté :

a. A^{-1} ; **b.** $-A$; **c.** $\frac{1}{A}$.

81 Vrai ou faux [3 points]

1. Une matrice peut admettre plusieurs inverses.

2. Les seules matrices pouvant admettre des inverses sont les matrices carrées.

3. Toutes les matrices carrées admettent des inverses.

4. Si A et B sont deux matrices, avec A matrice carrée et telles que AB soit calculable, alors BA est aussi calculable.

5. Si les deux produits AB et BA sont calculables, alors les matrices A et B sont toutes les deux carrées.

6. Tout système de n équations à p inconnues peut s'écrire sous forme matricielle, où la matrice est de taille $n \times p$.

82 [2 points]

Calculer, en le détaillant, le produit AB des matrices suivantes :

$$A = \begin{pmatrix} 1 & -3 & 5 \\ 9 & 5 & -2 \end{pmatrix} \text{ et } B = \begin{pmatrix} -5 \\ 6 \\ -7 \end{pmatrix}.$$

83 [3 points]

On considère la matrice A suivante :

$$A = \begin{pmatrix} 2 & -1 & 2 \\ 5 & -3 & 3 \\ -1 & 0 & -2 \end{pmatrix}.$$

1. Calculer $(A + I_3)^3$ à l'aide d'une calculatrice.

2. Développer $(A + I_3)^3$.

3. En factorisant correctement par A, en déduire que $A^{-1} = -(A^2 + 3A + 3I_3)$.

84 [1 point]

On considère l'algorithme suivant, permettant de définir une matrice A :

```
Saisi(n) ;
Saisir(p) ;
Pour j = 1 à p faire
   Pour i = 1 à n faire
      A[i][j] = 2i - j ;
   FinPour
FinPour
```

Donner la matrice A obtenue lorsque l'on prend $n = 4$ et $p = 3$.

85 [4 points]

On désire trouver toutes les matrices A, carrées de taille 2, inversibles et égales à leur inverse.

1. Démontrer que $A = A^{-1} \Leftrightarrow A^2 = I_2$.

2. On pose : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Calculer A^2 et démontrer que résoudre le problème donné revient à résoudre le système (S) suivant :

$$(S) \Leftrightarrow \begin{cases} a^2 + bc = 1 \\ b(a + d) = 0 \\ c(a + d) = 0 \\ d^2 + bc = 1 \end{cases}.$$

3. a. Démontrer que ce système est équivalent à (S_1) ou (S_2) donnés ci-dessous :

$$(S_1) \Leftrightarrow \begin{cases} d = -a \\ bc = 1 - a^2 \end{cases} ; \quad (S_2) \Leftrightarrow \begin{cases} d \neq -a \\ b = c = 0 \\ a^2 = d^2 = 1 \end{cases}.$$

b. Résoudre le système (S_1) en distinguant deux cas : $b = 0$ ou $b \neq 0$ et trouver les trois types de matrices A possibles.

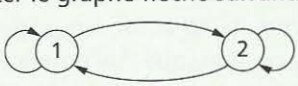
c. Résoudre le système (S_2) et trouver les deux matrices A possibles.

86 [2 points]

Un composant informatique possède deux états, en panne (1) ou fonctionnel (2).

Chaque minute, il passe de l'état 1 à l'état 2 avec une probabilité de 0,02 et passe de l'état 2 à l'état 1 avec une probabilité de 0,01.

1. a. Compléter le graphe fléché suivant.



b. Donner la matrice P représentant la situation, sachant que P_{ij} est la probabilité de passer de l'état j à l'état i.

2. a. On suppose que l'on part de l'état fonctionnel. Écrire le vecteur colonne de probabilité correspondant.

b. Quelle est la probabilité que le composant soit en panne au bout d'une minute ? deux minutes ?

Exercices guidés BAC

87 **1.** On considère l'algorithme suivant :

```
Saisir une matrice A ;
n = nombre de lignes A ;
p = nombre de colonnes de A ;
Pour i allant de 2 à n faire
   Pour j allant de 2 à p faire
      A[i][j] = A[i-1][j] + A[i][j-1] ;
   FinPour
FinPour
Afficher la matrice A ;
```

a. Donner la matrice affichée par l'algorithme si on lui donne en paramètre la matrice M suivante :

$$M = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ -1 & \ldots & \ldots & \ldots & \ldots \\ -3 & \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

b. Expliquer pourquoi les boucles portant sur les variables i et j commencent à 2 et non pas à 1.

2. Lors d'une autre simulation de cet algorithme, l'affichage a bogué et seulement une partie de la matrice était visible :

$$\begin{pmatrix} \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & 4 & 7 & 16 & 15 \\ \ldots & 9 & 16 & 32 & 47 \end{pmatrix}.$$

a. Peut-on retrouver tous les coefficients ? Expliquer pourquoi.

b. Retrouver le maximum de coefficients en expliquant brièvement la méthode.

c. On donne A[1][1] = –5. Cette donnée permet-elle de retrouver les coefficients manquants ? Si oui, les donner.

d. Même question avec en plus A[1][2] = 4.

Guide

1. a. On exécute l'algorithme pas à pas, sans tenter d'interpréter les résultats. La première boucle porte sur les lignes ; la seconde sur les colonnes. Le coefficient A[i][j] est celui situé à la i-ème ligne et j-ème colonne.

b. Il faut regarder attentivement les valeurs des indices utilisés dans l'algorithme.

2. La question 1 devrait suffire pour comprendre le principe de l'algorithme. Il suffit maintenant de procéder en sens inverse.

88 **1.** On considère les deux matrices suivantes :

$$A = \begin{pmatrix} 1 & 2 \\ -3 & -4 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 1 \\ -1 & -1 \\ 3 & 3 \end{pmatrix}.$$

a. Des deux produits AB et BA, lequel peut être calculé et pourquoi ?

b. Effectuer ce produit, que l'on notera P.

2. Quelle est la valeur du coefficient k tel que $P = kB$?

a. $k = 8$; **b.** $k = -2$; **c.** $k = 2$; **d.** $k = -8$.

3. On considère le système linéaire suivant : $\begin{cases} x + 2y = 9 \\ -3x - 4y = 0 \end{cases}$.

a. Écrire ce système sous forme matricielle.

b. Sans le calculer, dire si ce système admet-il un unique couple solution ? Justifier la réponse.

c. Dans le cas d'une réponse affirmative, déterminer ce couple.

Guide

1. a. On se réfère au cours et au nombre de lignes et colonnes nécessaires pour qu'un produit existe.

b. Le produit de deux matrices s'effectue ligne par colonne.

2. On se réfère à la définition du cours.

3. a. On commence toujours par poser $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $Y = \begin{pmatrix} 9 \\ 0 \end{pmatrix}$.

b. On teste si la matrice du système est inversible.

c. On utilise l'inverse de la matrice.

QCM - Vrai ou faux BAC

89 **Vrai ou Faux**

a. Une matrice nulle est une matrice carrée.

b. Une matrice identité est une matrice carrée.

c. Toute matrice possédant un inverse est carrée.

d. Il n'est possible d'inverser que des matrices dont les coefficients sont des nombres différents de 0.

90 **QCM**

Déterminer toutes les bonnes réponses.

1. Une matrice A est dite inversible lorsqu'il existe une matrice B telle que :

a. $AB = O$; **b.** $AB = I$; **c.** $BA = O$; **d.** $BA = I$.

2. Lorsqu'il est calculable, le produit $A(BC)$ est égal à :

a. $(AB)C$; **b.** ABC ; **c.** $(AB)(AC)$.

91 **Vrai ou Faux**

a. Si la matrice A est inversible, alors le système $AX = Y$ admet un unique vecteur colonne solution X.

b. Pour toutes matrices carrées A et B, on a $AB = BA$.

c. Pour toutes matrices carrées A et B pour lesquelles $AB = BA$, on peut affirmer que B est l'inverse de A.

d. L'identité $(A + B)^2 = A^2 + 2AB + B^2$ est vraie pour toutes matrices carrées A et B.

e. Soient A une matrice carrée inversible, et B et C telles que $AB = AC$.
Alors $B = C$.

92 **QCM**

On considère les matrices suivantes :

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} ; \quad B = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} ; \quad C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

1. Parmi les produits suivants, lesquels peut-on calculer :

a. AB ; **b.** AC ; **c.** BA ;

d. CA ; **e.** BC ; **f.** CB.

2. Calculer ces produits lorsque cela est possible.

3. Le système $AX = C$, où X est un vecteur colonne, admet pour solution :

a. $X = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$; **b.** $X = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$; **c.** $X = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$.

4. Le système $XA = B$, où X est un vecteur ligne, admet pour solution :

a. $X = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$;

b. $X = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$;

c. $X = \begin{pmatrix} 1 & -1 & 0 \end{pmatrix}$.

Exercice BAC

93 On considère la matrice P suivante :

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

1. a. Calculer, sans calculatrice, P^2, P^3 et P^4.

b. Quelle formule peut-on conjecture pour P^n, n étant un entier naturel non nul ?

c. Démontrer cette formule par récurrence.

2. On cherche, si elle existe, la matrice M telle que $PM = MP = I_2$.

a. En posant $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, écrire le système que doivent satisfaire les nombres a, b, c et d.

b. Résoudre ce système et en déduire la matrice M.

3. a. Écrire la matrice carrée A de dimension 2 telle que $a_{11} = 2$; $a_{22} = -2$; $a_{12} = 3$; $a_{21} = 5$.

b. Déterminer, sans calculer son inverse, si cette matrice est inversible.

4. a. Des deux systèmes suivants, lequel peut s'écrire sous une forme matricielle utilisant la matrice A ?

$$\begin{cases} 2x + 3y = 4 \\ 5x - 2y = 6 \end{cases} ;$$

$$\begin{cases} 2x + 5y = 4 \\ 3x - 2y = 6 \end{cases}.$$

On posera $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $Y = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$.

b. Résoudre ce système.

5. a. Calculer le produit $B = AP$.

b. Résoudre le système $BX = Y$ sans utiliser l'inverse de la matrice B.

c. Vérifier avec une calculatrice ou un logiciel, en utilisant l'inverse de la matrice B.

94 Soit A une matrice carrée de taille n telle que $I + A$ soit inversible. On pose $B = (I - A)(I + A)^{-1}$.
On souhaite exprimer A en fonction de B.
1. Démontrer que $(I + A)(I - A) = (I - A)(I + A)$.
2. En multipliant à gauche et à droite chaque membre de cette égalité par $(I + A)^{-1}$, démontrer que
$$B = (I + A)^{-1}(I - A).$$
3. Calculer astucieusement le produit $(I + A)(I + B)$ et en déduire l'inverse de $(I + B)$.
4. Calculer $(I - B)(I + B)^{-1}$ et répondre au problème posé.

95 Soient A et B les deux matrices suivantes :
$$A = \begin{pmatrix} 7 & 6 \\ 0 & 3 \end{pmatrix}; \quad B = \begin{pmatrix} -3 & -4 \\ 15 & 13 \end{pmatrix}$$
On désire déterminer, si elles existent, les matrices P inversibles telles que $B = P^{-1}AP$.
1. Trouver une condition nécessaire sur PB et AP, puis montrer que cette condition revient à :
$$(S) \Leftrightarrow \begin{cases} -10a + 15b + 6c = 0 \\ -2a + 3b + 3d = 0 \\ -2c + 5d = 0 \end{cases}$$
2. **a.** Ce système étant linéaire, l'écrire sous une forme matricielle.
b. Peut-on résoudre ce système à l'aide de la matrice inverse ?
3. **a.** Montrer que L_1 est une combinaison linéaire de L_2 et L_3.
b. Donner les solutions du système en fonction de b et d et en déduire la forme des matrices P.
4. **a.** Démontrer que P est inversible si et seulement si $3d^2 - 2bd \neq 0$.
b. Résoudre l'équation associée et démontrer que P est inversible si, et seulement si, $d \neq 0$ et $b \neq \frac{3}{2}d$.
c. Donner une matrice P dont tous les coefficients sont entiers et vérifier (à l'aide d'un logiciel ou d'une calculatrice) que l'on a bien $B = P^{-1}AP$.

96 1. **a.** Déterminer, si elles existent, les matrices inversibles P telles que $B = P^{-1}AP$ pour les matrices A et B suivantes :
$$A = \begin{pmatrix} 2 & 3 \\ 6 & 5 \end{pmatrix}; \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 8 \end{pmatrix}$$
On pourra s'aider d'un logiciel pour résoudre le système 4×4 obtenu.
b. Donner une matrice P dont les coefficients sont tous entiers.
2. **a.** Démontrer, par récurrence sur l'entier naturel n, que $B^n = P^{-1}A^nP$.
b. Démontrer, par récurrence sur l'entier n, que $B^n = \begin{pmatrix} (-1)^n & 0 \\ 0 & 8^n \end{pmatrix}$
c. Déduire des questions précédentes une méthode rapide pour calculer A^n.

97 Démontrer l'identité suivante, où A est une matrice inversible :
$$(A + UBV)^{-1} = A^{-1} - A^{-1}U(I_n + BVA^{-1}U)^{-1}BVA^{-1}.$$

98 On considère les matrices A et P suivantes :
$$A = \begin{pmatrix} -5 & -6 & 6 \\ -1 & 0 & 2 \\ -4 & -4 & 6 \end{pmatrix}; \quad P = \begin{pmatrix} 1 & 0 & 2 \\ -1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$
1. **a.** Calculer P^{-1}.
b. Calculer $D = P^{-1}AP$.
2. Donner, pour tout entier naturel n, l'expression de D^n.
3. En déduire, pour tout entier naturel n, l'expression de A^n.

99 On considère la matrice de taille 2 suivante :
$A = \left(\sin(a_i + a_j)\right)_{1 \leq i,j \leq 2}$, où a_1 et a_2 sont réels.
On veut déterminer à quelle(s) condition(s), portant sur a_1 et a_2, la matrice A est inversible.
1. **Conjecture**
a. Dans un logiciel de géométrie dynamique, placer deux points, M_1 et M_2 sur le cercle trigonométrique.
b. Mesurer les angles $a_1 = \widehat{IOM_1}$ et $a_2 = \widehat{IOM_2}$ puis faire calculer au logiciel la quantité d, permettant de savoir si A est inversible.
c. Placer le point $P(a_2 ; d)$ et demander le lieu de P lorsque M_1 décrit le cercle unité. Émettre une conjecture concernant le problème posé.
2. Démontrer cette conjecture.

100 **Matrice inversible à coefficients entiers**
Soit A une matrice de taille 2 à coefficients entiers :
$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ où $a, b, c, d \in \mathbb{Z}$. On note $\Delta_A = ad - bc$.
1. Soient M et N deux matrices carrées de taille 2. Montrer que $\Delta_{MN} = \Delta_M \times \Delta_N$.
2. **a.** Démontrer que si $\Delta_A = \pm 1$, alors A est inversible est que les coefficients de A^{-1} sont des entiers.
b. Démontrer la réciproque en utilisant le résultat de la question 1.

101 **Matrices et géométrie**
On considère la matrice R_a suivante, ou a est un réel :
$$R_a = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix}.$$
1. **a.** Dans un logiciel de géométrique dynamique, créer un curseur a allant de 0 à 360.
b. Créer la matrice R_a associée au réel a.

Aide

Dans CaRMetal, on créera les deux vecteurs colonnes représentant la matrice : $\vec{u_1}$ et $\vec{u_2}$.

Dans GeoGebra 4, on tapera : R={{cos(a), -sin(a)}, {sin(a), cos(a)}} dans la barre de saisie.

c. Créer un vecteur $\vec{u}$. Faire calculer $\vec{v} = R_a\vec{u}$ au logiciel et représenter $\vec{v}$ avec la même origine que $\vec{u}$.

Aide

Dans CaRMetal, on utilisera la macro prévue à cet effet.

Dans GeoGebra 4, on commencera par taper : R*u.

d. Que peut-on conjecturer sur l'angle géométrique $(\vec{u}; \vec{v})$?

2. Démontrer ceci en calculant les coordonnées du vecteur $\vec{v}$ en fonction de celles de $\vec{u}$ puis en utilisant un produit scalaire.

3. Prévoir le résultat de $(R_a)^2\vec{u}$ et le vérifier par un calcul.

4. On considère maintenant la matrice S_a suivante :

$$S_a = \begin{pmatrix} \cos a & \sin a \\ \sin a & -\cos a \end{pmatrix}.$$

a. Reprendre les questions **1.a.**, **b.** et **c.**

b. Quelle interprétation géométrique donner à S_a pour $a = 0°$? pour $a = 180°$?

c. Et pour a quelconque ?

102 **Matrice transposée**

Soit A une matrice de taille $n \times p$. La matrice transposée de A, notée ${}^tA$, est obtenue en échangeant les lignes et les colonnes de A.

1. D'après cette définition, quelle est la taille de ${}^tA$?

2. Donner ${}^tA$ pour la matrice A suivante :

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

3. Soit $B = {}^tA$. Pour tous $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant n$, quelle est la valeur de b_{ij} ?

4. Soient A une matrice de taille $n \times p$ et B une matrice de taille $p \times q$. On veut démontrer que ${}^t(AB) = {}^tB{}^tA$.

a. Vérifier cette propriété avec les matrices ci-dessous :

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \quad B = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}.$$

b. On note $C = AB$. Compléter la phrase suivante :

Pour tous $1 \leqslant i \leqslant \ldots$ et $1 \leqslant j \leqslant \ldots$, $c_{ij} = \sum_{k=\ldots}^{\ldots} a_{ik}b_{kj}$.

c. On note $D = {}^tB{}^tA$. Compléter la phrase suivante :

Pour tous $1 \leqslant i \leqslant \ldots$ et $1 \leqslant j \leqslant \ldots$, $d_{ij} = \sum_{k=\ldots}^{\ldots} b_{\ldots\ldots}a_{\ldots\ldots}$.

d. Comparer c_{ij} et d_{ji}.

5. Applications

a. L'inconnue de l'équation $AX = Y$ est un vecteur colonne. L'écrire avec un vecteur ligne.

b. Soit A une matrice inversible. Démontrer que ${}^tA$ est inversible et que son inverse est ${}^t(A^{-1})$.

c. Reprendre l'exercice 71 p. 131, mais à la question **4.a.**, on prendra :

$$\mu_X = \big(P(X = 1)\ \ P(X = 2)\ \ P(X = 3)\ \ P(X = 4)\big),$$

et de même pour μ_Y. Quelle sera alors la relation entre μ_X et μ_Y ?

Quel est le lien entre la matrice P ainsi trouvée et celle de l'exercice original ?

Défis

103 **Forme quadratique**

Écrire la forme quadratique de deux variables suivante à l'aide du vecteur dont les coordonnées sont x et y et d'une matrice à déterminer :

$$F(x ; y) = ax^2 + by^2 + 2cxy.$$

Communiquer à l'écrit ou à l'oral

Qu'est-ce que le déterminant d'une matrice et à quoi cela sert-il ?

Quelques pistes pour répondre :

1. On pourra commencer par s'intéresser aux calculs d'aires et de volumes et à la manière de calculer des déterminants d'ordre 2 et 3.

2. On pourra poursuivre l'investigation en s'intéressant aux systèmes de Cramer d'ordre 2 et 3.

3. Finalement, on pourra s'intéresser à une méthode de calcul pour les déterminants d'ordre supérieur (4 ou 5).

4. On pourra aussi s'orienter sur l'utilisation du déterminant dans le calcul de la matrice inverse.



Gabriel Cramer (1704-1752)

Communiquer les résultats

Réaliser un diaporama où on présentera pas à pas des calculs de déterminants d'ordre 2 et 3, ainsi que leurs applications. On pourra aussi détailler un exemple de calcul de déterminant d'ordre 4 ou 5.

Accompagnement personnalisé

Soutien

AP 1 Analyser une copie

Objectifs :
- Revoir le produit matriciel et l'écriture d'un système sous forme matricielle.
- Avoir une attitude critique vis-à-vis de documents.

On considère l'énoncé et la copie d'élève suivants. Corriger la copie en rectifiant les erreurs et en rédigeant correctement.

1. Effectuer le produit AB des matrices suivantes :

$$A = \begin{pmatrix} -1 & 2 \\ 3 & -4 \end{pmatrix} ; \quad B = \begin{pmatrix} 1 & -2 \\ -3 & 4 \end{pmatrix}.$$

2. Écrire le système suivant en utilisant une matrice puis le résoudre.

$$\begin{cases} 3x - 2y = -1 \\ -5x + 6y = 5 \end{cases}.$$

1. On commence par faire le produit des premières lignes de A et B :

$$(-1) \times 1 + 2 \times (-2) = -5$$

On continue avec le produit de la 1e ligne de A avec la 2e de B :

$$(-1) \times (-3) + 2 \times (4) = 11$$

etc.

On a donc : $AB = \begin{pmatrix} -5 & 11 \\ 11 & -25 \end{pmatrix}$

2. Le système peut alors s'écrire $MX = y$, *avec* $M = \begin{pmatrix} 3 & -2 \\ -5 & 6 \end{pmatrix}$.

On a alors

$$X = \frac{1}{M} y = \begin{pmatrix} \frac{1}{3} & -0{,}5 \\ -0{,}2 & \frac{1}{6} \end{pmatrix} \begin{pmatrix} -1 \\ 5 \end{pmatrix},$$

et on trouve : $x = -\frac{17}{6}$ *et* $y = \frac{31}{30}$.

Découvrir un métier

AP 2 Ingénieur informaticien

Objectifs :
- Aide à l'orientation.
- Comprendre l'utilité des mathématiques.

La transmission de données sensibles se fait après avoir codé le message. Pour cela, un ingénieur peut utiliser des matrices. À l'inverse, il peut aussi les utiliser pour tenter de casser le système de chiffrement ou pour tester sa robustesse.

1. **a.** Expliquer le principe du chiffrement par blocs.
b. Donner des exemples de tels chiffrements.

2. Mêmes questions avec le chiffrement linéaire.

3. Donner un exemple de chiffrement linéaire par blocs.

4. En quoi consiste la cryptanalyse linéaire et pour casser quel algorithme a-t-elle été développée ?



Approfondir

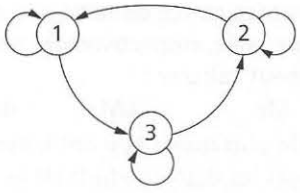
AP 3 Matrice associée à un graphe

Objectifs :
- *Calculer les vecteurs donnant les probabilités d'être en chaque état.*
- *En déduire la matrice correspondant à la situation.*

Un individu présente trois états face à une maladie contagieuse :
- immunisé (état 1) ;
- malade (état 2) ;
- non immunisé et non malade (état 3).

Chaque jour, son état peut changer selon les règles suivantes :
- s'il est dans l'état 1, il peut y rester avec une probabilité de 0,9 ou passer à l'état 3 ;
- s'il est dans l'état 2, il peut y rester avec une probabilité de 0,2 ou passer à l'état 1 ;
- s'il est dans l'état 3, il peut y rester avec une probabilité de 0,5 ou passer à l'état 2.

1 Compléter le graphe fléché correspondant à cette situation.



2 **a.** On note X et Y les variables aléatoires représentant les états d'un individu pour deux jours consécutifs. Quel est l'ensemble des valeurs prises par X et Y ?

b. En remarquant que les événements $(X = 1)$, $(X = 2)$ et $(X = 3)$ forment une partition de l'espace de probabilité, démontrer que
$P(Y = 1) = 0{,}9P(X = 1) + 0{,}8P(X = 2)$.

c. Faire de même pour $P(Y = 2)$ et $P(Y = 3)$.

d. On note $\mu_X = \begin{pmatrix} P(X = 1) \\ P(X = 2) \\ P(X = 3) \end{pmatrix}$ et de même pour μ_Y.

Déduire des questions **b.** et **c.** la matrice M telle que $\mu_Y = M\mu_X$.

3 On suppose que le premier jour, l'individu est malade.

a. Écrire μ_X.

b. En déduire la probabilité qu'il soit guéri le jour suivant.

c. On note Z la variable aléatoire représentant l'état de l'individu le 3e jour. Calculer μ_Z puis en déduire la probabilité que l'individu soit guéri le 3e jour ?

AP 4 Inverse d'une matrice

Objectifs :
- *Factoriser et développer des expressions algébriques.*
- *Revoir la notion de matrice inverse.*

Soit A une matrice telle qu'il existe un entier naturel n tel que $A^n = O$.
On veut montrer que $I - A$ et $I + A$ sont inversibles.

1 $n = 2$

a. Factoriser $I - A^2$ par $I - A$.

b. En déduire que $I + A$ et $I - A$ sont inversibles et donner leur inverse.

2 $n = 3$

a. Factoriser $I - A^3$ par $I - A$ puis en déduire que $I - A$ est inversible et donner son inverse.

b. Factoriser $I + A^3$ par $I + A$ puis en déduire que $I + A$ est inversible et donner son inverse.

3 $n = 4$

a. Factoriser $I - A^4$ par $I - A$ puis en déduire que $I - A$ est inversible et donner son inverse.

b. Montrer que la même technique de factorisation ne fonctionne pas pour $I + A^4$ par $I + A$.

c. Factoriser alors $I + A^5$ par $I + A$ et en déduire que $I + A$ est inversible et donner son inverse.

4 Traiter le cas général selon les valeurs de n.

5 Suites de matrices

Vérifier ses acquis

1 Sommes

1. Expliciter chacune des formules suivantes :

a. $\sum_{k=1}^{10} 2^k$; **b.** $\sum_{k=0}^{8} (-1)^k(2k+1)$;

c. $\sum_{k=0}^{5} M^{2k}$; **d.** $\sum_{k=0}^{4} (-1)^{k+1}M^k$.

2. Exprimer les sommes suivantes à l'aide du symbole Σ :

a. $a + a^3 + a^5 + a^7 + a^9 + a^{11} + a^{13}$;

b. $-A^{-1} + I - A + A^2 - A^3$ où A est une matrice carrée ;

c. $a - a^3 + a^5 - a^7$.

3. On considère la suite (u_n) définie par $u_{n+1} = au_n + b$. Démontrer que pour tout entier naturel n :

$$u_n = a^n u_0 + b\sum_{k=0}^{n-1} a^k.$$

2 QCM

On considère une matrice $A = (a_{ij})$ de taille $n \times p$ et un vecteur colonne u. On pose $v = Au$.

1. Pour que le produit Au soit calculable, la taille du vecteur u doit être :

a. n. **b.** p.

2. Quelle est alors la taille de v ?

3. On note u_k la k-ième coordonnée du vecteur u. Pour tout entier i entre 1 et n, la formule donnant la i-ème coordonnée de v, notée v_i, est :

a. $\sum_{k=1}^{p} a_{ik}u_k$. **b.** $\sum_{k=1}^{n} a_{ik}u_k$. **c.** $\sum_{k=1}^{p} a_{ki}u_k$. **d.** $\sum_{k=1}^{n} a_{ki}u_k$.

4. Soit $B = (b_{ij})$ une matrice de taille $p \times q$. On pose $C = AB$. Alors la formule donnant le coefficient c_{ij} est :

a. $\sum_{k=1}^{p} a_{ik}b_{jk}$. **b.** $\sum_{k=1}^{p} a_{ik}b_{kj}$. **c.** $\sum_{k=1}^{p} a_{ki}b_{kj}$. **d.** $\sum_{k=1}^{p} a_{ki}b_{kj}$.

3 QCM 2

Pour chacune des questions suivantes, choisir la ou les bonnes réponses.

1. On peut résoudre un système matriciellement si :

a. la matrice correspondant au système est carrée ;

b. la matrice correspondant au système est inversible ;

c. dans tous les cas.

2. Soit A une matrice de taille $n \times p$ et B une matrice de taille $p \times q$, alors :

a. le produit $C = AB$ est calculable ;

b. le produit $C = BA$ est calculable ;

Dans ce cas, la taille de C est :

c. $n \times q$. **d.** $p \times q$. **e.** $n \times p$. **f.** $q \times n$.

3. Soit M une matrice carrée de taille n, u et v deux vecteurs de même taille, respectivement en ligne et en colonne. On peut calculer :

a. Mu. **b.** Mv. **c.** uM. **d.** vM.

4. On suppose de plus que u et v ont les mêmes coordonnées, alors les deux produits de la question **3.** ont les mêmes coordonnées :

a. pour toute matrice M telle que pour tous i et j, $m_{ij} = m_{ji}$;

b. pour toute matrice M telle que pour tout i, $m_{ii} = 0$;

c. pour toute matrice M telle que pour tout i,

$$\sum_{k=1}^{n} u_k(m_{ik} - m_{ki}) = 0.$$

4 Probabilités

Le mathématicien Andreï Markov étudia en 1913 la succession des lettres dans un roman d'Alexandre Pouchkine. Dans l'alphabet russe, il remarqua que :

- une voyelle succède à une voyelle dans un huitième des cas ;
- une consonne succède à une consonne dans un tiers des cas.

On note $(X_n)_{n\geqslant 1}$ la suite de variables aléatoires définie de la manière suivante : $X_n = 0$ si la n-ième lettre est une voyelle et 1 sinon.

1. a. Donner les probabilités de succession d'une voyelle avec une consonne et d'une consonne avec une voyelle.

b. Pour tous i et j valant 0 ou 1, donner les probabilités suivantes : $P_{(X_n = i)}(X_{n+1} = j)$

2. a. Exprimer $P(X_{n+1} = 0)$ en fonction de $P(X_n = 0)$ et $P(X_n = 1)$.

b. Écrire cette expression comme le produit d'un vecteur ligne par le vecteur colonne

$$\mu^{(n)} = \begin{pmatrix} P(X_n = 0) \\ P(X_n = 1) \end{pmatrix}.$$

3. Mêmes questions pour $P(X_{n+1} = 1)$.

4. Donner la matrice M telle que $\mu^{(n+1)} = M\mu^{(n)}$.

Harmonie tonale

Dans la musique occidentale, les traités d'harmonie tonale décrivent les règles de disposition et d'enchaînement des accords. Ces règles, précises, résultent en général de constatations faites par des générations de musiciens.

Exemples : *En Do Majeur, la note sensible (si), est mélodiquement attirée par la tonique (do). Toujours en Do Majeur, un accord de septième de dominante avec fondamentale (sol – si – ré – fa), a vocation à être enchaîné avec un accord de tonique (do – mi – sol). De plus, la septième (fa), doit descendre au III^e^ degré (mi). Il y a donc deux notes à mouvement obligé dans cet accord et tout cela en respectant quelques autres règles d'écriture.*

Partition de la Flûte enchantée de W.A. Mozart

Qu'est-ce que la MAO ?

Peut-on composer de la musique en utilisant un algorithme et des matrices ? Que représente alors la matrice ?

Activité 1 Une urne, puis une autre...

OBJECTIFS
Revoir : résoudre manuellement un système linéaire.
Découvrir : vecteur de probabilité caractérisant une situation.

On se place dans la même situation que dans l'activité 2 p. 106 et on reprend les mêmes notations.

1 **a.** En faisant un raisonnement analogue à celui donné dans la question **1.** de l'activité 2 p. 106, démontrer que pour tout entier naturel n ainsi que pour tous i et j compris entre 1 et 3 :

$$P(X_{n+1} = i) = \sum_{j=1}^{3} p_{ij} P(X_n = j).$$

b. En déduire une expression de $\mu^{(n+1)}$ en fonction de $\mu^{(n)}$ et $P = (p_{ij})_{1 \leqslant i,j \leqslant 3}$.

c. À l'aide d'un raisonnement par récurrence, établir que pour tout entier naturel n : $\mu^{(n)} = P^n \mu_0$.

2 **a.** On suppose que $\mu^{(0)} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ et on reprend la matrice P donnée dans la question **3.** de l'activité 2 p. 107. Calculer $\mu^{(10)}$, $\mu^{(20)}$, etc. à l'aide d'un logiciel ou d'une calculatrice.
Que remarque-t-on ?

Aide
Dans Maxima, on calcule la puissance n-ième d'une matrice P en écrivant « P^^n ».
Dans XCas, ou avec une calculatrice, on utilise la syntaxe habituelle.

b. Reprendre la question **a.** avec $\mu^{(0)} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ puis $\mu^{(0)} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Que remarque-t-on ?

c. Quelle est la probabilité approchée de piocher un jeton portant le n° 1 ? le n° 2 ? le n° 3 ?

3 **a.** On suppose qu'il existe un vecteur colonne μ tel que $\mu = \lim\limits_{n \to +\infty} \mu^{(n)}$. Quelle est alors la relation vérifiée par μ ?
b. Démontrer que cette relation peut s'écrire $(P - I_3)\mu = 0$.

4 **a.** Calculer la matrice $P - I_3$.
b. Peut-on résoudre ce système en utilisant l'inverse de cette matrice ?
c. Résoudre ce système et démontrer qu'en choisissant la troisième coordonnée de μ comme paramètre, on a :

$\mu = \begin{pmatrix} \frac{20c}{27} \\ \frac{5c}{9} \\ c \end{pmatrix}$. Si on préfère choisir la première coordonnée, on a : $\mu = \begin{pmatrix} a \\ \frac{3a}{4} \\ \frac{27a}{20} \end{pmatrix}$.

d. Choisir une valeur arbitraire pour c (ou a). Le vecteur obtenu est-il un vecteur de probabilité (c'est-à-dire un vecteur dont la somme des coefficients est égale à 1) ?
e. Si ce n'est pas le cas, effectuer le quotient de chaque coordonnée du vecteur obtenu par la somme de ses coordonnées. On trouve alors un vecteur μ de probabilité, appelé probabilité stationnaire. Comparer les valeurs des coordonnées de ce vecteur avec celles trouvées aux questions **2.a.** et **2.b.**
f. Avec quelle probabilité exacte pioche-t-on un jeton portant le n° 1 ? le n° 2 ? le n° 3 ?

Activité 2 Étude du principe du calcul de la pertinence d'une page Web

Objectifs
Revoir : résoudre un système linéaire avec un logiciel.
Découvrir : une suite de vecteurs colonnes.



On reprend l'activité 3 p. 107, ainsi que ses notations.
On va maintenant naviguer de page en page et on note $\mu^{(n)}$ le vecteur colonne donnant la probabilité d'être en chaque page après n clics. Plus précisément, $\mu_i^{(n)}$ est la probabilité d'être sur la page P_i après n clics.
On rappelle que la matrice M permettant de définir l'importance d'une page Web par comptage récursif est :

$$M = \begin{pmatrix} 0 & \frac{1}{4} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \frac{1}{4} & 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{4} & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 \end{pmatrix}$$

1 **a.** On suppose que l'on commence à naviguer à partir de la page P_1. Donner le vecteur $\mu^{(0)}$.

b. Avec un logiciel ou une calculatrice, déterminer $\mu^{(10)}$, $\mu^{(20)}$, etc. Que remarque-t-on ?

c. Reprendre les questions **a.** et **b.** mais en commençant à naviguer à partir de la page P_5.

d. En déduire la probabilité approchée qu'un internaute soit sur le page P_1, c'est-à-dire la fraction de temps passée sur cette page.
Même question avec P_2.

2 On rappelle que l'équation matricielle vérifiée par μ est $\mu = M\mu$.
Démontrer que cette relation peut s'écrire $(M - I_7)\mu = 0$

3 Résolution de cette équation à l'aide du logiciel Maxima.

→ *Le symbole $ sert à ne pas afficher le résultat. Utile lorsque l'on manipule de grosses matrices.*

a. Saisir la matrice M ainsi que la matrice I_7. Faire calculer la différence $M - I_7$ et la stocker dans R.

```
(%i3) R:M-I$
```

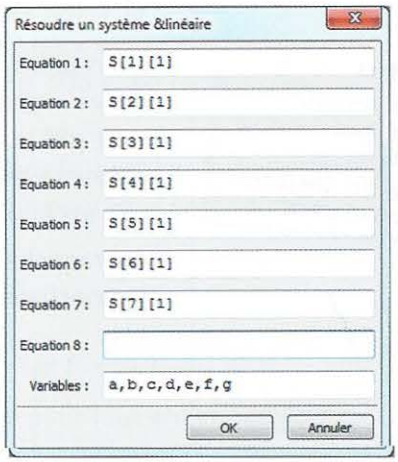
b. Saisir la matrice colonne μ en notant a, b, ..., f, g les coordonnées inconnues. Effectuer le produit $R\mu$ et le stocker dans S.

```
(%i4) mu: matrix([a],[b],[c],[d],[e],[f],[g])$
(%i5) S:R.mu;
```

c. On va résoudre ce système linéaire de 7 équations à 7 inconnues. Dans le menu « Équations », cliquer sur « Résoudre un système linéaire… » pour obtenir la fenêtre ci-contre.

→ *On n'est pas obligé de spécifier « = 0 ».*

Les 7 premières équations proviennent de la relation donnée en **2.a.** Compléter la 8e sachant que μ est un vecteur de probabilité.

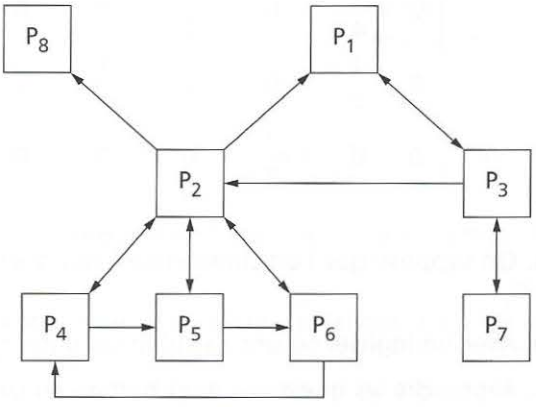


d. Analyser le résultat et expliquer comment retrouver le vecteur donné à la question **3.g.** de la page 109.

e. Avec quelle probabilité exacte un internaute est-il sur la page P_1 ? sur la page P_2 ?

4 On suppose à partir de maintenant que l'on rajoute une page P_8, vers laquelle pointe P_2 et qui n'émet pas de lien (ou seulement vers elle-même, ce qui revient au même).

a. Donner la matrice M, de taille 8, correspondant à ce graphe.



Aide

Mise à part la 2e colonne, les autres ne changent pas.

b. Comme à l'accoutumé, on suppose que l'on commence à naviguer à partir de la page 1. Ainsi, seule la première coordonnée de $\mu^{(0)}$ est non nulle et vaut 1. Calculer $\mu^{(200)} = M^{200}\mu^{(0)}$ à l'aide d'un logiciel ou une calculatrice et en déduire la probabilité qu'après 200 clics, on soit sur la page P_8.

c. Reprendre la question **3.** afin de trouver le vecteur μ tel que $\mu = M\mu$.

5 Afin de ne pas se faire piéger par une page non émettrice de lien, où l'internaute demeurerait le reste de sa vie numérique, on instaure un saut, dépendant d'un paramètre $c \in [0 ; 1]$. Plus précisément :

- avec la probabilité c, l'internaute abandonne la page actuelle pour aller sur une des autres pages, choisie de manière équiprobable ;
- avec la probabilité $1 - c$, l'internaute suit un des liens disponibles sur la page actuelle, toujours choisi de manière équiprobable.

On définit alors la suite de vecteurs de probabilité (cela sera démontré dans l'exercice 26 p. 157) suivante :

$$\mu^{(n+1)} = (1-c)M\mu^{(n)} + cE, \text{ où } E = \begin{pmatrix} 1/8 \\ \vdots \\ 1/8 \end{pmatrix}.$$

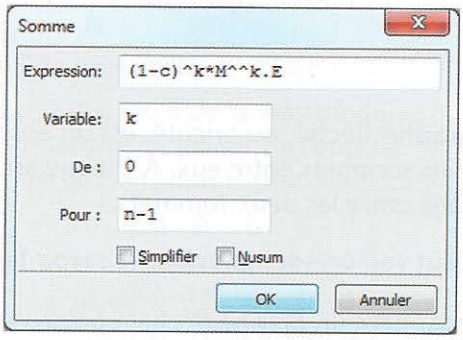
a. Démontrer par récurrence sur l'entier naturel n que :

$$\mu^{(n)} = (1-c)^n M^n \mu^{(0)} + c\sum_{k=0}^{n-1} (1-c)^k M^k E.$$

b. Avec un logiciel ou une calculatrice, déterminer $\mu^{(10)}$, $\mu^{(20)}$, etc. en prenant $c = 0{,}15$. Que remarque-t-on ?

Aide

• Avec Maxima, pour calculer une somme, on utilisera la commande « Calculs/Calculer la somme… » pour entrer la formule de la somme :



On tapera ensuite le reste de la formule manuellement.

```
(%i4) c:0.15$
      n:10$
      (1-c)^n*M^^n.mu + c*sum((1-c)^k*M^^k.E, k, 0, n-1);
```

• Avec XCas, on tapera manuellement la même formule, à la différence près que les puissances de matrices s'écrivent « M^k ».

c. Reprendre la question précédente avec $c = 0{,}99$ et interpréter le résultat obtenu. Est-ce une « bonne » valeur de c pour étudier la pertinence de ce réseau de pages Web ?

6 Comme dans la question **3.** déterminer le vecteur μ tel que

$$\mu = (1-c)M\mu + cE.$$

Aide

On pourra commencer par mettre cette équation sous la forme $A\mu = cE$, où A est une matrice à déterminer.
On prendra aussi garde à ne pas appeler c la troisième coordonnée du vecteur colonne $m\mu$.

A Matrices stochastiques

1 Définition

Définition 1

On dit qu'un vecteur ligne ou colonne est **stochastique** lorsque ses coordonnées sont des réels positifs et que leur somme est égale à 1.
On dit qu'une matrice est stochastique selon les lignes, (respectivement colonnes) si chaque vecteur ligne (respectivement colonne) de la matrice est stochastique.

Remarque : Dans un vecteur ou une matrice stochastique, tous les coefficients sont compris entre 0 et 1.

Exemple : La matrice suivante est stochastique à la fois selon les lignes et les colonnes :

$$A = \begin{pmatrix} 0,2 & 0,7 & 0,1 \\ 0,5 & 0,3 & 0,2 \\ 0,3 & 0 & 0,7 \end{pmatrix}.$$

Définition 2

Un **graphe fléché**, ou orienté, est un ensemble de sommets et d'arrêtes qui relient certains sommets entre eux. À chaque arrête peut être associée la probabilité de passage entre les deux sommets.

On peut voir un exemple dans le savoir-faire 1.

Propriété 1

On considère un graphe fléché représentant les probabilités de transitions entre plusieurs états numérotés de 1 à n. Alors la matrice A, où chaque coefficient a_{ij} est la probabilité de passage de l'état j à l'état i est une matrice stochastique selon les colonnes. Elle est appelée matrice de transition associée au graphe et de plus, A est carrée de taille n.

2 Image d'un vecteur stochastique

Propriété 2

Si A est une matrice stochastique selon les colonnes et u un vecteur colonne stochastique, alors $v = Au$ est aussi un vecteur colonne stochastique.
Si A est une matrice stochastique selon les lignes et u un vecteur ligne stochastique, alors $v = uA$ est aussi un vecteur ligne stochastique.

Démonstration

Notons $n \times p$ la taille de A. A est stochastique selon les colonnes donc pour tout k entre 1 et p, on a :

$$\sum_{i=1}^{n} a_{ik} = 1.$$

$v = Au$, donc, pour tout i entre 1 et n, on a : $v_i = \sum_{k=1}^{p} a_{ik}u_k$.

Ainsi : $$\sum_{i=1}^{n} v_i = \sum_{i=1}^{n}\sum_{k=1}^{p} a_{ik}u_k = \sum_{k=1}^{p} u_k \sum_{i=1}^{n} a_{ik} = \sum_{k=1}^{p} u_k = 1.$$

De plus, pour tout i entre 1 et n, v_i est positif car somme de nombres positifs.

Savoir-faire 1 Déterminer une matrice de transition

→ Exercice corrigé 9 p. 155
→ Exercices d'application 10 et 11 p. 155

Énoncé

On lance une pièce équilibrée et on veut obtenir au moins quatre fois consécutives le même résultat. Déterminer la matrice de transition représentant cette situation.

Méthode

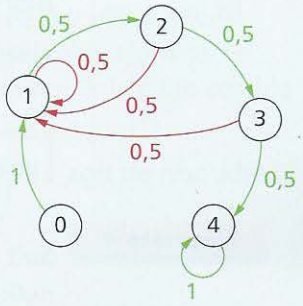
- On traduit la situation par un graphe fléché.
- On écrit la matrice de transition.

Solution

La situation comporte cinq états, de 0 à 4 : chacun représente le nombre de fois consécutives où l'on a obtenu le même résultat.

Le graphe aura donc cinq sommets et :

- au premier lancer, on passe de l'état 0 à l'état 1 avec la probabilité 1 ;
- à chaque lancer suivant :
  - pour chaque état $k = 1$ ou 2 ou 3, on passe à l'état $k + 1$ avec la probabilité 0,5 et on revient à l'état 1 avec la même probabilité ;
  - on reste à l'état 4 avec la probabilité 1.



Chaque coefficient a_{ij} pour $0 \leqslant i, j \leqslant 4$ de la matrice de transition représente la probabilité de passer de l'état j à l'état i. On a donc la matrice de transition ci-dessous :

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0{,}5 & 0{,}5 & 0{,}5 & 0 \\ 0 & 0{,}5 & 0 & 0 & 0 \\ 0 & 0 & 0{,}5 & 0 & 0 \\ 0 & 0 & 0 & 0{,}5 & 1 \end{pmatrix}.$$

Savoir-faire 2 Image d'un vecteur stochastique

→ Exercice corrigé 12 p. 155
→ Exercices d'application 13 et 14 p. 155

Énoncé

On considère la matrice M et le vecteur u suivants, où M est stochastique selon les colonnes :

$$M = \begin{pmatrix} 0{,}4 & 0 & 0{,}2 \\ 0{,}6 & 0{,}5 & 0{,}7 \\ 0 & 0{,}5 & 0{,}1 \end{pmatrix} \text{ et } u = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Vérifier que les vecteurs $M^{10}u$, $M^{20}u$, $M^{30}u$ sont bien stochastiques.

Solution

On utilise le logiciel Maxima pour calculer ces vecteurs et vérifier que la somme des coordonnées est bien égale à 1.

```
(%i2) v:(M^^10).[1,0,0];
      v[1][1]+v[2][1]+v[3][1];
                [0.1063836736]
(%o2)           [             ]
                [0.5744676384]
                [             ]
                [0.319148688 ]
(%o3) 1.0
```

```
(%i4) v:(M^^20).[1,0,0];
      v[1][1]+v[2][1]+v[3][1];
                [0.106382978723945]
(%o4)           [                 ]
                [0.574468085106036]
                [                 ]
                [0.31914893617002 ]
(%o5) 1.0
```

```
(%i6) v:(M^^30).[1,0,0];
      v[1][1]+v[2][1]+v[3][1];
                [0.106382978723404]
(%o6)           [                 ]
                [0.574468085106383]
                [                 ]
                [0.319148936170213]
(%o7) 1.0
```

B Étude asymptotique

1 Puissance d'une matrice

Propriété 3

Soit M une matrice stochastique selon les colonnes correspondant à un graphe fléché à p états.
Pour tout entier naturel k, on note $M^k = \left(m_{ij}^{(k)}\right)_{1\leqslant i,j\leqslant p}$.
Alors $m_{ij}^{(k)}$ représente la probabilité de passage de l'état j à l'état i après une marche aléatoire de k pas sur le graphe.

Démonstration
Voir exercice 50 p. 166.

Propriété 4

Soit $u^{(0)}$ le vecteur colonne stochastique ayant seulement sa j-ème coordonnée non nulle. On pose $u^{(n)} = M^n\, u^{(0)}$. Alors chaque coefficient $u_i^{(n)}$ donne la probabilité de passer de l'état j à l'état i après une marche aléatoire de exactement n pas sur le graphe.

Exemple : Soit $M = \begin{pmatrix} 0,2 & 0,7 \\ 0,8 & 0,3 \end{pmatrix}$ et $u^{(0)} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, alors $u^{(1)} = \begin{pmatrix} 0,2 \\ 0,8 \end{pmatrix}$ et il est immédiat que 0,2 est bien la probabilité de passer de l'état 0 à l'état 1 en un pas et 0,8 celle de passer de l'état 1 à l'état 2 en un pas.

2 Convergence

Propriété 5

Soit M une matrice stochastique selon les colonnes. Alors il existe un vecteur stochastique π tel que $\pi = M\pi$. π est appelé **mesure stationnaire** correspondant à la matrice M.

Note :
On rencontre aussi le terme de probabilité invariante.

Démonstration
Admise.

Remarques :
- Une mesure stationnaire n'est pas nécessairement unique.
Voir exercice 17 p. 156.
- Lorsque la suite $(M^n u)_n$ converge pour un certain vecteur stochastique u, alors elle converge vers une mesure stationnaire.
- Il se peut que la suite $(M^n u)_n$ ne converge pas pour un certain vecteur stochastique u, mais qu'il existe tout de même une mesure stationnaire. Voir exercice 16 p. 156.
- On peut démonter, mais ce sont des théorèmes difficiles, que si la matrice M ou seulement une puissance de M possède des coefficients strictement positifs, alors la mesure stationnaire est unique. Ce sont les théorèmes de Perron-Frobenius.

Note :
On dit que M est ergodique.

Savoir-faire 3 Mesure stationnaire

→ Exercice corrigé 15 p. 156
→ Exercices d'application 16 et 17 p. 156

Méthode

- On commence par tester si la suite définie par $u^{(n+1)} = Mu^{(n)}$ semble converger pour un vecteur stochastique $u^{(0)}$ choisi arbitrairement.
- Si c'est le cas, on résout l'équation $\pi = M\pi$.

Énoncé

Soit M la matrice suivante, stochastique selon les colonnes.

$$M = \begin{pmatrix} 0,4 & 0 & 0,2 \\ 0,6 & 0,5 & 0,7 \\ 0 & 0,5 & 0,1 \end{pmatrix}.$$

Déterminer, si elle existe, une mesure stationnaire de M.

Solution

Le n-ième terme de la suite définie par $u^{(n+1)} = Mu^{(n)}$ est donnée par $u^{(n)} = M^n u^{(0)}$.
On choisit $u^{(0)}$ un vecteur stochastique quelconque, par exemple celui ayant sa première coordonnée égale à 1. D'après les résultats du savoir-faire 2, la suite semble converger vers une mesure stationnaire π.
L'équation $\pi = M\pi$ s'écrit aussi $(I - M)\pi = 0$. En notant $\pi = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$, il s'agit de résoudre l'équation suivante : $\begin{pmatrix} 0,6 & 0 & -0,2 \\ -0,6 & 0,5 & -0,7 \\ 0 & -0,5 & 0,9 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = 0$.

Cette matrice n'est pas inversible, mais on peut en extraire deux équations et compléter par $a + b + c = 1$ venant du fait que π est un vecteur stochastique.
Le nouveau système, écrit sous forme matricielle est donc :

$$\begin{pmatrix} 0,6 & 0 & -0,2 \\ -0,6 & 0,5 & -0,7 \\ 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$ et la solution de cette équation est : $\pi = \begin{pmatrix} \frac{5}{47} \\ \frac{27}{47} \\ \frac{15}{47} \end{pmatrix}$.

Savoir-faire 4 Vecteur stochastique représentant la n-ième étape d'une marche aléatoire

→ Exercice corrigé 18 p. 156
→ Exercices d'application 19 p. 156

Énoncé

On lance une pièce équilibrée.
a. Quelle est la probabilité d'obtenir consécutivement au moins quatre fois le même résultat en 50 lancers.
b. À partir de combien de lancers a-t-on plus d'une chance sur deux d'obtenir consécutivement quatre fois le même résultat ?

Solution

a. La matrice de transition est celle du savoir-faire 1. L'état initial est l'état 0, on pose donc $u^{(0)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. On calcule ensuite $u^{(50)} = A^{50}u^{(0)} \approx \begin{pmatrix} 0 \\ 0,01 \\ 0,006 \\ 0,003 \\ 0,981 \end{pmatrix}$.

La probabilité recherchée est égale à un peu plus de 98 %.
b. En procédant par tâtonnements, on trouve que $u_5^{(10)} \approx 0,46$ et que $u_5^{(11)} \approx 0,5$.
Il faut donc faire au moins 11 lancers.

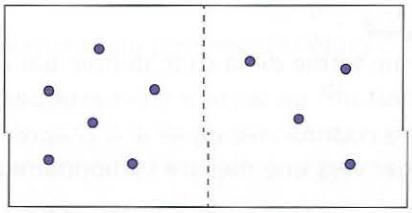
TP Algorithmique 1 Le modèle d'urnes d'Ehrenfest



Objectifs :
- Modéliser une situation.
- Utiliser un algorithme et le calcul matriciel pour émettre une conjecture.

Le but est de modéliser la répartition au cours du temps de N molécules de gaz à l'intérieur d'un récipient séparé en deux compartiments par une membrane poreuse.

Ce modèle simplifié fut proposé en 1907 par les physiciens autrichiens Tatiana et Paul Ehrenfest pour décrire en termes de physique statistique les échanges de chaleur entre deux systèmes portés initialement à températures différentes.



On considère le modèle mathématique suivant :
Deux urnes A et B et N boules numérotées de 1 à N.
Initialement, toutes les boules sont dans l'urne A. À chaque étape, on choisit au hasard un nombre entre 1 et N et on change d'urne la boule correspondante.

On ne s'intéressera ici qu'au cas $N = 2$.

1 Dénombrer et décrire les répartitions possibles dans les urnes A et B.

2 Voici un algorithme permettant de simuler 10 étapes.

```
UA est une liste contenant les nombres 1 et 2 ;
UB est une liste vide ;
Pour i = 1 à 10 par pas de 1, faire
   n est un entier aléatoire valant 1 ou 2 ;
   Si n est dans UA, alors
      Supprimer n de UA ;
      Ajouter n à UB ;
   Sinon
      Supprimer n de UB ;
      Ajouter n à UA ;
   FinSi
FinPour
Afficher UA et UB ;
```

a. Programmer cet algorithme dans un logiciel adapté.
b. Exécuter plusieurs fois cet algorithme. Que remarque-t-on ?
c. Exécuter à nouveau plusieurs fois l'algorithme en simulant 4 étapes ; 6 étapes ; 28 étapes.
Quelle conjecture peut-on faire ?
d. Même consigne avec 5 étapes ; 13 étapes ; 27 étapes.

3 **a.** Établir le graphe fléché représentant les probabilités de transition entre chaque état.
b. Vérifier que la matrice de transition associée au graphe est :

$$M = \begin{pmatrix} 0 & 0{,}5 & 0 \\ 1 & 0 & 1 \\ 0 & 0{,}5 & 0 \end{pmatrix}.$$

4 Soit $(u^{(n)})_n$ la suite de vecteurs tels que $u_i^{(n)}$ représente la probabilité d'être dans l'état i après n étapes.

a. Donner le vecteur $u^{(0)}$.

b. À l'aide d'une calculatrice ou d'un logiciel, calculer $M^n u^{(0)}$ pour un certain nombre de valeurs paires de n, puis de valeurs impaires afin de vérifier qu'au bout d'un nombre pair d'étapes, toutes les boules sont soit dans l'urne A, soit dans l'urne B et qu'au bout d'un nombre impair d'étapes, il y a une boule dans chaque urne.

c. Démontrer ce résultat par récurrence.

TP TICE 1 Suite de Fibonacci

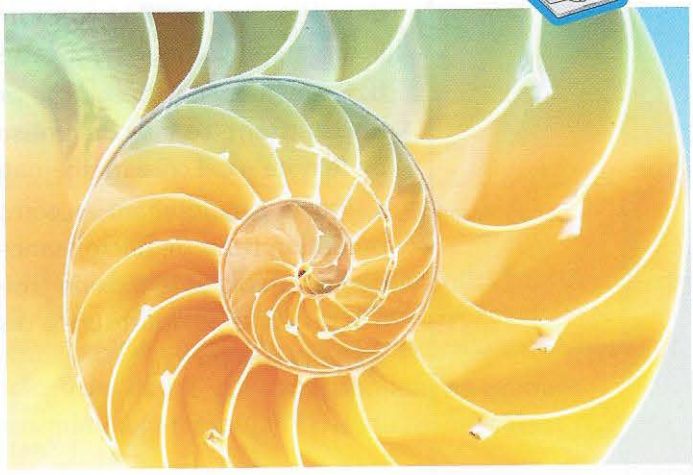
Objectif :

- *Apprendre à conjecturer et se servir de la conjecture comme piste d'investigation.*

On considère la matrice F suivante et la suite de matrices F^n définie pour tout $n > 0$.

$$F = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Le but est de trouver une formule explicite permettant de donner F^n, pour tout $n \in \mathbb{N}$.



1 **a.** Calculer quelques premiers termes de la suite (F^n) et observer l'évolution des coefficients.

b. En calculant F^{n+1} de deux manières différentes, démontrer (sans récurrence) que pour tout entier $n \geqslant 0$, $F^n{}_{1,2} = F^n{}_{2,1}$.

c. On définit la suite (u_n) pour tout entier naturel n par $u_n = F^n{}_{1,2} = F^n{}_{2,1}$. À quels autres termes de la suite correspondent les autres coefficients de F^n ?

d. En déduire la relation de récurrence (R) d'ordre 2 satisfaite par la suite (u_n). Cette suite est dite « de Fibonacci ».

e. Pour n assez grand, quelle relation semble-t-il exister entre u_{n+1} et u_n ?

2 **a.** Démontrer que si (v_n) est une suite géométrique de premier terme v_0 et de raison q vérifiant la relation (R), alors : $q^2 = q + 1$.

b. En déduire les valeurs possibles de q, que l'on notera ϕ_1 et ϕ_2, avec $\phi_1 > \phi_2$. On pourra calculer une valeur approchée de ϕ_1 et comparer ce résultat à celui de la question **1.e.**

c. Montrer que les suites $(\phi_1{}^n)$ et $(\phi_2{}^n)$ satisfont la relation (R).

d. En déduire que pour tous réels λ et μ, la suite $(\lambda\phi_1{}^n + \mu\phi_2{}^n)$ satisfait la relation (R).

e. Une suite vérifiant (R) étant déterminée par les valeurs de u_0 et u_1, déterminer le système vérifié par λ et μ, le résoudre et donner l'expression du terme général de la suite (u_n).

f. Vérifier cette expression à l'aide d'un logiciel (cf. fiche logiciel, Maxima).

3 Expliquer pourquoi la suite (u_n) ainsi définie est « presque géométrique de raison $q = \phi_1$ pour n assez grand ».

4 **a.** En déduire une formule donnant F^n pour tout entier naturel n.

b. Vérifier en effectuant quelques calculs de puissance de F.

TP TICE 2 Le modèle proies/prédateurs de Lotka-Volterra

Objectifs :
- *Modéliser l'évolution conjointe de deux suites.*
- *Linéarisation d'un problème.*

En 1926, le mathématicien Vito Volterra propose un modèle décrivant l'évolution conjointe de deux populations interagissant l'une avec l'autre : les proies et les prédateurs.
On note respectivement u_n et v_n le nombre de proies et de prédateurs l'année n.

1 Formules définissant les suites (u_n) et (v_n)

Aide

Le taux de croissance est donné par $\frac{u_{n+1} - u_n}{u_n}$.

a. En l'absence de prédateurs, les proies ont un taux de croissance positif et constant que l'on note a. Écrire mathématiquement cette affirmation.

b. De même, en l'absence de proies, les prédateurs disparaissent. Le taux de croissance est alors négatif et constant ; on le note $-c$. Écrire mathématiquement cette affirmation.

c. Prenons maintenant en compte les interactions entre les espèces. Le taux de prédation (taux de décroissance des proies) est supposé proportionnel au nombre de prédateurs et le taux de croissance du nombre de prédateurs est proportionnel à la quantité de nourriture à disposition. Vérifier que ces informations amènent au système suivant :

$$\begin{cases} u_{n+1} = u_n(1 + a - bv_n) \\ v_{n+1} = v_n(1 - c + du_n) \end{cases} \quad a,b,c,d > 0.$$

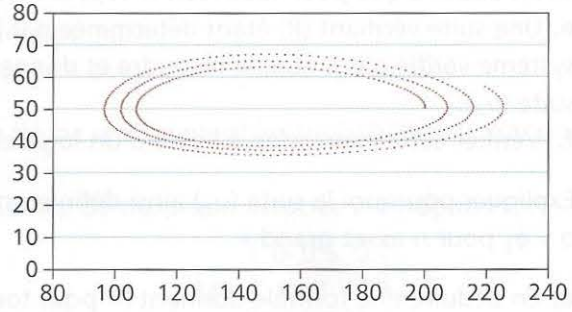
Que représentent b et d ?

2

a. Dans un tableur, simuler l'évolution conjointe des deux populations pour des effectifs initiaux de 200 proies et 50 prédateurs pendant 500 années. On prendra un taux de natalité (croissance) des proies de 0,05 ; un taux de mortalité (décroissance) des proies de 0,001 ; un taux de natalité des prédateurs de 0,0002 ; un taux de mortalité des prédateurs de 0,03.

b. Représenter sur un même graphique les évolutions des deux espèces au cours du temps. Graphiquement, qu'engendre augmentation du nombre de proies ? du nombre prédateurs ? Qu'engendre une baisse du nombre de proies ? du nombre de prédateurs ?

c. Représenter graphiquement l'évolution conjointe du nombre de proies et prédateurs, c'est-à-dire un graphique où le nombre de proies est représenté en abscisse et le nombre de prédateurs en ordonnée.



L'évolution semble périodique et la spirale semble avoir un « centre »

3 Recherche empirique de la période et de l'état d'équilibre

On parle d'état d'équilibre lorsque les deux suites sont constantes, c'est-à-dire que d'une année sur l'autre, les populations gardent les mêmes nombres d'individus.

a. Voici un algorithme (ou script), écrit dans les logiciels de géométrie dynamique CaRMetal et GeoGebra, permettant de visualiser **dynamiquement** l'évolution conjointe des deux espèces pendant 500 ans.

```
proies = 200;
pred = 50;

p = Point("A"+0, proies, pred);
SetPointType(p,"circle");

for(i=1; i<=500; i=i+1){
    proies = "x_p*(1 - b*y_p + a)";
    pred = //formule à compléter
    p = //création du point Ai
    SetPointType(p, "cross");
}
```

CarMetal

```
proies = 200 ;
pred = 50;

ggbApplet.evalCommand("A_{0}=("+proies+","+pred+")");

for(i=1; i<=500; i=i+1){
  proies = "x(A_{"+(i-1)+"})*(1 - b*y(A_{"+(i-1)+"})+a)";
  pred = /* formule à compléter */
  /* création du point Ai */
  ggbApplet.setLabelVisible("A_{"+i+"}", false);
  ggbApplet.setPointStyle("A_{"+i+"}", 3);
}
```

GeoGebra 4

Aide

On créera d'abord quatre curseurs a, b, c et d afin de pouvoir modifier facilement les paramètres.
On pourra se reporter aux pages http://db-maths.nuxit.net/CaRMetal/carJSdoc/index.html et http://wiki.geogebra.org/en/Reference:JavaScript pour une aide sur la syntaxe utilisée.

b. Lancer le script, puis relever les indices des points qui correspondent au premier, deuxième puis troisième retour approximatif à l'état initial. En déduire une valeur approchée de la période.

c. Afficher les coordonnées du point représentant l'état initial puis déplacer ce point afin d'obtenir un état d'équilibre et relever ses coordonnées.

4 Recherche théorique de l'état d'équilibre

a. Traduire mathématiquement le fait que les deux suites sont constantes.

b. Résoudre le système obtenu afin de trouver les deux états d'équilibre possibles. Vérifier que l'un d'entre eux coïncide bien avec celui trouvé empiriquement.

c. Dans le tableur, vérifier que ces données donnent bien deux suites constantes.

5 Linéarisation du problème autour du point d'équilibre

a. En posant $U_n = u_n - \frac{c}{d}$ et $V_n = v_n - \frac{a}{b}$, démontrer que le système de la question **1.c.** est équivalent au système suivant :

$$(S_1) \Leftrightarrow \begin{cases} U_{n+1} = U_n - \dfrac{bc}{d} V_n - bU_nV_n \\ V_{n+1} = \dfrac{ad}{b} U_n + V_n + dU_nV_n \end{cases}$$

b. Étant donné que U_n et V_n sont proches de 0 (par exemple 0,01), montrer par des considérations d'ordre de grandeur que le produit U_nV_n est négligeable par rapport à U_n ou V_n. En déduire une approximation de (S_1) et traduire ce nouveau système matriciellement, où l'on notera M la matrice utilisée.

c. On dit qu'il y a retour à l'état initial lors de la n-ième année lorsque $U_n = U_0$ et $V_n = V_0$. Dans ce cas-là, que peut-on dire de M^n ? Vérifier qu'en prenant pour valeur de n la période trouvée empiriquement à la question **3.c.**, on obtient approximativement une telle matrice.

Maîtriser le cours

Matrices stochastiques

1 **Vrai ou faux**

a. Une matrice ne peut être stochastique que selon les lignes ou bien que selon les colonnes.

b. La matrice unité est stochastique.

c. Si une matrice est stochastique selon les colonnes, alors la somme des coefficients de chaque colonne est égale à 1.

d. Si dans une matrice, la somme des coefficients de chaque colonne est égale à 1, alors la matrice est stochastique selon les colonnes.

e. Si M et P sont deux matrices stochastiques selon les colonnes telles que le produit MP soit calculable, alors il en est de même pour PM.

2 **QCM**

1. Soit M une matrice de taille nxp, stochastique selon les colonnes, alors :

a. pour tout j, $\sum_{i=1}^{n} m_{ij} = 1$. **b.** pour tout j, $\sum_{i=1}^{p} m_{ij} = 1$.

c. pour tout i, $\sum_{j=1}^{n} m_{ij} = 1$. **d.** pour tout i, $\sum_{j=1}^{p} m_{ij} = 1$.

2. Même question avec M stochastique selon les lignes.

3 **Vrai ou faux**

Dire si les propositions suivantes sont vraies ou fausses. Si elles sont fausses, proposer un contre-exemple.
Soit $v = Au$.

a. Si u et v sont des vecteurs stochastiques, alors la matrice A est stochastique selon les colonnes.

b. Si A est stochastique selon les colonnes et u est un vecteur stochastique, alors v aussi.

c. Si A est stochastique selon les lignes et u est un vecteur stochastique, alors v aussi.

4 **QCM**

1. Si T est la matrice de transition associée à un graphe, telle que t_{ij} est la probabilité de passage de l'état j à l'état i, alors T est stochastique :

a. selon les colonnes ; **b.** selon les lignes.

2. Même question lorsque t_{ij} est la probabilité de passage de l'état i à l'état j.

5 **Vrai ou faux**

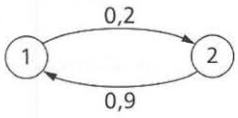
a. Une matrice stochastique est carrée.

b. Une matrice stochastique associée à un graphe est carrée.

c. La matrice associée à un graphe possédant n sommets est de taille n.

d. La matrice associée au graphe ci-contre est :

$$M = \begin{pmatrix} 0,2 & 0,9 \\ 0,8 & 0,1 \end{pmatrix}.$$



Étude asymptotique

6 **QCM**

1. La mesure stationnaire π d'une matrice stochastique M selon les colonnes satisfait la relation :

a. $\pi = M\pi$. **b.** $\pi = \pi M$.

2. Même question avec M stochastique selon les lignes.

3. Soit $M = \begin{pmatrix} 0,6 & 0,1 \\ 0,4 & 0,9 \end{pmatrix}$. Alors une mesure invariante de M est :

a. $\pi = \begin{pmatrix} 0,2 \\ 0,8 \end{pmatrix}$. **b.** $\pi = \begin{pmatrix} 0,8 \\ 0,2 \end{pmatrix}$.

c. $\pi = \begin{pmatrix} 0,2 & 0,8 \end{pmatrix}$. **d.** $\pi = \begin{pmatrix} 0,8 & 0,2 \end{pmatrix}$.

4. Même question avec la matrice $P = \begin{pmatrix} 0,6 & 0,4 \\ 0,1 & 0,9 \end{pmatrix}$.

7 **Vrai ou faux**

a. La mesure stationnaire d'une matrice stochastique n'est pas obligatoirement stochastique.

b. Si $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, alors $\pi = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $\mu = \begin{pmatrix} 0,5 \\ 0,5 \end{pmatrix}$ sont deux mesures stationnaires de M.

c. Si M admet une mesure stationnaire, alors elle est unique.

d. Si $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, alors tout vecteur stochastique est mesure invariante de M.

8 **Vrai ou faux**

M est une matrice stochastique selon les colonnes et u un vecteur colonne stochastique.

a. Pour obtenir les probabilités de passage d'une marche aléatoire en k pas, on doit calculer M^k.

b. Pour obtenir les probabilités de passage de l'état 1 à n'importe quel autre état pour une marche en k pas, on doit calculer $M^k u$, avec $u_1 = 0$.

c. Le i-ème coefficient de $M^n u$ donne la probabilité d'être dans l'état i après une marche aléatoire de n pas sur le graphe pour n'importe quel vecteur stochastique u.

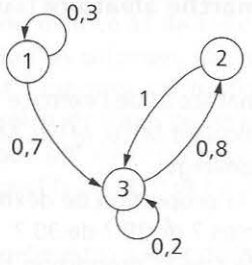
Appliquer les capacités attendues

Matrices stochastiques

Déterminer une matrice de transition

[savoir-faire 1 p. 147]

9 Donner la matrice de transition associée au graphe suivant :



10 Le glucose admet deux isomètres, le dextrose et le lévulose. Lors d'une réaction chimique, une partie du dextrose se transforme en lévulose et vice-versa. Lors d'une unité de temps, on a :

- 60 % des molécules de dextrose qui se transforment en lévulose ;
- 35 % des molécules de lévulose ne se transforment pas.

a. Traduire la situation par un graphe fléché. On prendra comme convention que l'état 1 correspond au dextrose et que l'état 2 correspond au lévulose.

b. Donner la matrice de transition, notée M.

11 L'ADN est une séquence de nucléotides, composés entre autre d'adénine (1), de thymine (2), de guanine (3) et de cytosine (4).

On possède la matrice de transition suivante, représentant les probabilités de successions des quatre composés azotés :

$$M = \begin{pmatrix} 0,3 & 0,17 & 0,25 & 0,32 \\ 0,21 & 0,3 & 0,2 & 0,3 \\ 0,29 & 0,3 & 0,3 & 0,08 \\ 0,2 & 0,23 & 0,25 & 0,3 \end{pmatrix}.$$

1. Chaque coefficient m_{ij} représente la probabilité de succession de :

a. la base azotée j avec la base azotée i ;

b. la base azotée i avec la base azotée j ;

2. Quelles sont les probabilités de trouver :

a. de l'adénine suivie de cytosine ?

b. de la guanine suivie d'adénine ?

c. de thymine précédée d'adénine ?

d. de cytosine précédée de thymine ?

3. Quelle est la succession la moins probable ? la plus probable ?

Image d'un vecteur stochastique

[savoir-faire 2 p. 147]

12 Soit M une matrice stochastique selon les lignes de taille nxp et u un vecteur colonne stochastique de taille p pour lequel il existe un réel λ tel que $Mu = \lambda u$.

1. Quel est le signe de λ ? Justifier.

2. Retranscrire mathématiquement le fait que M soit stochastique selon les lignes.

3. On pose $v = Mu$.

a. Pour tout $i = 1 \ldots n$, donner la formule permettant de calculer v_i.

b. Notons u_{i_0} le plus grand des coefficients de u. Déduire de la question **a.** que pour tout $i = 1 \ldots n$, $v_i \leqslant u_{i_0}$.

c. En déduire que $\lambda \leqslant 1$.

13 Soit M une matrice stochastique selon les colonnes de taille 2 telle que :

$$M\begin{pmatrix} 0,5 \\ 0,5 \end{pmatrix} = \begin{pmatrix} 0,45 \\ 0,55 \end{pmatrix}.$$

1. Démontrer que l'on ne peut pas en déduire les coefficients de M.

2. On donne alors l'information supplémentaire :

$$M\begin{pmatrix} 0,1 \\ 0,3 \end{pmatrix} = \begin{pmatrix} 0,11 \\ 0,29 \end{pmatrix}.$$

Déterminer les coefficients de M.

14 L'entreprise LCC commercialise un produit et souhaite augmenter ses ventes. Elle lance une campagne de publicité et une étude statistique révèle qu'au bout d'une semaine :

- x % des clients qui achetaient à la concurrence achètent maintenant la marque LCC ;
- y % des clients qui achetaient la marque LCC achètent maintenant à la concurrence.

1. D'après la matrice de transition suivante, donner les valeurs de x et y (LCC est l'état 1 et la concurrence l'état 2) :

$$M = \begin{pmatrix} 0,9 & 0,2 \\ 0,1 & 0,8 \end{pmatrix}.$$

2. Cette semaine, il y a 30 % d'acheteurs de la marque LCC.

a. Donner le vecteur stochastique u représentant les parts de marché.

b. Calculer M^3u et en déduire la proportion de vente au bout de 3 semaines de publicité. La campagne fonctionne-t-elle ?

Étude asymptotique

Mesure stationnaire [savoir-faire 3 p. 149]

15 On considère la matrice M suivante :

$$M = \begin{pmatrix} 0,4 & 0,65 \\ 0,6 & 0,35 \end{pmatrix}.$$

a. Déterminer empiriquement une mesure stationnaire de M. On prendra pour cela le vecteur stochastique $u^{(0)}$ de son choix.

b. Déterminer cette mesure stationnaire par le calcul.

16 On considère la matrice M suivante, stochastique selon les colonnes :

$$M = \begin{pmatrix} 0 & 0,5 & 0,2 & 0 \\ 1 & 0 & 0 & 0,7 \\ 0 & 0 & 0 & 0,3 \\ 0 & 0,5 & 0,8 & 0 \end{pmatrix}.$$

1. Déterminer une mesure stationnaire π de M.

2. On considère les deux vecteurs colonnes suivants :

$$u = \begin{pmatrix} 0,5 \\ 0,5 \\ 0 \\ 0 \end{pmatrix} \text{ et } v = \begin{pmatrix} 0,5 \\ 0 \\ 0 \\ 0,5 \end{pmatrix}.$$

a. Vérifier que la suite $(M^n u)_n$ semble converger vers π.

b. Vérifier que la suite $(M^n v)_n$ ne semble pas converger.

17 On considère la matrice M suivante, stochastique selon les colonnes :

$$M = \begin{pmatrix} 0,25 & 0 & 0 & 0 \\ 0,25 & 1 & 0 & 0 \\ 0,25 & 0 & 0,5 & 1 \\ 0,25 & 0 & 0,5 & 0 \end{pmatrix}.$$

1. a. En procédant comme dans le savoir-faire 3, vérifier que M admet les deux mesures stationnaires suivantes :

$$\pi = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ et } \mu = \begin{pmatrix} 0 \\ 0 \\ 2/3 \\ 1/3 \end{pmatrix}.$$

b. En déduire que toute combinaison linéaire de la forme $v = a\pi + b\mu$ vérifie $v = Mv$.

c. Comment faut-il choisir a et b pour que v soit une mesure stationnaire ? En déduire le nombre de mesures stationnaires de la matrice M.

2. a. À l'aide d'un logiciel ou d'une calculatrice, conjecturer la limite v de la suite $(M^n u)$, où seule la première coordonnée de u est non nulle et vaut 1.

b. Déterminer les valeur de a et b telles que $v = a\pi + b\mu$

c. Mêmes questions avec un vecteur u ayant sa seule deuxième, puis troisième, puis quatrième coordonnée non nulle et égale à 1.

d. Mêmes questions pour un vecteur u tel que $u_2 = u_4 = 0,5$.

Vecteur stochastique représentant la n-ième étape d'une marche aléatoire [savoir-faire 4 p. 149]

18 On reprend la matrice M de l'exercice 10 p. 155

1. Vérifier, en calculant $M^{10}u$, $M^{30}u$, $M^{40}u$ que la suite $(M^n u)$ semble converger.

2. a. Quelle est la proportion de dextrose au bout de 10 unités de temps ? de 20 ? de 30 ?

b. Quelle semble être la proportion limite de chacun des deux isomères du glucose ?

19 **Erreur de transmission**

Un message codé en binaire est transmis à travers un réseau comportant plusieurs relais. À chaque relais, chaque bit est transmis avec une probabilité d'erreur. Une étude statistique donne les probabiltiés d'erreurs suivantes :

- le bit 0 est transmis en 1 avec la probabilité $a = 0,02$;
- le bit 1 est transmis en 0 avec la probabilité $b = 0,01$.

1. a. Traduire la situation par un graphe fléché.

b. Donner la matrice de transition associée, notée M.

2. On note $u^{(n)}$ le vecteur colonne défini pour $n \geqslant 0$ par :

$$u^{(n)} = \begin{pmatrix} P \text{ (au } n\text{-ième relais, le bit est 0)} \\ P \text{ (au } n\text{-ième relais, le bit est 1)} \end{pmatrix}$$

Exprimer $u^{(n+1)}$ en fonction de $u^{(n)}$, puis $u^{(n)}$ en fonction de $u^{(0)}$.

3. On suppose que l'on transmet le bit 1.

a. Donner $u^{(0)}$.

b. Quelle est la probabilité d'avoir le bit 1 au 3e relais, arrondie à 10^{-2} ?

c. Démontrer par récurrence que, pour tout n, $u_2^{(n)} > \frac{2}{3}$, puis en déduire que la suite $\left(u_2^{(n)}\right)$ est décroissante.

d. On souhaite que la probabilité de recevoir le même bit soit au moins égale à 90 %. Quel est le nombre maximum de relais ?

4. a. On suppose maintenant que l'on transmet le bit 0. Quel est le nombre maximum de relais pour que la probabilité de recevoir le même bit soit au moins égale à 90 % ?

b. En déduire la taille maximum du réseau.

Pour l'étude théorique, se reporter à l'exercice **46** p. 164.

Manipulation de matrices stochastiques

20 **Caractérisation d'une matrice stochastique**

Soit u un vecteur colonne stochastique non nul dont tous les coefficients sont égaux. Démontrer que M est une matrice stochastique selon les colonnes si, et seulement si, $Mu = u$.

21 **Inverse d'une matrice stochastique**

On considère une matrice M de taille n, inversible et stochastique selon les colonnes. On voudrait savoir si la matrice $P = M^{-1}$ est aussi stochastique et si c'est le cas, si elle l'est selon les lignes ou les colonnes.

1. On rappelle que $MP = I$ et on note m_{ij}, p_{ij} et I_{ij} les coefficients respectifs de M, P et I à la i-ème ligne et j-ème colonne.

a. Pour tout j, quelle est la valeur de la somme $\sum_{i=1}^{n} I_{ij}$?

b. Pour tous i et j, rappeler la formule donnant le coefficient I_{ij} en fonction des coefficients de M et de P.

c. Déduire de **a.** et **b.** que pour tout j, $\sum_{k=1}^{n} p_{kj} = 1$.

d. Conclure.

2. Tenter de refaire la démonstration mais en prenant $PM = I$ et constater qu'elle ne peut aboutir.

22 **a.** En se basant sur la démonstration de l'exercice précédent, démontrer que si v est un vecteur stochastique et A une matrice stochastique selon les colonnes, alors le vecteur u tel que $v = Au$ est aussi stochastique.

b. Ce résultat est-il plus facile à démontrer si l'on suppose la matrice A inversible ? Expliquer pourquoi.

23 Démontrer que si M est une matrice stochastique dont toutes les colonnes sont identiques, alors $M^2 = M$.

Aide

Retranscrire l'hypothèse par une égalité.

24 **Convergence d'une matrice stochastique**

Aide

Dans cet exercice, on pourra utiliser le théorème de la division euclidienne des polynômes :
« Si A et B sont deux polynômes, alors il existe un unique couple $(Q ; R)$ de polynômes tels que pour tout réel x, $A(x) = B(x)Q(x) + R(x)$, avec $\deg(R) < \deg(B)$ ».
On pourra aussi utiliser la propriété suivante :
« Si P et Q sont deux polynômes et A une matrice, alors $(PQ)(A) = P(A)Q(A)$ »

La forme générale d'une matrice stochastique selon les colonnes de taille 2 est :

$$A = \begin{pmatrix} a & 1-b \\ 1-a & b \end{pmatrix}, \text{ où } a, b \in [0 ; 1].$$

Le but de l'exercice est de déterminer si la suite (A^n) converge.

1. Calculer A^n dans le cas $a = b = 1$. Conclure.

2. Même consigne avec $a = b = 0$.

3. On suppose maintenant $(a ; b) \neq (1 ; 1)$ et $(a ; b) \neq (0 ; 0)$.

a. Soit $P(x) = (x - 1)(x - (a + b - 1))$.
Montrer que $P(A) = (A - I)(A - (a + b - 1)I) = 0$.

b. Dans la division euclidienne de x^n par P, démontrer que le reste $R(x)$ s'écrit $mx + p$, où m et p sont deux nombres réels.

c. Quelles sont les racines du polynôme P ? En déduire que m et p satisfont le système :

$$\begin{cases} 1 = m + p \\ (a + b - 1)^n = m(a + b - 1) + p \end{cases}.$$

Résoudre ce système par la méthode de votre choix.

d. En déduire que pour tout n, on a :

$$A^n = \frac{1}{a + b - 2} M_n,$$

où M_n est une matrice à déterminer.

e. Donner un encadrement de $a + b - 1$.

f. En déduire que la suite (A^n) converge vers :

$$\frac{1}{a + b - 2} \begin{pmatrix} b-1 & b-1 \\ a-1 & a-1 \end{pmatrix}.$$

25 **Puissance d'une matrice**

On considère la matrice $M = \begin{pmatrix} 146 & 84 \\ -245 & -141 \end{pmatrix}$. On désire établir une formule permettant de donner, pour tout entier naturel n, la valeur de M^n.

1. On pose $P = \begin{pmatrix} 3 & 4 \\ -5 & -7 \end{pmatrix}$ et $D = \begin{pmatrix} 6 & 0 \\ 0 & -1 \end{pmatrix}$.

Vérifier que $M = PDP^{-1}$.

2. **a.** Calculer les premières puissances de D, établir une conjecture et la démontrer par récurrence.

b. À l'aide d'un raisonnement par récurrence, démontrer que pour tout entier naturel n : $M^n = PD^nP^{-1}$.

c. En déduire les quatre formules donnant chacun des coefficients de M.

26 **Suite de vecteurs stochastiques**

On reprend la suite de vecteurs définie dans l'activité 2 p. 144 :

$$\mu^{(n+1)} = (1 - c)M\mu^{(n)} + cE, \text{ où } E = \begin{pmatrix} 1/8 \\ \vdots \\ 1/8 \end{pmatrix}.$$

On souhaite montrer que si $\mu^{(n)}$ est un vecteur stochastique, alors $\mu^{(n+1)}$ aussi. On utilisera seulement le fait que M est une matrice stochastique de taille 8 selon les colonnes, sans se préoccuper des valeurs des coefficients.

1. **a.** On pose $v^{(n)} = M\mu^{(n)}$. Donner la formule de la i-ème coordonnée $v_i^{(n)}$ de ce vecteur.

b. Démontrer que $\sum_{i=1}^{8} v_i = 1$.

Aide

On pourra s'aider de la démonstration de la propriété 2 p. 146

2. a. Écrire la formule donnant la i-ème coordonnée du vecteur $\mu^{(n+1)}$.

b. Démontrer que $\mu^{(n+1)}$ est un vecteur stochastique.

Marches aléatoires

27 Évolution d'une population

On considère une population d'êtres unicellulaires, que l'on conserve dans une enceinte close. Chacun de ces êtres peut se trouver dans deux états physiologiques notés A et B. On désigne par a_n et b_n les effectifs, en milliers d'individus, des deux populations à l'instant n.

Des observations ont montré que :

- 95 % des individus se trouvant dans l'état A à l'instant n n'en changent pas à l'instant $n+1$;
- 80% des individus se trouvant dans l'état B à l'instant n n'en changent pas à l'instant $n+1$.

1. a. Écrire a_{n+1} en fonction de a_n et b_n.

b. Écrire b_{n+1} en fonction de a_n et b_n.

2. On considère qu'à l'instant initial, $a_0 = 375$ pour un effectif total de 500 000 individus.

a. En déduire la valeur de b_0.

b. Sur tableur ou calculatrice, calculer les 31 premiers termes de ces suites.

c. Que peut-on conjecturer ?

3. Pour tout entier n, on pose $u_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

a. Déduire de la question **1.** la matrice M telle que $u_{n+1} = Mu_n$.

b. Sans faire de calculs supplémentaires, pourquoi peut-on conjecturer l'existence d'une mesure stationnaire pour M.

c. Déterminer cette mesure stationnaire.

d. En déduire la proportion limite d'individus dans l'état A et dans l'état B.

4. On pose $D = \begin{pmatrix} 0{,}75 & 0 \\ 0 & 1 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 1 \\ -1 & 0{,}25 \end{pmatrix}$.

a. Vérifier que $M = PDP^{-1}$.

b. En déduire la forme général de M^n.

c. En déduire le nombre d'individus dans chaque état lorsque $n = 50$; $n = 100$.

5. Quel est l'intérêt, informatiquement parlant, de calculer la puissance n-ième de M à partir de la forme PDP^{-1} plutôt que de faire brutalement le calcul à partir de la forme trouvée en **3.a.** ?

28 Évolution d'une population 2

On reprend l'énoncé de l'exercice 10 p. 155 et la matrice M correspondante.

1. Préliminaires

On rappelle la formule suivante, pour tout entier $n \geqslant 0$, où x et y sont deux réels :

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \Leftrightarrow \text{(F)}.$$

a. Donner la formule pour $(x-y)^n$.

b. En calculant $(1-1)^n$ de deux manières différentes, démontrer que $\sum_{k=0}^{n-1} \binom{n}{k} (-1)^k = (-1)^{n-1}$.

2. On pose $P = \begin{pmatrix} 0{,}52 & 0{,}52 \\ 0{,}48 & 0{,}48 \end{pmatrix}$ et $Q = 4(P - M)$.

a. Calculer quelques puissances successives de P, émettre une conjecture et la démontrer.

b. Même question pour Q.

c. Vérifier que M et P commutent, c'est-à-dire que $MP = PM$. Donner la valeur de ce produit.

d. En déduire que pour tout entier $k \geqslant 0$, $PM^k = P$.

3. a. Sachant que la formule (F) est aussi valable pour deux matrices qui commutent, démontrer que :

$$Q^n = 4^n((-1)^{n-1}P + (-1)^n M^n)$$

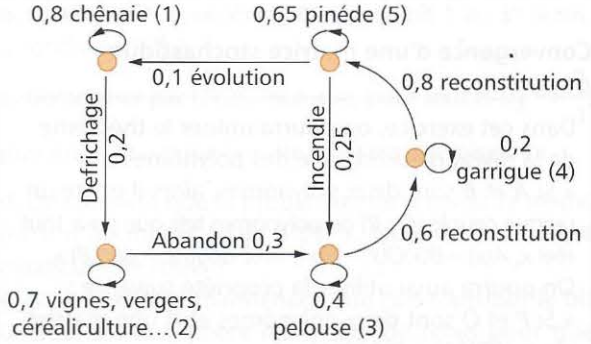
b. En déduire la formule donnant M^n pour tout entier naturel n.

29 Évolution d'une succession végétale

On considère une succession typique du midi de la France, composée potentiellement de pinède, chênaie, exploitation agricole, pelouse ou garrigue.

Chaque parcelle peut subir des transformations, qu'elles soient d'ordre accidentel, naturel, ou volontaire.

Grâce aux statistiques, on a pu approximer la probabilité qu'a l'écosystème de passer d'un état à un autre.



On voudrait savoir si, étant donné une composition initiale, le système pourrait se rapprocher d'un modèle stationnaire au fil du temps.

1. a. On numérote les états de la manière suivante : chênaie (1), exploitation agricole (2), pelouse (3),

garrigue (4), pinède (5). Donner la matrice M de transition où chaque coefficient m_{ij} représente la probabilité de transition de l'état i à l'état j.

b. M est-elle une matrice stochastique selon les lignes ou les colonnes ?

c. Comment aurait-on du définir les coefficients pour avoir une matrice stochastique selon les colonnes ?

2. a. On suppose que l'état initial du système est représenté par le vecteur ligne :

$$V_0 = (0{,}1 \;\; 0{,}3 \;\; 0{,}2 \;\; 0{,}3 \;\; 0{,}1).$$

Pour calculer V_1, on doit calculer V_0M, mais doit-on prendre la matrice M stochastique selon les lignes ou les colonnes ?

b. Même question dans le cas où l'on aurait choisi de prendre V_0 en tant que vecteur colonne.

3. a. Calculer V_{20}, V_{30}, etc. à l'aide d'un logiciel ou d'une calculatrice. La suite $(V_n)_n$ semble-t-elle converger ?

b. Résoudre l'équation $V = VM$ à l'aide d'un logiciel et en déduire la proportion de chaque état végétal.

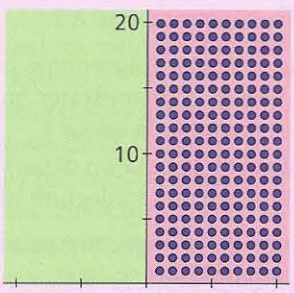
Algorithmique

30 Urne d'Ehrenfest



On se propose de visualiser à l'aide d'un algorithme l'évolution de 200 particules dans le modèle des urnes d'Ehrenfest.

On se place dans un repère (O ; I, J). Chaque particule est alors représentée par un point. La partie du plan dont les abscisses sont positives correspondra à l'urne A tandis que l'urne B correspondra aux abscisses négatives. À l'instant initial, toutes les particules sont dans A.



1. Placement des particules

On veut faire 20 rangées de 10 points en utilisant la boucle suivante :

```
Pour i = 0 à 199, faire
   x = … ;
   y = … ;
   Placer le point i de coordonnées (x, y) ;
FinPour
```

a. On veut que les points n° 0 ; 10 ; 20, etc. aient une abscisse égale à 1, que les points n° 1 ; 11 ; 21, etc. aient une abscisse égale à 2, etc. Déterminer le contenu de la variable `x`.

b. On veut que les points n° 0 à 9 aient une ordonnée égale à 1, que les points de 10 à 19 aient une ordonnée égale à 2, etc. Déterminer le contenu de la variable `y`.

c. Écrire cet algorithme dans le logiciel de géométrique dynamique CaRMetal ou GeoGebra et le tester.

2. Simulation de l'échange

Écrire un algorithme répétant $N = 5\,000$ fois l'opération suivante : choisir un point au hasard parmi les 200, numérotés de 0 à 199, et modifier son abscisse en son opposée.

3. Amélioration de l'algorithme

On désire connaître, à chaque instant le nombre de boules dans chaque « urne ». Pour cela, on stockera ces nombres dans deux variables UA et UB.

a. Comment doivent-être initialisée ces variables ?

b. Compléter l'algorithme pour que les valeurs de ces variables soient mises à jour après chaque échange.

4. On veut utiliser un point C, permettant de visualiser dynamiquement l'évolution de la proportion de particules dans l'urne A. Pour cela, l'abscisse de C représentera le nombre d'échanges effectués et son ordonnée la proportion de particules dans l'urne A. On complètera alors l'algorithme avec le code suivant :

```
Déplacer le point C à (i/100, …) ;
```

a. Pourquoi choisir i/100 comme abscisse et non pas i ?

b. Compléter l'ordonnée.

c. Activer la trace du point C, langer l'algorithme et visualiser l'évolution. Que constate-t-on ?

31 Gestion d'un hôpital

Dans un hôpital, les patients peuvent se trouver dans l'une des quatre services suivants : soins réguliers (1), chirurgie (2), soins intensifs (3), congé (4).

On résume dans le tableau suivant la probabilité de changement de service de chaque patient :

→	Soins réguliers	Chirurgie	Soins intensifs	Congé
Soins réguliers	0,6	0,2	0	0,2
Chirurgie	0,1	0	0,8	0,1
Soins intensifs	0,5	0	0,33	0,17
Congé	0	0	0	1

C'est-à-dire qu'un patient se trouvant en soins réguliers se retrouve le jour suivant en soins réguliers avec une probabilité de 0,6, en chirurgie avec une probabilité de 0,2 et sort avec une probabilité de 0,2.

On considère la matrice M de taille 4 reprenant ces mêmes informations.

1. a. La matrice M est-elle stochastique selon les lignes ou les colonnes ?

b. On suppose qu'un certain jour, la répartition des patients dans les quatre services est 12 ; 5 ; 6 ; 3. Devra-t-on utiliser un vecteur V en ligne ou en colonne pour stocker ces informations ?

c. Devra-t-on calculer VM ou bien MV pour connaître le nombre de patients le jour suivant ?

d. Donner le nombre de patients dans tous les services, le jour suivant.

2. Dans cet hôpital, rentrent chaque jour 10 nouveaux patients en soins réguliers. On note $X_0 = (10\ 0\ 0\ 0)$ la répartition des patients le jour de l'ouverture et X_n la répartition après n jours.

a. Écrire X_1 en fonction de X_0 et M.

b. Écrire X_2 en fonction de X_1 et M, puis en fonction de X_0 et M.

c. Démontrer par récurrence que pour tout entier naturel n :

$$X_n = X_0 \sum_{k=0}^{n} M^k.$$

d. À l'aide d'un logiciel ou d'une calculatrice, déterminer X_{30}, X_{40}, X_{50}. En déduire le nombre de lits que l'hôpital doit prévoir dans chaque service.

Aide

Avec Maxima, on utilisera le menu « Calculs/ Calculer la somme... »

32 Marche aléatoire sur un segment

On se déplace sur le segment ci-dessous selon la matrice de transition suivante :

$$M = \begin{array}{c} \\ \text{A} \\ \text{I} \\ \text{B} \end{array} \begin{array}{c} \begin{array}{ccc} \text{A} & \text{I} & \text{B} \end{array} \\ \begin{pmatrix} 0 & 0{,}5 & 0 \\ 1 & 0 & 1 \\ 0 & 0{,}5 & 0 \end{pmatrix} \end{array}$$



1. Compléter le graphe avec les probabilités de passage de chaque état à un autre.

2. a. Calculer quelques puissances successives de M et émettre une conjecture sur les formules donnant les coefficients de M^n.

b. Démontrer cette conjecture par récurrence.

3. I'll be back

En partant d'un état donné e (A, B ou I), on souhaite connaître le nombre de pas nécessaires pour y revenir pour la première fois. On note X_e la variable aléatoire donnant ce nombre de pas et on souhaite établir la loi de probabilité de X_e. Pour cela, on se propose d'abord de la découvrir empiriquement.

Pour cela, on attribue à l'état A la valeur –1, à l'état B la valeur 1, à l'état I la valeur 0 et on désigne par `e` la variable contenant la valeur de l'état actuel.

a. Si `e` = 0, quelle est la prochaine valeur de `e` possible ?

b. Même question avec `e` = 1, puis `e` = –1.

c. Un nombre aléatoire `alea` est un réel compris entre 0 et 1. Déterminer les entiers a, b et c pour que la valeur de la variable `a*Ent(b*alea) - c` soit égale à –1 ou 1.

Aide

Ent est la fonction partie entière : pour tout réel x, Ent(x) est le plus grand entier inférieur ou égal à x. Par exemple Ent(6,9) = 6 ; Ent(–2,7) = – 3.

Compléter alors l'algorithme suivant pour un départ et un retour à la valeur 1 (état B) :

```
e = ... ;
Faire
   Si (e == 0) alors
      e = ...;
   Sinon
      e = ...;
   FinSi
   Afficher (e) ;
TantQue (e ! = ...)
```

d. Exécuter cet algorithme pour vérifier qu'il fonctionne correctement.

e. Compléter l'algorithme afin de compter et afficher le nombre de fois que la boucle a été exécutée.

f. Encapsuler cet algorithme dans une boucle `Pour` afin de compter le nombre de retour en 2 étapes, c'est-à-dire le nombre de fois que la boucle a été exécutée 2 fois.

g. En déduire la fréquence de retour en 2 pas.

h. Modifier (légèrement) l'algorithme pour déterminer la fréquence de retour en 3 pas, 4 pas, 5 pas, etc. Émettre une conjecture sur $P(X_B = n)$, où n est un entier naturel supérieur ou égal à 2.

4. a. De même, exécuter l'algorithme pour un départ et retour à la valeur –1 et constater que les résultats sont les mêmes que pour la valeur 1.

b. Exécuter l'algorithme pour un départ et un retour à la valeur 0 et émettre une conjecture sur $P(X_I = n)$.

5. Démonstration de la conjecture pour l'état I.

Si e_1 et e_2 sont deux états, on note $(e_1 \xrightarrow{n} e_2)$ l'événement : « passer de l'état e_1 à l'état e_2 en n pas ». La marche aléatoire étant « sans mémoire », ces événements sont indépendants. De plus, on ne spécifie pas n lorsqu'il est égal à 1.

a. En remarquant que les événements (I → A) et (I → B) forment une partition de l'espace de probabilité, calculer $P(X_I = 2)$.

b. En déduire la loi de probabilité de X_I.

6. Démonstration de la conjecture pour les états A et B. Les états A et B étant symétriques, on fait la démonstration uniquement pour l'état A.

a. Expliquer pourquoi $P(X_A = n) = 0$ pour n impair.

b. Déterminer $P(X_A = 2)$.

c. Expliquer pourquoi

$$P(X_A = 4) = P(A \xrightarrow{2} B) \times P(B \xrightarrow{2} A).$$

Déterminer $P(A \xrightarrow{2} B)$ puis en déduire la valeur de $P(X_A = 4)$.

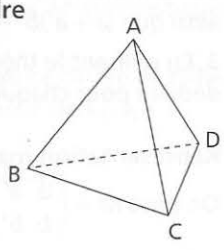
d. Pour $n \geqslant 3$, expliquer pourquoi

$$P(X_A = 2n) = P(A \xrightarrow{2} B) \times P(B \xrightarrow{2n-4} B \text{ sans revenir en A}) \times P(B \xrightarrow{2} A).$$

e. À l'aide d'un raisonnement par récurrence, déterminer $P(B \xrightarrow{2n} B$ sans revenir en A) pour tout $n \geqslant 1$ et conclure.

33 Marche aléatoire sur un tétraèdre

On se déplace sur les sommets du tétraèdre ci-dessous sans jamais rester deux fois de suite au même sommet :



1. a. À partir d'un sommet donné, quels sommets peut-on atteindre ?

b. En déduire les coefficients nuls de la matrice M de transition puis déterminer cette matrice, sachant que l'on fait l'hypothèse d'une marche aléatoire équiprobable.

2. Calculer quelques puissances successives de M à l'aide d'un logiciel.

On remarquera qu'il y a deux types de coefficients. Notons u_n les coefficients diagonaux de M^n et v_n les autres.

a. Quel lien semble-t-il exister entre les suites (u_n) et (v_n) ? On ne s'intéressera donc par la suite qu'à la suite (u_n) et pour tout $n \geqslant 1$, on pose $u_n = \dfrac{a_n}{b_n}$.

b. Quelle conjecture peut-on émettre sur le terme général de la suite (b_n) ?

c. D'après les puissances successives de M^n, écrire les 6 premiers termes de (a_n).

d. Effectuer les sommes de deux termes consécutifs et émettre une conjecture sur la formule donnant $a_{n+1} + a_n$, pour tout $n \geqslant 1$.

e. À l'aide d'un logiciel de calcul formel, déterminer la formule du terme général a_n. (Voir fiche TICE, Maxima)

f. Compléter l'opération suivante et en déduire l'expression de a_5 correspondante.

Faire de même pour a_4 et en déduire que l'on peut conjecturer que la formule donnant le terme général a_n est, pour tout $n \geqslant 2$:

$$a_n = (-1)^n \sum_{k=0}^{n-2} (-3)^k.$$

$$\begin{array}{rl} a_5 & = \ldots \\ -a_4 & = \ldots \\ +a_3 & = \ldots \\ -a_2 & = \ldots \\ \hline a_5 & = \ldots \end{array}$$

g. En déduire que pour tout $n \geqslant 1$, on obtient bien la formule donnée par le logiciel à la question **e.**

h. En déduire la forme des termes généraux de (u_n) et (v_n).

3. a. Démontrer que $\dfrac{1}{3}u_n + \dfrac{2}{3}v_n = v_{n+1}$.

b. Démontrer par récurrence la forme de M^n.

Fractales

Algorithmique

34 Le triangle de Sierpinsky

1. Préliminaires

Pour tout point Ω du plan et tout réel $k \neq 0$, on considère la transformation du plan suivante :

$$f_\Omega : M \mapsto M',$$

telle que $\overrightarrow{\Omega M'} = k\overrightarrow{\Omega M}$.

On pose $M(x\,;y)$ et $M'(x'\,;y')$.

a. Écrire analytiquement sous forme d'un système la relation vectorielle définissant la transformation f_Ω.

b. Écrire ce système sous la forme matricielle $Y = AX + B$, où on aura posé $X = \begin{pmatrix} x \\ y \end{pmatrix}$ et $Y = \begin{pmatrix} x' \\ y' \end{pmatrix}$.

c. On prend à partir de maintenant $k = 0{,}5$. Réécrire le système obtenu en **a.**

2. On considère un triangle ABC et M_1 un point quelconque du plan. Pour tout entier $n \geqslant 1$, on définit alors la suite de points (M_n) de la manière suivante :

$$M_{n+1} = f_\Omega(M_n)$$

où Ω est aléatoirement et équiprobablement choisi parmi les trois sommets du triangle.

Voici l'ébauche d'un algorithme permettant de représenter les N premiers points de la suite (M_n).

```
N = 5 000 ;
m est un point quelconque du plan ;
Pour i = 2 à N faire
   choix est un entier aléatoire entre 0 et 2 ;
   Si (choix==0) alors
      x = … ;
      y = …. ;
   Sinon Si (choix==1) alors
      x = … ;
      y = …. ;
   Sinon
      x = … ;
      y = …. ;
   FinSi
   m est le point de coordonnées (x ; y) ;
FinPour
```

a. Expliquer pourquoi le deuxième `Sinon` ne possède pas de test sur la valeur de la variable `choix` .

b. Compléter les lignes donnant les cordonnées x et y en s'aidant des questions préliminaires.

c. Un nombre aléatoire `alea` étant un réel compris entre 0 et 1, quelles opérations doit-on lui appliquer afin d'obtenir successivement un nombre aléatoire entre 0 et 3 ? un nombre entier égal à 0 ou 1 ou 2 ?

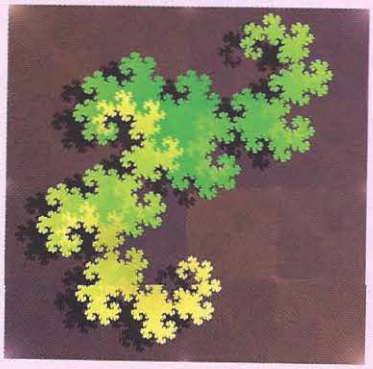
Aide

On utilisera la partie entière.

d. Programmer puis tester cet algorithme dans un logiciel adapté. On pourra faire des essais en prenant N = 10 000 ou 20 000 selon le logiciel utilisé et la puissance de l'ordinateur.

Algorithmique

35 La courbe du dragon



On considère deux transformations du plan f_i : $M(x\,;y) \mapsto M'(x'\,;y')$, $i = 1$ ou 2, données sous forme matricielle par :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 0{,}5 & -0{,}5 \\ 0{,}5 & 0{,}5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix};$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -0{,}5 & -0{,}5 \\ 0{,}5 & -0{,}5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

En s'aidant de l'exercice précédent, écrire un algorithme permettant de représenter les N premiers points de la suite définie par :

- A_0 est l'origine du repère ;
- $A_{n+1} = f_i(A_n)$, où f_i est l'une des deux transformations données, choisies aléatoirement et équiprobablement.

On pourra représenter $N = 50\,000$ points pour avoir une bonne idée de la courbe (selon la puissance de l'ordinateur utilisé).

Arbre de Stern-Brocot

L'arbre de Stern-Brocot permet de représenter tous les rationnels strictement positifs sous forme d'une fraction irréductible. En voici le principe :

On part du couple de « fractions » $\frac{0}{1}$ et $\frac{1}{0}$, en prenant comme convention que $1/0 = +\infty$ et on applique le procédé suivant :

« Entre deux fractions $\frac{a}{b}$ et $\frac{a'}{b'}$, on insère la fraction $\frac{a+a'}{b+b'}$. »

36 Le principe

1. Faire fonctionner ce procédé trois fois, en écrivant chaque suite de fractions sur une seule ligne, et vérifier que l'on aboutit à la suite de fractions :

$$\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}, \frac{3}{2}, \frac{2}{1}, \frac{3}{1}, \frac{1}{0}$$

2. On souhaite démontrer par récurrence que si $\frac{a}{b}$ et $\frac{a'}{b'}$ sont deux fractions consécutives, alors $ab' - ba' = -1$.

a. Vérifier la propriété au rang 0 (ligne 0).

b. On suppose la propriété vraie au rang p et que la fraction $\frac{a+a'}{b+b'}$ se trouve à la ligne p+1.

Calculer $a(b+b') - b(a+a')$
ainsi que $(a+a')b' - (b+b')a'$ et conclure.

3. En utilisant le théorème de Bézout, que peut-on en déduire pour chaque fraction ?

37 Représentation matricielle

On pose $M = \begin{pmatrix} a & a' \\ b & b' \end{pmatrix}$.

1. Déterminer la matrice D telle que :

$$MD = \begin{pmatrix} a+a' & a' \\ b+b' & b' \end{pmatrix}.$$

2. Déterminer la matrice G telle que :

$$MG = \begin{pmatrix} a & a+a' \\ b & b+b' \end{pmatrix}.$$

3. On pose $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

a. Calculer $JGGD$ et vérifier que l'on obtient le bon résultat en comparant avec la question **1.** de l'exercice 36.

b. Même question avec $JGDG$.

c. À votre avis, pourquoi les matrices s'appellent-elles D et G ?

Algorithmique

38 Algorithme



On considère un nombre décimal `x` et on voudrait lui trouver un encadrement par des fractions irréductibles.

1. Compléter l'ébauche suivante, le programmer et le tester.

```
Saisir le nombre d'étapes N ;
Saisir x ;
J est la matrice (ligne) [[0,1],[1,0]] ;
Pour i = 1 à ... faire
   d = JD ;
   g = JG ;
   Si (... ≤ x && x ≤ ...) alors
      J = d ;
   Sinon
      J = g ;
   FinSi
FinPour
Afficher J ;
```

2. Améliorer l'algorithme pour connaître la matrice M, produit de D et G, permettant d'obtenir le résultat final.

Devoir de synthèse

Revoir les bases suivantes : cours A et B, savoir-faire 1 à 4.

[Le devoir est corrigé p. 175]

Chaque exercice peut être fait de manière indépendante.

39 QCM [3 points]

1. Soient M une matrice stochastique selon les colonnes, u et v les vecteurs ligne et colonne dont les coordonnées sont toutes égales à 1, alors :

a. $u = uM$; **b.** $u = Mu$;

c. $v = vM$; **d.** $v = Mv$.

2. Même question pour une matrice M stochastique selon les lignes.

3. On pose $v = Mu$, pour M une matrice carrée de taille n et u un vecteur colonne. Alors pour tout i, $v_i =$:

a. $\sum_{k=1}^{n} m_{ik}u_k$. **b.** $\sum_{k=1}^{n} u_k m_{ki}$.

40 [2 points]

On donne la matrice M suivante, stochastique selon les colonnes :

$$M = \begin{pmatrix} 0{,}2 & 0{,}5 & 0 \\ 0{,}8 & 0 & 0{,}6 \\ 0 & 0{,}5 & 0{,}4 \end{pmatrix}.$$

Déterminer le graphe fléché associée à cette matrice.

41 [3 points]

On considère la matrice M suivante :

$$M = \begin{pmatrix} 0{,}6 & 0{,}4 \\ 0{,}1 & 0{,}9 \end{pmatrix}.$$

1. a. Cette matrice est-elle stochastique selon les lignes ou les colonnes ?

b. Écrire la matrice P, stochastique selon les colonnes correspondantes.

2. On pose $u = \begin{pmatrix} 0{,}25 \\ 0{,}75 \end{pmatrix}$.

a. Calculer $P^{10}u$, $P^{20}u$, $P^{30}u$.
Que peut-on conjecturer ?

b. Déterminer la mesure stationnaire $\pi = \begin{pmatrix} a \\ b \end{pmatrix}$ de P.

c. Vérifier que cette mesure stationnaire vérifie $(a \;\; b) = (a \;\; b)M$.

42 [6 points]

Dans une population, chaque individu est susceptible de contracter une maladie et il peut présenter trois états face à cette maladie :

- immunisé, état 1 ;
- malade, état 2 ;
- non immunisé et non malade, état 3.

Chaque jour, son état peut changer selon les règles suivantes :

- s'il est dans l'état 1, il peut y rester avec une probabilité de 0,9 ou passer à l'état 3 ;
- s'il est dans l'état 2, il peut y rester avec une probabilité de 0,2 ou passer à l'état 1 ;
- s'il est dans l'état 3, il peut y rester avec une probabilité de 0,5 ou passer à l'état 2.

1. Représenter la situation par un graphe fléché.

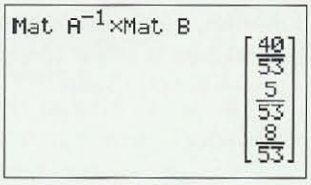
2. a. Déterminer la matrice M représentant la situation.

b. M semble-t-elle admettre une mesure stationnaire ? Si oui, la déterminer empiriquement (les valeurs seront arrondies à 10^{-2}).

3. a. Écrire l'équation que doit satisfaire cette mesure stationnaire π sous la forme $P\pi = 0$ en précisant la matrice P.

b. P est-elle inversible ?
Combien d'équations du système correspondant peut-on garder ?
Quelle équation doit-on rajouter ?

c. Voici un calcul permettant de trouver la mesure stationnaire, lorsque B est le vecteur colonne $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$:



Que contient la matrice A ? Justifier.

d. Quelle est, en permanence, la proportion de la population toujours malade ?

43 ROC [3 points]

Soient u un vecteur colonne stochastique de taille n, M une matrice stochastique selon les colonnes de taille n.

a. Démontrer que le vecteur $v = Mu$ est un vecteur colonne stochastique.

b. En déduire que le vecteur $v = (1 - c)Mu + c\varepsilon$, où ε est le vecteur colonne stochastique ayant toutes ses coordonnées égales, est aussi un vecteur stochastique.

44 [3 points]

Deux suites (a_n) et (b_n) sont définies par :

$$a_{n+1} = 0{,}3a_n + 0{,}85b_n \; ; \; a_0 = 0{,}5.$$
$$b_{n+1} = 0{,}7a_n + 0{,}15b_n \; ; \; b_0 = 0{,}5.$$

1. Écrire cette relation sous forme matricielle.

2. Démontrer que pour tout entier naturel n, $a_n + b_n = 1$.

3. En déduire la limite de chacune des suites.

Exercices guidés BAC

45 La météo

Un modèle météo simplifié propose deux états : pluie (1) et soleil (2). Une étude statistique montre que l'on passe d'un état de pluie à un état de soleil avec la probabilité $a = 0{,}3$ et d'un état de soleil à un état de pluie avec la probabilité $b = 0{,}8$.

1. Réaliser le graphe correspond à cette situation.

2. Déterminer la matrice de transition correspondante, notée M.

3. Aujourd'hui, il fait beau. On souhaite connaître la probabilité de l'état du ciel les jours suivants. Pour cela, on considère la suite $(u^{(n)})$, où $u_1^{(n)}$ et $u_2^{(n)}$ désignent respectivement les probabilités de pluie et de soleil après n jours.

a. Donner le vecteur $u^{(0)}$.

b. Exprimer $u^{(n)}$ en fonction de $u^{(0)}$.

c. Calculer la probabilité de pluie dans une semaine.

d. La suite $u^{(n)}$ semble-t-elle converger ? Si oui, donner la mesure stationnaire arrondie à 10^{-2}.

4. On note $\pi = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$ la mesure stationnaire.

a. Démontrer que déterminer cette mesure amène la résolution du système suivant : $\begin{cases} -a\pi_1 + b\pi_2 = 0 \\ \pi_1 + \pi_2 = 1 \end{cases}$

b. Écrire ce système matriciellement sous la forme $Y = AX$. On précisera Y, A et X.

c. Pour résoudre ce système à l'aide du logiciel maxima, deux élèves proposent les solutions suivantes, quelle est la bonne et pourquoi ? Vérifier que la valeur obtenue correspond bien la valeur conjecturée en **3.d.**

```
(%i2) invert(A).[0,1], ratsimp;
(%o2) [ b/(b+a) ]
      [ a/(b+a) ]
```

```
(%i3) [0,1].invert(A), ratsimp;
(%o3) [ 1/(b+a)  a/(b+a) ]
```

Guide

1. Le graphe comporte deux états. On complète les probabilités en se rappelant que la somme des probabilités des arrêtes partant d'un même état est égale à 1.

2. m_{ij} est la probabilité de passer de l'état j à l'état i.

3. a. Aujourd'hui, il fait beau !

c. Une semaine, c'est-à-dire 7 jours.

d. On calcule $u^{(20)}$, $u^{(30)}$, plus si nécessaire.

4. a. La mesure stationnaire π satisfait l'équation $\pi = M\pi$. De plus, une mesure stationnaire est un vecteur de probabilité.

c. Écrire matriciellement la résolution de l'équation $Y = AX$.

46 Transmission de données

Un message codé en binaire est transmis à travers un réseau comportant plusieurs relais. À chaque relais, chaque bit est transmis avec une probabilité d'erreur. Une étude statistique donne les probabilités d'erreurs suivantes :

- le bit 0 est transmis en 1 avec la probabilité a ;
- le bit 1 est transmis en 0 avec la probabilité b.

On suppose que la matrice de transition est $M = \begin{pmatrix} 1-a & b \\ a & 1-b \end{pmatrix}$ et que la probabilité invariante est $\pi = \begin{pmatrix} p \\ 1-p \end{pmatrix}$, où $p = \dfrac{b}{a+b}$.

1. On note $p_n = P$(au relais n, le bit est 0). Démontrer que
$$p_{n+1} - p = (1 - a - b)(p_n - p).$$

2. En déduire que $p_{n+1} = (1 - a - b)^n (p_0 - p) + p$.

3. On pose $a = 0{,}02$ et $b = 0{,}01$.

a. On suppose que l'on transmet le bit 0, calculer la taille maximale du réseau pour que la probabilité de recevoir le même bit soit au moins égale à 90 % et retrouver la valeur empirique de l'exercice 19 p. 156.

b. Même question avec la transmission du bit 1.

4. On transmet 4 bits égaux à 0 indépendamment les uns des autres. Démontrer que la taille du réseau est au maximum de 2 relais.

Guide

1. Par définition, on a
$$\begin{pmatrix} p_{n+1} \\ 1-p_{n+1} \end{pmatrix} = M \begin{pmatrix} p_n \\ 1-p_n \end{pmatrix}.$$

2. La suite $(p_n - p)$ est géométrique de raison $1 - a - b$.

3. a. On doit résoudre l'équation $p_n \geqslant 0{,}9$, d'inconnue n.

b. On doit résoudre l'équation $1 - p_n \geqslant 0{,}9$, d'inconnue n.

4. Les transmissions étant indépendantes, la probabilité d'obtenir les 4 mêmes bits est p_n^4.

QCM - Vrai ou faux BAC

Logique

47 **Vrai ou Faux**

a. Si la suite $(M^n u)$ converge pour un certain vecteur stochastique u, alors M admet une mesure invariante.

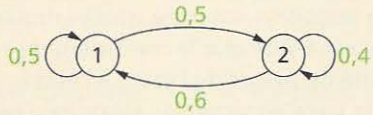
b. Si la suite $(M^n u)$ ne converge pas pour un certain vecteur stochastique u, alors M n'admet pas de mesure invariante.

c. Si la suite $(M^n u)$ est constante, alors u est une mesure invariante de M.

d. Si u est une mesure invariante de M, alors la suite $(M^n u)$ est constante.

48 **QCM**

La matrice stochastique associée au graphe ci-dessous est :

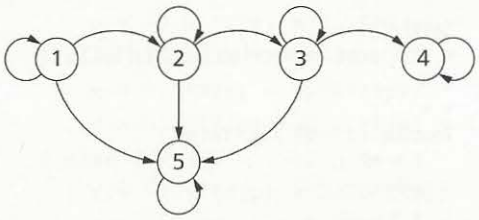


a. $M = \begin{pmatrix} 0{,}5 & 0{,}6 \\ 0{,}5 & 0{,}4 \end{pmatrix}$.

b. $M = \begin{pmatrix} 0{,}5 & 0{,}5 \\ 0{,}6 & 0{,}4 \end{pmatrix}$.

Exercice BAC

49 Une grande école propose une formation diplômante en trois ans. À l'issue de chaque année, chaque élève a la probabilité p de passer dans l'année supérieure (ou d'obtenir son diplôme s'il est en 3e année), une probabilité q de redoubler et une probabilité r d'être renvoyé.



1. Compléter le graphe ci-dessus où les états 1, 2 et 3 symbolisent les 3 années d'études ; l'état 4 l'obtention définitive du diplôme et l'état 5 le renvoi définitif de l'école.

2. Quelle est la taille de la matrice de transition, notée M, associée à ce graphe ? Donner cette matrice. On rappelle que le coefficient m_{ij} représente la probabilité de passer de l'état j à l'état i.

3. On souhaite connaître la probabilité pour un élève de 1re année d'obtenir son diplôme. On considère pour cela la suite $(u^{(n)})$ définie pour tout $n \in \mathbb{N}$ par : $u^{(n)} = M^n u^{(0)}$, $u^{(0)}$ représentant la condition initiale.

a. Donner vecteur $u^{(0)}$.

b. Quel terme de la suite faut-il calculer pour connaître la probabilité d'obtenir son diplôme en exactement 3 ans ? Quel coefficient de ce terme permet de connaître cette probabilité ? La déterminer.

c. À partir de combien d'année la probabilité d'obtention du diplôme est-elle supérieure à 80 % ?

d. La suite $(u^{(n)})$ semble-t-elle converger ? Si oui, en déduire la probabilité que l'élève obtienne son diplôme.

4. Pour tout $i = 1, \ldots, 5$, on note a_i la probabilité d'obtenir son diplôme lorsqu'on est dans l'état i.

a. Donner les valeurs de a_4 et a_5. Justifier.

b. On note A_{ji} l'événement : « on passe de l'état i à l'état j ». Par exemple, $a_1 = P(A_{41})$.
En remarquant que les événements A_{11}, A_{21} et A_{51} forment une partition de l'espace de probabilités, démontrer que $a_1 = qa_1 + pa_2$.
On admettra qu'on a aussi :

$$a_2 = qa_2 + pa_3 \text{ et } a_3 = qa_3 + p.$$

c. On note $u = (a_1\ a_2\ a_3\ a_4\ a_5)$ et v le même vecteur mais en colonne. À partir des égalités de la question **b.** laquelle des deux égalités peut-on écrire : $0 = u(M - I)$ ou bien $0 = (M - I)v$?

5. La résolution de ces systèmes dans le logiciel Maxima nous donne ceci :

```
(%i3) S:[a1,a2,a3,1,0].(M-I)$
      linsolve([S[1][1]=0, S[1][2]=0, S[1][3]=0], [a1,a2,a3]), factor;
(%o4) [a1=-p^3/(q-1)^3, a2=-p^2/(q-1)^2, a3=-p/(q-1)]

(%i5) S:(M-I).[a1,a2,a3,1,0]$
      linsolve([S[1][1]=0, S[2][1]=0, S[3][1]=0], [a1,a2,a3]), factor;
(%o6) [a1=0, a2=0, a3=0]
```

a. Déduire de cette capture la valeur exacte de la probabilité d'obtenir son diplôme pour un élève entrant en 1re année et vérifier que cela correspond à la valeur approchée trouvée à la question **3.d.**

b. Que représentent les valeurs de a_2 et a_3 ?

c. Vérifier empiriquement en s'appuyant sur la méthode de la question **3.** et décrire la démarche utilisée.

50 Démonstration de la propriété 3 p. 148

On considère un graphe fléché à p états et M la matrice de transition associée, stochastique selon les colonnes, c'est-à-dire que le coefficient m_{ij} représente la probabilité de passer de l'état j à l'état i.
Soit $(X_n)_n$ la suite de variables aléatoires, où la valeur de X_n est l'état dans lequel on se trouve après une marche aléatoire de n étapes sur le graphe.

1. Préliminaires

a. Quelle est la taille de M ?

b. Quelles sont les valeurs possibles pour chacune des variables aléatoires ?

c. Pour tout entier naturel n, à quel coefficient de M est égale la probabilité suivante : $P_{X_n=j}(X_{n+1}=i)$?

d. Soient A et B deux événements d'un espace de probabilité. Rappeler la formule de $P_B(A)$ (probabilité de A sachant B).

2. On désire montrer que pour tout i et j compris entre 1 et p et pour tout entier $k \geqslant 1$ que :

$$m_{ij}^{(k)} = P_{X_n=j}(X_{n+k}=i).$$

On va procéder par récurrence sur l'entier k.

a. Vérifier que la propriété est vraie pour $k=1$.

b. On suppose maintenant la propriété vraie au rang $k-1$. En remarquant que les événements $(X_{n+k-1}=1)$, $(X_{n+k-1}=2)$, …, $(X_{n+k-1}=p)$ forment une partition de l'espace de probabilité, démontrer que :
$P(X_n=j \cap X_{n+k}=i) =$

$$\sum_{l=1}^{p} P(X_n=j \cap X_{n+k-1}=l) P_{X_n=j \cap X_{n+k-1}=l}(X_{n+k}=i)$$

c. Des deux événements $(X_n=j)$ et $(X_{n+k-1}=l)$, quel est le seul ayant une influence sur la valeur de X_{n+k} ? En utilisant la propriété au rang 1, en déduire le coefficient de M égal à :

$$P_{X_n=j \cap X_{n+k-1}=l}(X_{n+k}=i).$$

d. D'après l'hypothèse de récurrence au rang $k-1$, déduire que :

$$P(X_n=j \cap X_{n+k}=i) = P(X_n=j) \sum_{l=1}^{p} m_{il} m_{lj}^{(n+k-1)}$$

e. Conclure.

Algorithmique

51 Approximation de $\sqrt{2}$

Préliminaires

On considère la fonction f définie par : $f(x) = \dfrac{ax+b}{cx+d}$, où a, b, c et d sont quatre réels, c et d non nuls.

1. À quelle condition sur les coefficients c et d la fonction f est-elle continue sur $\mathbb{R}^+$.

2. Sous cette condition, déterminer un encadrement de $f(x)$, pour tout $x \geqslant 0$.
Le nombre $\sqrt{2}$ est la solution positive de l'équation $x^2 - 2 = 0$.

3. Démontrer que $\sqrt{2}$ est aussi solution de :

$$x = \frac{x+2}{x+1}.$$

4. On considère alors la fonction $f : x \mapsto \dfrac{x+2}{x+1}$.

Aide

Pour la question 2, on envisagera deux cas, selon que f est croissante ou décroissante et dans chaque cas, on établira le tableau de variations de f sur $[0 ; +\infty[$.

a. Donner un encadrement de $f(x)$. Peut-on donner une valeur approchée de $\sqrt{2}$? Si oui, donner la précision de cette valeur approchée.

b. Expliquer pourquoi $\sqrt{2} = f\big(f(\sqrt{2})\big)$.

c. Donner la matrice associée à la fonction homographique f (voir activité 1 p. 106).

d. En déduire la matrice associée à la fonction $x \mapsto f\big(f(x)\big)$. Peut-on donner une valeur approchée de $\sqrt{2}$? Si oui, donner la précision de cette valeur approchée.

e. Même consigne avec $x \mapsto f\big(f(f(x))\big)$, etc. jusqu'à obtenir une précision de 10^{-2}.

5. Voici l'ébauche d'un l'algorithme permettant d'afficher une valeur approchée de $\sqrt{2}$, selon une précision de 10^{-n}, déterminée par l'utilisateur.

```
Saisir(n) ;
M et P sont la matrice [[1,2],[1,1]] ;
u = ... ;
v = ... ;
TantQue (u - v) > ... faire
   P = MP ;
   u = ... ;
   v = ... ;
FinTantQue
Afficher(u) ;
```

b. Compléter cet algorithme, le programmer et le tester.

c. Modifier l'algorithme afin qu'il compte et affiche la puissance de la matrice M nécessaire pour donner la valeur approchée à 10^{-n} près.

d. Pour obtenir plus rapidement un résultat, Pauline propose de remplacer la ligne $P = MP$ par $P = PP$. Marie prétend que cette technique ne permet pas de connaître la puissance de la matrice de base qui a été calculée. Qui a raison ?

52 Approximation de ϕ

ϕ est le nombre d'or, solution positive de l'équation $x^2 = x + 1$.

1. a. Donner la fonction homographique f telle que $\phi = f(\phi)$.

b. Donner la matrice correspondante.

2. En reprenant le principe de l'exercice précédent, déterminer une approximation à 10^{-3} près de ϕ.

Algorithmique

53 La fougère de Barnsley

On considère quatre transformations f_i du plan, $f_i : M(x ; y) \mapsto M'(x' ; y')$, où

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u_i \\ v_i \end{pmatrix}.$$

Le principe de la construction est le suivant :

- le premier point placé est l'origine du repère ;
- le point suivant est l'image du précédant par la transformation f, choisie parmi les quatre transformations f_i, selon les probabilités suivantes :

$P(f = f_1) = 0{,}1$; $P(f = f_2) = 0{,}76$;
$P(f = f_3) = 0{,}07$; $P(f = f_4) = 0{,}07$.

1. Voici l'ébauche de l'algorithme permettant de placer les N premiers points de la construction, écrit dans le module JavaScript de CaRMetal.

```
1  N = 10000;
2  p = Point("A1",0,0);
3
4  for(i=2; i<=N; i++){
5      choix = Math.random();
6      if(choix <     ){ //f1
7          x = 0;
8          y = 0.16*Y(p);
9      } else if(choix <      ) { //f2
10         x = 0.85*X(p) + 0.04*Y(p);
11         y = -0.04*X(p) + 0.85*Y(p) + 1.6;
12     } else if(choix <      ){ //f3
13         x = 0.2*X(p) - 0.26*Y(p);
14         y = 0.23*X(p) + 0.22*Y(p) + 1.6;
15     } else { //f4
16         x = -0.15*X(p) + 0.28*Y(p);
17         y = 0.26*X(p) + 0.24*Y(p) + 0.44;
18     }
19     p = Point("A"+i,x,y);
20 }
```

a. À l'aide des formules données aux lignes 7&8, 10&11, 13&14, 16&17, déterminer les matrices et vecteurs colonnes permettant de définir chacune des quatre transformations.

b. Sachant que la variable `choix` contient un nombre aléatoire compris entre 0 et 1, compléter la ligne 6 afin de choisir la transformation f_1 avec la probabilité voulue.

c. Si l'on complète par `0.76` à la ligne 9, quelle sera la probabilité de choisir f_2 ? Compléter alors correctement cette ligne.

d. Compléter la ligne 12. Pourquoi le dernier `Sinon` (l. 15) ne possède-t-il pas de test sur la valeur de la variable `choix` ?

2. a. Écrire puis tester cet algorithme dans le logiciel de votre choix.

b. Modifier cet algorithme afin que les points créés par chacune des quatre fonctions soient de quatre couleurs différentes.

@ Un fichier mis à disposition sur http://libtheque.fr/mathslycee contient un algorithme permettant de visualiser dynamiquement l'effet des 24 paramètres a_i, b_i, c_i, d_i, u_i et v_i.

Défis

54 On considère une matrice A, carrée de taille p, telle qu'il existe deux matrices P inversible et D diagonale telles que $A = P^{-1}DP$, avec $D = \text{diag}(1, \ldots, 1, x_{r+1}, \ldots, x_p)$, $r < p$ et $|x_i| < 1$ pour tout i entier compris entre $r + 1$ et p.

1. On pose : $M_n = \frac{1}{n}\sum_{k=1}^{n} D^k$ et $B_n = P^{-1}M_nP$.

Montrer que la suite (M_n) converge vers la matrice $\Delta = \text{diag}(1, \ldots, 1, 0, \ldots, 0)$, où le dernier 1 est en r-ième position.

On admet alors que la suite (B_n) converge vers $P^{-1}\Delta P$.

2. a. Démontrer que B_n est une matrice stochastique.

b. En déduire que $P^{-1}\Delta P$ est une matrice stochastique.

Communiquer à l'écrit ou à l'oral

Qu'est-ce qu'une IFS (Iterated Function System) ?

Quelques pistes pour répondre :

1. On pourra commencer par se renseigner sur la Fougère de Barnsley.

2. Trouver d'autres fractales de type IFS en axant vos recherches sur Sierpinsky, Von Koch, Martin Gardner.

3. Expliquer le principe.

Communiquer les résultats

Réaliser un diaporama où l'on présentera quelques fractales de type IFS avec leurs fonctions caractéristiques.



Accompagnement personnalisé

Soutien

Objectifs :
- Gérer les valeurs initiales et finales du compteur dans une boucle Pour.
- Gérer les variables dans un algorithme.
- Programmer une somme.

AP 1 Analyser une copie

Voici un algorithme permettant de calculer le produit de deux matrices carrées de taille 2.

```
Saisir les matrices A et B ;
C est une matrice de taille 2 ;
Pour i = 0 à 1 faire
   Pour j = 0 à 1 faire
      C[i][j] = A[i][0]*B[0][j] + A[i][1]*B[1][j] ;
   FinPour
FinPour
Afficher C ;
```

1. Modifier l'algorithme afin qu'il fonctionne pour le produit d'une matrice de taille $n \times 2$ par une matrice de taille $2 \times p$.

2. Modifier l'algorithme pour qu'il fonctionne dans le cas général.

3. Calculer le produit AB avec les matrices suivantes :

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}.$$

1. La première boucle devient :
`Pour i = 0 à n` *et la seconde :*
`Pour j = 0 à p` *, sans oublier que la matrice C est maintenant de taille* $n \times p$.

2. Pour étudier le cas général, il faut changer la formule donnant la valeur de `C[i][j]`*. La formule est la suivante :*

$$c_{ij} = \sum_{k=1}^{q} a_{ik}b_{kj}$$ *où* q *est le nombre de colonnes de* A.

On la programme par une boucle :

```
q est le nombre de colonnes de A ;
Pour k = 0 à q faire
   C[i][j] = C[i][j] + A[i][k]*B[k][j] ;
FinPour
```

3. On saisit les matrices
$A = [[1,3],[2,4]]$
et $B = [[5,7],[6,8]]$
et on obtient $C = [[23,34],[31,46]]$

Découvrir un métier

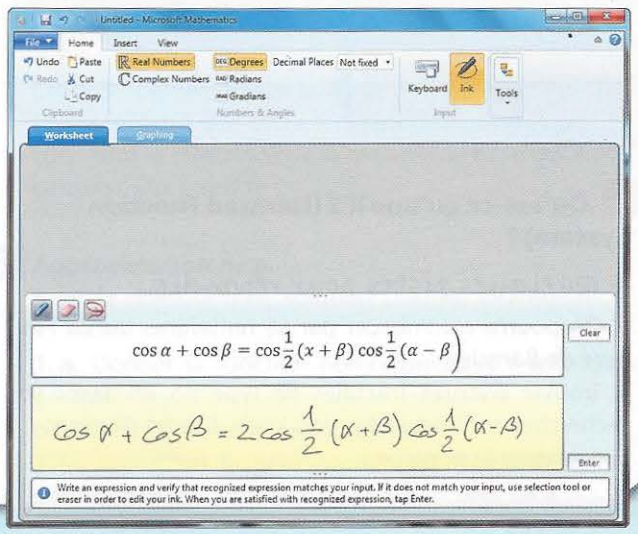
Objectifs :
- Aide à l'orientation.
- Comprendre l'utilité des mathématiques.

AP 2 Analyste programmeur (développeur)

Sur certaines tablettes ou Smartphones, il est possible d'écrire un texte en utilisant un stylet, texte alors converti en une suite de caractères, exploitable par un traitement de texte. La conversion se fait à l'aide d'un algorithme et il se peut que par moments, la conversion ne soit pas correcte : certaines lettres sont mal reconnues.

1. En quoi la reconnaissance d'écriture manuscrite utilise-t-elle des matrices ?

2. Dans le cas où une lettre n'est pas clairement identifiable, comment l'algorithme de conversion peut-il « deviner » la bonne lettre ?



Approfondir

AP 3 Manger – Boire – Dormir !

Objectifs :
- *Établir un graphe en utilisant les données du texte.*
- *Interpréter une mesure stationnaire.*

Dans sa cage, un hamster a le choix entre trois endroits : des copeaux (parfumés) de bois où il dort, sa mangeoire et sa pipette à eau.
Statistiquement, on a noté qu'à chaque unité de temps (minute), il peut changer d'activité ou bien continuer celle qu'il est en train de faire :
- s'il dort, il a 9 chances sur 10 de ne pas se réveiller la minute suivante et lorsqu'il se réveille, il va boire ou manger de manière équiprobable ;
- le repas et la boisson ne dure toujours qu'une minute ;
- après avoir mangé, il a 3 chances sur 10 d'aller boire ;
- après avoir bu, il a 8 chances sur 10 d'aller dormir.

1 On note 1 l'état de repos, 2 l'état de manger et 3 celui de boisson. Établir le graphe représentant cette situation.

2 Donner la matrice de transition associée, notée M.

3 On désire connaître l'état du hamster au bout de n minutes.

a. Quelle suite $(u^{(n)})$ de vecteurs doit-on considérer ?

b. Actuellement, le hamster dort. Donner $u^{(0)}$.

c. Calculer la probabilité qu'il dorme encore au bout de 5 minutes.

d. La suite $(u^{(n)})$ semble-t-elle converger ?

4 On voudrait connaître la proportion de temps que le hamster alloue à chaque « activité ».

a. Justifier le fait que l'on doive pour cela déterminer la mesure stationnaire de la matrice M.

b. La déterminer.

c. En déduire la proportion de temps que le hamster passe à dormir.

AP 4 Le modèle de Leontiev

Objectif :
- *Prendre une initiative.*

Trois superpuissances économiques, numérotées de 1 à 3, partagent le fruit de leur production selon le modèle suivant :
- le pays 1 consomme le tiers de sa production et partage équitablement le reste entre les pays 2 et 3 ;
- le pays 2 consomme la moitié de sa production et partage le reste équitablement entre les pays 1 et 3 ;
- le pays 3 consomme le cinquième de sa production et en donne la moitié au pays 1.

Quelle est la proportion de richesse détenue par chaque pays ?

AP 5 Les élections

Objectif :
- *Étudier une perturbation dans un modèle.*

Lors du second tour de chaque élection, deux partis politiques, numérotés 1 et 2 s'affrontent.
Une étude statistique a montré que :
- 80 % des électeurs du parti n° 1 lui restent fidèle à l'élection suivante.
- 90 % des électeurs du parti n° 2 lui reste fidèle à l'élection suivante.

1 Si l'on suit ce modèle, quel sera le parti qui finira toujours par gagner, à terme ?

2 On suppose maintenant qu'une proportion c des électeurs continue de voter de la même façon tandis que l'autre proportion, par mécontentement, vote systématiquement pour le candidat adverse de leur précédent vote, en proportion inverse des résultats de la précédente élection.

a. Montrer que si $u^{(n)}$ représente les proportions de vote lors de la n-ième élection, alors on a la relation suivante, où l'on précisera le vecteur $v^{(n)}$:

$$u^{(n+1)} = cMu^{(n)} + (1-c)v^{(n)}.$$

b. Effectuer quelques simulations et en déduire le parti gagnant des élections lors des première années si l'on part d'une proportion $u^{(0)} = \begin{pmatrix} 0{,}33 \\ 0{,}67 \end{pmatrix}$. On pourra effectuer plusieurs simulations, avec $c = 0{,}6$ pour des élections moyennement mécontents et $c = 0{,}2$ avec des électeurs très mécontents.

1 Divisibilité et congruence

Appliquer les capacités attendues

13 **a.** $21 = 1 \times 21 = 3 \times 7$. Les diviseurs de 21 sont donc : 1, 3, 7, 21, –1, –3, –7, –21.
b. De même $270 = 1 \times 270 = 2 \times 135 = 3 \times 90 = 5 \times 54 = 6 \times 45 = 9 \times 30 = 10 \times 27 = 1 \times 18$. Les diviseurs entiers naturels de 270 : sont :1, 2, 3, 5, 6, 9, 10, 15, 18, 27, 30, 45, 54, 90, 135, 270.

19 Soit n un entier solution, alors $n - 4$ divise $n + 7$ et $n - 4$, donc divise $(n + 7) - (n - 4) = 11$. Les diviseurs de 11 sont –11, –1, 1 et 11, donc $n - 4 = -11$ ou $n - 4 = -1$ ou $n - 4 = 1$ ou $n - 4 = 11$, soit $n = -7$ ou $n = 3$ ou $n = 5$ ou $n = 15$. On vérifie que ces entiers sont bien solutions. Les solutions sont donc : –7,3, 5 et 15.

26 La propriété est vraie pour $n = 0$, car 7 divise $3^{2\times0} - 2^0 = 1 - 1 = 0$.
Supposons la propriété vraie pour un entier naturel n, donc 7 divise $3^{2n} - 2^n$, et $3^{2n} - 2^n = 7k$, soit $3^{2n} = 2^n + 7k$ ($k \in \mathbb{Z}$).
$3^{2(n+1)} - 2^{n+1} = 3^{2n+2} - 2^{n+1} = 3^2 \times 3^{2n} - 2 \times 2^n$
$= 9(2^n + 7k) - 2^n \times 2 = 2^n (9 - 2) + 7(9k) = 7(2^n + 9k)$.
$2^n + 9k \in \mathbb{Z}$, donc 7 divise $3^{2(n+1)} - 2^{n+1}$.
Donc la propriété est vraie pour $n + 1$, et donc vraie pour tout n.

31 Soit $(x ; y)$ un couple solution. Puisque $(x - 3)(y + 5) = 6$, $y + 5 \in \mathbb{N}$, donc $x - 3 \in \mathbb{N}$ et $x - 3$ et $y + 5$ sont deux diviseurs associés de 6. $6 = 1 \times 6 = 2 \times 3$, d'où $(x ; y) = (4 ; 1)$ ou $(9 ; -4)$ ou $(5 ; -2)$ ou $(6 ; -3)$. On vérifie que ces 4 couples sont solutions. Il y a donc 4 solutions : $(4 ; 1)$, $(9 ; -4)$, $(5 ; -2)$ et $(6 ; -3)$.

36 Soit $(x ; y)$ une solution. $3x^2 + y^2 = 21$, donc $3x^2 \leqslant 21$, soit $x^2 \leqslant 7$; dans $\mathbb{Z}$, les seules valeurs possibles de x sont : 0, –1 et 1, –2 et 2. On fait une étude exhaustive suivant les valeurs de x :
Si $x = 0$, alors $y^2 = 21$, ce qui est impossible dans $\mathbb{Z}$.
Si $x = 1$ ou $x = -1$, alors $y^2 = 18$, ce qui est impossible dans $\mathbb{Z}$.
Si $x = 2$ ou $x = -2$ alors, $y^2 = 9$, d'où $y = -3$ ou $y = 3$.
Les solutions possibles sont les couples : $(-2 ; -3)$, $(-2 ; 3)$, $(2, -3)$ et $(2, 3)$. On vérifie que ces couples sont bien solutions. Les solutions sont : $(-2 ; -3)$, $(-2 ; 3)$, $(2, -3)$ et $(2, 3)$.

38 $\dfrac{5n+7}{n+2}$ est un entier si, et seulement si, $n + 2$ divise $5n + 7$.
Soit n un entier naturel solution, alors $n + 2$ divise $n + 2$ et $5n + 7$. $n + 2$ divise alors $5(n + 2) - (5n + 7) = 3$.
D'où $n + 2 = -1$ ou $n + 2 = 1$ ou $n + 2 = -3$ ou $n + 2 = 3$. Donc, $n = -3$ ou $n = -1$ ou $n = -5$ ou $n = 1$. Il y a donc un seul entier naturel solution $n = 1$. On vérifie que $n = 1$ est solution.

40 $363 = 36 \times 10 + 3$ et $0 \leqslant 3 < 10$, donc $q = 36$ et $r = 3$.
D'où $363 = 45 \times 8 + 3$ et $0 \leqslant 3 < 8$, donc $q = 45$ et $r = 3$.
D'où $-363 = (-36) \times 10 - 3$, d'où $-363 = (-36) \times 10 - 10 + 10 - 3$, soit $-363 = (-37) \times 10 + 7$ et 0. Donc, $q = -37$ et $r = 7$.

43 $a = 7q + r$ avec $0 \leqslant r < 7$ et $q = 4r$. D'où $a = 29r$ avec $0 \leqslant r < 7$.
D'où $a = 0$, $a = 29$,
$a = 2 \times 29 = 58$, $a = 3 \times 29 = 87$, $a = 4 \times 29 = 116$,
$a = 5 \times 29 = 145$, $a = 6 \times 29 = 174$.
On vérifie que ces entiers naturels sont solutions. Les solutions sont donc : 0, 29, 58, 87, 116, 145, 174.

48 $838 = b \times 31 + r$ et $0 \leqslant r < b$, ce qui équivaut à $r = 838 - 31b$ et $0 \leqslant r < b$. On en déduit :
$0 \leqslant 838 - 31b < b$, ce qui équivaut à $31b \leqslant 838$ et $838 < 32b$, soit $31b \leqslant 838 < 32b$, d'où, $b = 27$ et $r = 838 - 27 \times 31 = 1$.

51 Évariste roule pendant 7 h 40 min, soit 460 min.De plus, il fait un tour complet en 80 minutes ($8 \times 10 = 80$).
$460 = 80 \times 5 + 60$. Il fait donc 5 tours complets et entame un 6ème tour et arrive en A_6.

54 $4n + 27 = (n + 5)\,4 + 7$ et $0 \leqslant 7 < n + 5$ si, et seulement si, $n > 2$.
Donc pour $n > 2$, q = 4 et r = 7.
Pour $n = 0$, $4n + 27 = 27$ et $n + 5 = 5$, et $27 = 5 \times 5 + 2$, donc $q = 5$ et $r = 2$. Pour $n = 1$, $4n + 27 = 31$ et $n + 5 = 6$, et $31 = 6 \times 5 + 1$ et $q = 5$ et $r = 1$. Pour $n = 2$ et $4n + 27 = 35$ et $n + 5 = 7$, et $35 = 7 \times 5 + 0$ et $q = 5$ et $r = 0$.

56 **a.** Si $n = 2k$, alors $n(n + 1) = 2k(2k + 1)$; si $n = 2k + 1$, alors $n(n + 1) = (2k + 1)(2k + 2) = 2(2k + 1)(k + 1)$. Dans les deux cas, $n(n + 1)$ est divisible par 2.
b. Si $n = 3k$, alors $n(n^2 - 1) = 3k(9k2 - 1)$.
Si $n = 3k + 1$, alors $n(n^2 - 1) = (3k + 1)((3k + 1)2 - 1) = (3k + 1)(9k2 + 6k) = 3(3k + 1)(3k2 + 2k)$.
Si $n = 3k + 2$, alors $n(n^2 - 1) = (3k + 2)((3k + 2)2 - 1)$
$= (3k + 2)(9k2 + 12k + 3) = 3(3k + 2)(3k2 + 4k + 1)$.
Dans les 3 cas, $n(n^2 - 1)$ est divisible par 3.
Donc, pour tout entier naturel n, $n(n^2 - 1)$ est divisible par 3.

62 **a.** $37 = 11 \times 3 + 4$, donc $37 \equiv 4$ [11] et $0 \leqslant 4 < 11$.
b. $186 = 11 \times 16 + 10$, donc $186 \equiv 10$ [11] et $0 \leqslant 10 < 11$.
c. $-7 - 7 + 11$ [11], donc $-7 \equiv 4$ [11].
d. $5002 = 11 \times 454 + 8$, donc $5002 \equiv 8$ [11]
e. $4002 = 11 \times (-363) - 9$, donc $4002 \equiv -9$ [11],
d'où $4002 \equiv -9 + 11$ [11], soit $4002 \equiv 2$ [11].

64 **a.** $421 \equiv 1$ [7], d'où $421^{120} \equiv 1^{120}$ [7].
De même $99 \equiv 1$ [7], d'où $99^{15} \equiv 1^{15}$ [7].
Par compatibilité avec la multiplication :
$421^{120} \times 99^{15} \equiv 1^{120} \times 199$ [7], d'où
$421^{120} \times 99^{15} \equiv 1$ [7]. Le reste est 1.
b. $93 \equiv 2$ [7], d'où $93^{120} \equiv 2^{120}$ [7];
$44 \equiv 2$ [7], d'où $44^{120} \equiv 2^{120}$ [7].
D'où $93^{120} \times 44^{120} \equiv 2^{120} - 2^{120}$ [7]. D'où,
D'où $93^{120} \times 44^{120} \equiv 0$ [7]. Le nombre est donc divisible par 7.

71 **a.** $x \equiv -3$ [7] équivaut à $x = -3 + 7k$ ($k \in \mathbb{Z}$).
Or $0 < x < 20$, donc $0 < -3 + 7k < 7$, soit $3 < 7k < 10$, soit $k = 1$, d'où une seule solution $x = 4$.
b. Si $x + 3 \equiv -1$ [7], alors $x \equiv -3 - 1$ [7], soit $x \equiv -4$ [7].
Réciproquement, si $x \equiv -4$ [7], alors $x + 3 \equiv 3 - 4$ [7], soit $x + 3 \equiv -1$ [7]. Donc $x + 3 \equiv -1$ [7] équivaut à $x \equiv -4$ [7], soit $x = -4 + 7k$ ($k \in \mathbb{Z}$).
$100 < x < 120$ équivaut à $100 < 4 + 7k < 120$,
soit $96 < 7k < 116$, soit $k = 14$ ou 15 ou 16,
d'où $x = 102$ ou 109 ou 116.

74

xmod3	0	1	2
x^2mod3	0	1	1
$2x^2$mod3	0	2	2

a. Soit $(x ; y)$ une solution, alors $2x^2 + 3y^2 = 16$. Or $16 \equiv 1$ [3] ; $3y^2 \equiv 0$ [3], d'où $2x^2 + 3y^2 \equiv 2 \times 2$ [3] ; On a donc $2x^2 \equiv 1$ [3].
b. On constate que la congruence $2x^2 \equiv 1$ [3] n'a pas de solution, donc l'équation $2x^2 + 3y^2 = 16$ n'a pas de solution.

Devoir de synthèse

135 Question 1 : cf. propriété 3.
Question 2 : cf. propriété 5.

136 Soit $(x ; y)$ une solution.
De $9x^2 - y^2 = 20$, donc $(3x - y)(3x + y) = 20$.
$y \geqslant 0$, donc $3x + y > 3x - y$. $20 = 20 \times 1 = 10 \times 2 = 5 \times 4$.

• si $(3x + y) = 20$ et $(3x - y) = 1$, alors $2y = 19$,
• si $(3x + y) = 10$ et $(3x - y) = 2$, alors $6x = 12$ et $2y = 8$
• si $(3x + y) = 5$ et $(3x - y) = 4$, alors $2y = 1$.
Il y a un seul couple solution (2, 4) et $36 - 16 = 20$.

137 Soit n un entier solution, alors $n + 3$ divise $4n + 7$ et $n + 3$, donc divise $4(n + 3) - (4n + 7) = 5$.
Les diviseurs de 5 sont -5, -1, 1 et 5, donc $n + 3 = -5$ ou $n + 3 = -1$ ou $n + 3 = 1$ ou $n + 3 = 5$ soit $n = -8$ ou $n = -4$ ou $n = -2$ ou $n = 2$. On vérifie que ces entiers sont bien solutions. Les solutions sont donc : -8, -4, -2 et 2.

138 Soit P_n la proposition : 7 divise $3^{2n+1} + 2^{n+2}$,
7 divise $3^{2\times0+1} + 2^{0+2} = 3 + 4 = 7$, donc P_0 est vraie.
Supposons P_n est vraie pour un certain n.
7 divise $3^{2n+1} + 2^{n+2}$, donc il existe un entier k tel que $3^{2n+1} + 2^{n+2} = 7k$, soit $3^{2n+1} = 7k - 2^{n+2}$.
$3^{2(n+1)+1} + 2^{(n+1)+2} = 3^2 \times 3^{2n+1} - 2 \times 2^{n+2} = 9(7 - 2^{n+2}) - 2^{n+2} \times 2 = -2^{n+2}(9 - 2) + 7(9k) = 7(-2^{n+2} + 9k)$.
$2^n + 9k$ est un entier, donc 7 divise $3^{2(n+1)+1} + 2^{n+1+2}$, donc P_{n+1} est vraie. Pour tout entier naturel n, 7 divise $3^{2n+1} + 2^{n+2}$.

139 **a.** Dans la division euclidienne par 3, il y a 3 restes possibles, donc tout entier relatif est de la forme $3k$ ou $3k + 1$ ou $3k + 2$ où $k \in \mathbb{Z}$.
b. Voir savoir-faire 7, en remplaçant $n^3 - 4n$ par $n^3 - 7n$.

140 **a.** Si d divise $3n + 13$ et $2n + 17$, alors d divise $-2(3n + 13) + 3(2n + 17) = 25$, donc $d = 1$ ou $d = 5$ ou $d = 25$.
D'autre part d divise $3n + 13 - (2n + 17) = n - 4$.
b. Donc $n = 4 + kd$, $k \in Z$. Les couples $(d ; n)$: $(1 ; k)$, $(5 ; 4 + 5k)$; $(25 ; 4 + 25k)$ sont tels que d divise $3n + 13$ et $2n + 17$.

141 $n^2 + 3n + 1 = n(n - 1) + 4(n - 1) + 5$.
Si $(n - 1)$ divise $n^2 + 3n + 1$, alors $(n - 1)$ divise $(n - 1)$ et $n(n - 1) + 4(n - 1) + 5$, donc $(n - 1)$ divise 5, donc $(n - 1) = -1$ ou $(n - 1) = 1$ ou $(n - 1) = 5$, donc $n = 0$ ou $n = 2$ ou $n = 6$.
Réciproquement, -1 divise 1, 1 divise 8, 5 divise 45 donc les entiers sont 0, 2 ou 6.

142 Supposons les a, b et c impairs. $a \equiv 1$ [2], donc $a^2 \equiv 1$ [2], donc $b^2 \equiv 1$ et $a^2 + b^2 \equiv 0$ [2], et $c^2 \equiv 1$. C'est impossible, donc l'un au moins des trois entiers naturels a, b et c est pair.

143 Cf. propriété 11.

144 **a.** $5^2 = 25 = 26 - 1$, donc $5^2 \equiv (-1)$ [13] et $5^4 \equiv 1$ [13], d'où $5^{4n} \equiv 1$ [13], donc $5^{4n+1} \equiv 5$ [13], $5^{4n+2} \equiv 12$ [13], $5^{4n+3} \equiv 8$ [13].
b. $1981 = 152 \times 13 + 5$, donc $1981 \equiv 5$ [13], d'où $1981^{1981} \equiv 5^{1981}$ [13]. Or $1981 = 495 \times 4 + 1$, donc le reste de la division euclidienne de 1981^{1981} par 13 est 5.
c. $31 = 26 + 5$ donc $31 \equiv 5$ [13] et $18 = 13 + 5$, donc $18 \equiv 5$ [13], d'où $31^{4n+1} + 18^{4n-1} \equiv 5^{4n+1} + 5^{4n-1} \equiv 5 + 8$ [13], donc pour tout n non nul, $31^{4n+1} + 18^{4n-1}$ est divisible par 13.

145 **a.** $11 \equiv 1$ [5] et $7 \equiv 2$ [5], donc si $11x^2 - 7y^2 = 5$ (E), alors $x^2 \equiv 2y^2$ [5] (E').
b.

Modulo 5, x est congru à	0	1	2	3	4
Modulo 5, x^2 est congru à	0	1	4	4	1

Modulo 5, y est congru à	0	1	2	3	4
Modulo 5, $2y^2$ est congru à	0	2	3	3	2

c. Le seul couple $(x ; y)$ qui vérifie (E') est (0,0), donc x et y sont des multiples de 5.
d. Soit $(x ; y)$ solution de (E). $x = 5x'$, $y = 5y'$,
donc $25(11x'^2 - 7y'^2) = 5$, d'où $5(11x'^2 - 7y'^2) = 1$
et 5 divise 1, ce qui est faux. (E) n'a donc pas de solution.

146 **1. a.** $12 = 4 \times 3$, donc $12 \equiv 0$ [3] et par somme, $N \equiv a_0$ [3].
b. Un nombre écrit en base 12 est divisible par 3 si, et seulement si, son dernier chiffre l'est.
2. a. $12 \equiv 1$ [11], donc $N \equiv a_n + \ldots + a_1 + a_0$ [3].
b. Un nombre écrit en base douze est divisible par 11 si, et seulement si, la somme de ses chiffres l'est.
3. Soit en base 12, $N = \overline{\beta 1 \alpha}$. N est divisible par 3 si α l'est.
Or $\alpha = 10$ n'est pas divisible par 3. N est divisible par 11 si $\beta + 1 + \alpha$ l'est. Or $\beta + 1 + \alpha = 11 + 1 + 10 = 22$ est divisible par 11, donc N est divisible par 11, mais pas par 3.

2 PGCD, théorèmes de Bézout et de Gauss

Appliquer les capacités attendues

18 **a.** Soit d un diviseur commun de a et b. d divise $1a + (-6)b = a - 6b$. d divise $a - 6b$ et b. D'où $D(a ; b) \subset D(a - 6b, b)$.
Réciproquement, soit d un diviseur commun de $a - 6b$ et b, alors d divise $(a - 6b) + 6b = a$, donc d est un diviseur commun de a et b, d'où $D(a - 6b, b) \subset D(a ; b)$. Donc $D(a ; b) = D(a - 6b, b)$.
b. On déduit $PGCD(a ; b) = PGCD(a - 6b, b)$.

23 On vérifie que 66 divise 1 320 ($1\,320 = 66 \times 20$). Soit b une solution, $PGCD(a ; b) = 66$, donc 66 divises b, donc $b = 66k$ ($k \in \mathbb{Z}$). On a aussi $400 < b < 700$, d'où $400 < 66k < 700$, soit $\frac{400}{66} < k < \frac{700}{66}$, k étant un entier cela équivaut à $6 < k < 11$. Les valeurs possibles de k sont 7, 8, 9, 10.
• $k = 7$ alors $b = 462$ et $PGCD(1\,320 ; 462) = 66$.
• $k = 8$ alors $b = 528$ et $66 \times 2 = 132$ est un diviseur commun de 1 320 et 528, donc $PGCD(a ; b) \neq 66$.
• $k = 9$ alors $b = 594$ et $PGCD(1\,320 ; 54) = 66$.
• $k = 10$ alors $b = 660$ et $PGCD(a ; b) = 660 \neq 66$.
Le problème a deux solutions : $b = 462$ et $b = 594$.

25 **a.** Si d divise a et b, alors d divise $a - b$ et b. Réciproquement si d divise $a - b$ et b, alors d divise $(a - b) + b = a$ et b. On en déduit : $D(a ; b) = D(a - b ; b)$, d'où $PGCD(a ; b) = PGCD(a - b ; b)$.
b. On applique plusieurs fois cette propriété.
$PGCD(616 ; 280) = PGCD(616 - 280 ; 280) = PGCD(336 ; 280) = PGCD(336 - 280 ; 280) = PGCD(56 ; 280) = PGCD(56 ; 280 - 56) = PGCD(56 ; 224) = PGCD(56 ; 224 - 56) = PGCD(56 ; 168) = 56$, car $168 = 3 \times 56$.

30 **a.** On sait que $PGCD(a ; b) = PGCD(a - kb ; b)(k \in \mathbb{Z})$. Donc $PGCD(n ; 3n + 7) = PGCD(n ; 3n + 7 - 3n) = PGCD(n ; 7)$.
b. Si n est un multiple de 7, alors $PGCD(n ; 7) = 7$, donc d'après a. $PGCD(n ; n + 7) = 7$.
c. Si n n'est pas un multiple de 7, alors 7 n'est donc pas un diviseur commun de n et de 7 et donc $PGCD(n ; 7) = 1$.
En conclusion : Si n est multiple de 7. Donc $PGCD(n ; n + 7) = 1$; si n n'est pas multiple de 7. Donc $PGCD(n ; n + 7) = 1$.

34 On utilise encore "$PGCD(a ; b) = PGCD(a - kb ; b)$".
$PGCD(2a + b ; 3a + b) = PGCD(2a + b ; 3a + b - (2a + b)) = PGCD(2a + b ; a) = PGCD(2a + b - 2a ; a) = PGCD(b ; a)$.
D'où $PGCD(2a + b ; 3a + b) = PGCD(a ; b)$.

36 On utilise l'algorithme d'Euclide.
a. $2\,400 = 210 \times 11 + 90$ et $0 \leqslant 90 < 210$.
$210 = 90 \times 2 + 30$ et $0 \leqslant 30 < 90$. $90 = 30 \times 3 + 0$.
D'où $PGCD(2\,400 ; 210) = PGCD(210 ; 90) = PGCD(90 ; 30) = 30$.
b. $792 = 660 \times 1 + 132$ et $0 \leqslant 132 < 660$.
$660 = 132 \times 5 + 0$. Le PGCD est le dernier reste non nul, d'où : $PGCD(2\,400 ; 210) = 30$.
c. $128 = 48 \times 2 + 32$ et $0 \leqslant 32 < 48$. $48 = 32 \times 1 + 16$ et $0 \leqslant 16 < 32$. $32 = 16 \times 2 + 0$. Donc $PGCD(128 ; 48) = 16$.

40 Les diviseurs positifs de 2 574 et 630 sont les diviseurs positifs de leur PGCD. $PGCD(2\,574 ; 630) = 18$.
Or $18 = 1 \times 18 = 2 \times 9 = 3 \times 6$. Les diviseurs positifs communs de a et b sont : 1, 2, 3, 6, 9 et 18.

45 **a.** $PGCD(-240 \times 17 ; 240 \times 9) = 240\ PGCD(-17 ; 9)$.
Or $PGCD(-17 ; 9) = 1$, d'où $PGCD(a ; b) = 240$.

b. PGCD(4 000 ; 700) = 100 PGCD(40 ; 7).
Or PGCD(40 ; 7) = 1, d'où PGCD(a ; b) = 100.
c. PGCD(3 600 ; 21 000) = 100 PGCD(36 ; 210)
= 100 × 6 PGCD(6 ; 35). Or PGCD(6 ; 35) = 1, donc PGCD(a ; b) = 600.

49 **a.** Faux. Contre-exemple : 3 et 5 sont premiers entre eux mais 3 + 5 = 8 et 5 – 3 = 2 ne sont pas premiers entre eux.
b. Vrai. Soit d un diviseur commun de a et b, alors d divise $a + b$ et $a - b$, donc d divise leur PGCD qui est égal à 1 puisque $a + b$ et $a - b$ sont premiers entre eux. On en déduit que les seuls diviseurs communs a et b sont +1 et –1, donc a et b sont premiers entre eux.

53 **a.** PGCD(n ; $3n + 1$) = PGCD(n ; $3n + 1 - 3n$) = PGCD(n ; 1) = 1 ; donc n et $3n + 1$ sont premiers entre eux.
b. n et $3n + 1$ sont premiers entre eux, la fraction $\frac{n}{3n+1}$ est donc irréductible.

57 a et b jouent un rôle symétrique, on cherchera les couples (a ; b) tels que $a \leqslant b$. Soient (a ; b) un couple d'entiers naturels solution. PGCD(a ; b) = 14, donc il existe deux entiers naturels a' et b' premiers entre eux tels que $a = 14a'$ et $b = 14b'$.
$a + b = 210$ implique $14a' + 14b' = 210$, soit $a' + b' = 15$.
a' et b' sont premiers entre eux tels que $a' + b' = 15$. $a' = 1$, $b' = 14$ ou $a' = 2$, $b' = 13$ ou $a' = 4$, $b' = 11$ ou $a' = 7$, $b' = 8$, ce qui correspond aux couples : (14 ; 196), (28 ; 182), (56 ; 154), (98 ; 112).
Réciproquement : On vérifie que ces couples sont solutions.
Les solutions sont donc les couples (14 ; 196), (28 ; 182), (56, 154) et (98, 112).

62 On cherche à l'aide l'algorithme d'Euclide deux entiers relatifs u et v tels que $88u + 63v = 1$. On pose $a = 88$ et $b = 63$,

$88 = 63 + 25$	$25 = a - b$
$63 = 25 \times 2 + 13$	$13 = b - 2(a - b) = 3b - 2a$
$25 = 13 \times 1 + 12$	$12 = (a - b) - (3b - 2a) = 3a - 4b$
$13 = 12 \times 1 + 1$	$1 = (3b - 2a) - (3a - 4b) = 7b - 5a$
$12 = 12 \times 1 + 0$	

$(-5)88 + 7 \times 63 = 1$, donc on a trouvé un couple d'entiers relatifs (u ; v) = (–5 ; 7) tel que $88u + 63v = 1$, d'après le théorème de Bézout, 88 et 63 sont premiers entre eux.

67 **a.** $(-3)n + (3n + 1) = 1$, on a donc trouvé un couple (u, v) tel que $au + bv = 1$, d'après le théorème de Bézout, $a = n$ et $b = 3n + 1$ sont premiers entre eux.
b. $3(2n + 1) - 2(3n + 1) = 1$. a et b sont premiers entre eux.

73 **a.** Soit (a ; b) un couple d'entiers relatifs tels que $5a = 7b$. 5 divise $7b$, or 5 est premier avec 7, d'après le théorème de Gauss 5 divise b, $b = 5k$ ($k \in \mathbb{Z}$). $5a = 7(5k)$, soit $a = 7k$. Donc si (a ; b) est solution alors il existe $k \in \mathbb{Z}$ tel que $a = 7k$ et $b = 5k$.
b. Réciproquement s'il existe $k \in \mathbb{Z}$ tel que (a ; b) = ($7k$; $5k$) alors $5(7k) = 7(5k)$, donc (a, b) est solution de l'équation $5a = 7b$. Les solutions sont les couples ($7k$; $5k$) où $k \in \mathbb{Z}$.

76 **a.** On pose N = 38 808. N est divisible par 9 (3 + 8 + 8 + 0 + 8 = 27 est divisible par 9). N est aussi divisible par 2. N est pair. N est donc divisible par 2 et 9 qui sont premiers entre eux, on en déduit que N est divisible par leur produit 2 × 9 = 18.
b. 3 – 8 + 8 – 0 + 8 = 11 est divisible par 11, donc, N est divisible par 11. N est donc divisible par 18 et 11 qui sont premiers entre eux, donc par 11 × 18 = 198.

79 **a.** 9 et 14 sont premiers entre eux, donc il existe des entiers relatifs x_0 et y_0 tels que $9x_0 + 14y_0 = 1$, d'où $9x_0 - 14(-y_0) = 1$. Il existe donc un couple (u ; v) = (x_0 ; $-y_0$) d'entiers relatifs tels que $9u - 14v = 1$.
L'équation $9x - 14y = 1$ admet donc une solution (u ; v).
b. De $9u - 14v = 1$, on déduit $9(11u) - 14(11v) = 11$, donc le couple (u_1 ; v_1) = ($11u$; $11v$) est solution de l'équation $9x - 14y = 11$.
c. $18x - 28y = 6$ équivaut à $9x - 14y = 3$. D'après le même raisonnement qu'en **b**, (u_2 ; v_2) = ($3u$; $3v$) est solution de cette équation.
d. On raisonne par l'absurde : si l'équation admettait une solution, 2 divisant le 1er membre devrait diviser 3, ce qui est faux. Donc l'équation n'a pas de solution dans $\mathbb{Z}$.

83 **a.** On remarque que $4 \times 2 - 3 \times 2 = 2$, donc une solution évidentes est le couple (x_0 ; y_0) = (2 ; 2).
b. D'après **a.** $4x_0 - 3y_0 = 2$. Donc $4x - 3y = 2$ équivaut à $4x - 3y = 4x_0 - 3y_0$ soit $4(x - x_0) = 3(y - y_0)$ (E')
c. • Soit (x ; y) une solution de (E) ou de (E').
On a donc $4(x - x_0) = 3(y - y_0)$ (E'). On en déduit que 4 divise $3(y - y_0)$, comme 4 est premier avec 3, d'après le théorème de Gauss, 4 divise $(y - y_0)$, donc il existe $k \in \mathbb{Z}$ tel que $y - y_0 = 4k$.
De l'équation (E') on déduit : $4(x - x_0) = 3 \times 4k$, d'où $x - x_0 = 3k$.
Donc si (x ; y) est solution de (E) alors il existe un entier relatif k tel que $x - x_0 = 3k$ et $y - y_0 = 4k$.
• Réciproquement, si $(x ; y) = (x_0 + 3k ; y_0 + 4k)$ alors $4 \times 3k = 3 \times 4k$, donc l'équation (E') est vérifiée, donc aussi l'équation équivalente (E).
• Conclusion : Les solutions sont les couples $(2 + 3k ; 2 + 4k)$ où k est un entier relatif.

Devoir de synthèse

114 **a.** Pour tout entier relatif k, $-5(12k+7)+12(5k+3) = 1$. D'après le théorème de Bézout $(12k+7)$ et $(5k+3)$, sont premiers entre eux.
b. $51x + 69y = 3(17x + 23y)$ est un multiple de 3 donc l'équation $51x + 69y = 1$ n'a pas de solutions.
c. $a = 11a'$ et $b = 11b'$ donc $a' + b' = 12$, a' et b' sont premiers entre eux donc $a' = 1$ et $b' = 11$ ou $a' = 5$ et $b' = 7$ ou $a' = 7$, $b' = 5$ ou $a' = 11$, $b' = 1$. On obtient a et b en multipliant a' et b' par 11. On vérifie que les couples obtenus conviennent. Les solutions sont donc {(11, 121), (55, 77), (77, 55), (121, 11)}

115 **a.** (E) : $7x - 3y = 1$. (1, 2) est solution de (E). Si (x, y) solution, alors $7x - 3y = 7.1 - 3.2$ donc $7.(x - 1) = 3(y - 2)$. D'après le théorème de Gauss, 3 divise $7(x - 1)$ et est premier avec 7 donc divise $x - 1$ et $x - 1 = 3k$. En remplaçant, $y - 2 = 7k$. Réciproquement, $(1 + 3k, 2 + 7k)$ est bien solution, donc les solutions sont de la forme $(1 + 3k, 2 + 7k)$.
b. 7 + 3 = 10 et 70 – 60 = 10, donc (1, –1) et (10, 20) sont bien solutions de (E') : $7x - 3y = 10$.
2. (1, –1) n'est pas de la forme $(10k + 30, 20k + 70)$, donc le raisonnement est faux. Par une étude analogue au 1, on montre que les solutions sont de la forme $(1 + 3k, -1 + 7k)$.

116 **a.** Faux : $2x + 3y = 5$ a pour solution (1, 1).
b. Faux, PGCD(2, 3) = 1 et : $2x + 3y = 5$ a des solutions.
c. Faux, l'équation $3x + 6y = 2$ n'a pas de solution, 3 divise $(3x + 6y)$ et 3 ne divise pas 2.
d. Vrai, si d = PGCD(a, b) divise c, alors en posant $a = da'$, $b = db'$, $c = dc'$, $ax + b = c$ équivaut à $a'x + b'y = c'$ qui a toujours des solutions, a' et b' étant premiers entre eux.

117 **a.** $a = 2n^3 + 5n^2 + 4n + 1 = 2n^3 + n^2 + 4n^2 + 2n + 2n + 1 = n^2(2n + 1) + 2n(2n + 1) + (2n + 1) = (2n + 1)(n^2 + 2n + 1)$
$b = 2n^2 + n = n(2n + 1)$, donc $(2n + 1)$ divise a et b.
b. $c - d(n + 2) = n^2 + 2n + 1 - (n^2 + 2n) = 1$ donc c et d sont premiers entre eux.
c. Par homogénéité du PGCD, PGCD(a, b) = $(2n + 1)$.
PGCD(c, d) = $2n + 1$.

118 **a.** 5 divise 65 et 40 et ne divise pas 1 donc l'équation $65x - 40y = 1$ n'a pas de solution dans $\mathbb{Z}^2$.
b. 40 et 17 sont premiers entre eux donc d'après le théorème de Bézout, (E) $17x - 40y = 1$ admet au moins une solution dans $\mathbb{Z}^2$.
c. $40 = 2 \times 17 + 6$, donc $6 = 40 - 2 \times 17$. $17 = 2 \times 6 + 5$ donc $5 = 17 - 2 \times 6 = 17 - 2 \times (40 - 2 \times 17) = 5 \times 17 - 2 \times 40$.
$6 = 5 + 1$, donc $1 = 6 - 5 = (40 - 2 \times 17) - (5 \times 17 - 2 \times 40)$, donc $1 = 3 \times 40 - 7 \times 17$. $(-7, -3)$ est alors solution particulière de (E).
d. Par la méthode de 115 **a.** les solutions sont de la forme $(-7 + 40k, -3 + 17k)$
e. $-17x \equiv 1$ [40] si et seulement si il existe un entier relatif y tel que $17x - 40y = 1$. D'après **d.**, x est de la forme $-7 + 40k$. 33 convient et si $k > 1$, $x > 40$ et si $k \leqslant 0$, $x \leqslant 0$. 33 est l'unique entier naturel x_0 inférieur à 40 tel que $17x_0 \equiv 1$ [40].
f. si $a^{17} \equiv b$ [55] , alors par compatibilité avec les puissances, $a^{17.33} \equiv b^{33}$ [55]. Or d'après **e.** il existe k tels que $17.33 = 1 + 40k$, donc, $a^{17.33} =, a^{1+40k} = a.a^{40k}$. Enfin, si, $a^{40} \equiv 1$ [55], alors $a^{40k} \equiv 1$[55] donc $a^{17.33} \equiv a$ [55] et $a \equiv b^{33}$ [55].

119 **a.** Vrai, car 2 est premier avec 7 (Gauss).
b. Faux. Contre exemple : $3 \times 7 - 5 \times 3 = 6$ et PGCD(7 ; 3) = 1.
c. Vrai (Bézout).
d. Vrai, 4 et 15 étant premiers entre eux.
e. Vrai, car $p = 5n - 3$ et $q = n + 1$, donc $p = 5q - 8$ et PGCD(p ; q) = PGCD (q, –8) = PGCD(8 ; n + 1).

120 **a.** Cf cours propriété 10 p. 54.
b. L'algorithme cherche le plus petit entier x tel que $ax \equiv 1$ [b]. Une fois qu'il l'a trouvé, il cherche y tel que $ax + by = 1$. Il donne donc les coefficients de Bézout associés à deux nombres premiers entre eux.

121 **1.** Voir propriété 11 p. 54.
2. a. $29 = 19 + 10$, donc $10 = 29 - 19$, $19 = 10 + 9$ donc $9 = 19 - 10 = 2 \times 19 - 9$ et $10 = 9 + 1$ donc $1 = 10 - 9 = -3 \times 19 + 2 \times 29$ donc (–3, 2) est alors une solution particulière de (E) : $19x + 29y = 1$.
b. (–2 454, 1 636) est une solution particulière de l'équation $19x + 29y = 818$ (E').
c. Par la méthode de 115 **a.** les solutions sont de la forme $(-2\,454 + 29k, 1\,619 - 19k)$ $(k \in \mathbb{Z})$
3. Soit x le nombre d'abonnés et y celui des non abonnés, x et y étant entiers naturels. $19x + 29y = 818$ donc d'après **2.c.**, $x = -2\,454 + 29k \geqslant 0$ et $y = 1\,636 - 19k \geqslant 0$ donc

$$\frac{2\,454}{29} \leqslant k \leqslant \frac{1636}{19}.$$

On en déduit que $k = 85$, $x = 29 \times 85 - 2\,454 = 11$ et $y = 1\,636 - 19.\ 85 = 4$.La caissière a vendu 11 places au tarif abonné et 21 au tarif non abonné.

122 **1. a.** Si a est premier avec b, alors d'après le théorème de Bézout, il existe deux entiers relatifs, u et v tels que $au + bv = 1$, donc $au - av + av + bv = 1$, donc $a(u - v) + (a + b)v = 1$ donc a est premier avec $a + b$.
b. $(au + bv)^2 = 1$ donc $a(au^2 + 2abv) + v^2b^2$ et a est premier avec b^2.
2. a. Si d divise a et $a + b$, alors d divise a et $a + b - a$, donc d divise a et b ; a étant premier avec b, $d = 1$, donc a est premier avec $a + b$.
b. Soit d tel que d divise a et b^2 ; a est premier avec b donc d est premier avec b donc d'après Gauss, d divise b, donc $d = 1$ et a est premier avec b^2.

3 Nombres premiers

Appliquer les capacités attendues

22 **a.** 15790 est divisible par 10.
b. 21457894 est pair, divisible par 2.
c. 465325 est terminé par 5, donc divisible par 5.
d. 123456789 est divisible par 3, la somme de ses chiffres est un multiple de 3.

34 $a \geqslant 2$, $b \geqslant 2$, donc $p \geqslant 4$ et p premier, donc p impair.
Si a et b sont pairs, $a + b$ est pair et si a et b sont impairs, $a + b$ pairs donc a et b sont de parité différentes.
Si d divise a et d divise b, alors d divise p. Or p premier donc $d = 1$ ou $d = p$. Or $a + b = p$ et $b > 0$ donc $a < p$; de même $b < p$ donc $d = 1$ et que a et b sont premiers entre eux.

42 **a.** 5 est premier donc premier avec 2. Par Bézout, l'équation $2x - 5y = 1$ a des solutions. Par étude de tous les cas,
$2 \times 1 \equiv 2$ [5], $2 \times 2 \equiv 4$ [5], , $2 \times 3 \equiv 1$ [5] et $2 \times 4 \equiv 3$ [5].
Il existe un unique entier x de [1, 4] tel que : $2x \equiv 1$ [5], à savoir 3
b. L'équation $2x \equiv 3$ [5] a une unique solution entière dans [1, 4], à savoir 4.

47 Un nombre dont la décomposition en facteurs premiers n'a que des exposants pairs est un carré parfait.
$a = 2^4 \times 3^6 \times 7^2 = (2^2 \times 3^3 \times 7)^2$.
$b = 3^2 \times 5^4 \times 7^6 = (3 \times 5^2 \times 7^3)^2$.

55 **a.** $d = \text{PGCD}(a, b) = 3^2 \times 7^2 = 441$.
b. $a' = 2^3 \times 3^3 = 216$ et $b' = 5^4 \times 7^4 = 1500625$.
c. $m = 2^3 \times 3^5 \times 5^4 \times 7^6 = 142\,943\,535\,000$.
d. $\dfrac{a}{b} = \dfrac{a'}{b'} = \dfrac{216}{1500625}$.
e. $\dfrac{1}{a} + \dfrac{1}{b} = \dfrac{1}{da'} + \dfrac{1}{db'} = \dfrac{b'}{da'b'} + \dfrac{a'}{da'b'} = \dfrac{b' + a'}{da'b'}$,
donc $\dfrac{1}{a} + \dfrac{1}{b} = \dfrac{1500841}{m}$. $a' + b'$ n'est divisible ni par 2, ni par 3, ni par 5 ni par 7, donc la fraction est irréductible.

Devoir de synthèse

96 **1.** Définition 1 p. 82. **2.** Propriété 1 p. 82.
3. $N = 2 \times 3 \times 5 \times 7 + \times 11 + 1$. $N \equiv 1$ [2], $N \equiv 1$ [3], $N \equiv 1$ [5], $N \equiv 1$ [7], $N \equiv 1$ [11]. Donc n'est divisible ni par 2, ni par 3, ni par 5, ni par 7 ni par 11. De plus, $N = 2311$ n'est pas divisible par 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, nombres premiers inférieurs à sa racine carrée. N est premier.

97 **1.** Cet algorithme teste si N est divisible par un nombre impair supérieur à 3. La partie décimale de $\dfrac{N}{T}$ est nulle si, et seulement si, T divise N.
2. $N = 293717$ est premier.

98 **a.** $ab = 2595 = 3^4 \times 2^5$. Or $a = da'$ et $b = db'$ donc $ab = d^2a'b'$ donc d^2 divise $3^4 \times 2^5$. Il existe n et m tels que $d^2 = 2^n \times 3^m$ avec n et m sont pairs $n = 2n'$, $m = 2m'$
b. $d = 2^{n'} \times 3^{m'}$ a 6 diviseurs, donc $(n' + 1)(m' + 1) = 6$. $n' \leqslant 2$, $n' + 1 \leqslant 3$, $m' \leqslant 2$ et $m' + 1 \leqslant 3$. Soit $n' = 1$, $m' = 2$ donc $d = 3 \times 2^2 = 12$, soit $n' = 2$, $m' = 1$, donc $d = 3^2 \times 2 = 18 > 15$, donc $d = 3 \times 2^2$, $d^2 = 2^4 \times 3^2$, $a'b' = 2 \times 3^2$. $a' < b'$ et a' et b' sont premiers entre eux donc $a' = 2$ et $a = 24$, $b' = 9$ et $b = 108$.

99 **1.** Tout nombre entier n s'écrit $4k$, $4k + 1$, $4k + 2$, $4k + 3$. Si p est premier supérieur strictement à 2, il est impair alors $p \equiv 1$ (mod 4) ou $p \equiv 3$ (mod 4).
2. a. Soit p supérieur ou égal à 5 et différent de 3, donc $p \equiv 1$ (mod 3) ou $p \equiv 2$ (mod 3). Dans les deux cas, $p^2 \equiv 1$ (mod 3), donc $p^2 - 1$ est divisible par 3.
b. $p \geqslant 5$ donc $p > 2$.
Si $p = 4k + 1$, $p^2 - 1 = 16k^2 + 8k = 8k(2k + 1)$.
Si $p = 4k + 3$, $p^2 - 1 = 16k^2 + 24k + 8 = 8(2k + 3k + 1)$.
$p^2 - 1$ est divisible par 8.
c. $p^2 - 1$ est divisible par 3 et 8 premiers entre eux est divisible par 24.

100 **1.** $a = 276 = 2^2 \times 3 \times 23$ et $D_a = \{1, 2, 3, 4, 6, 12, 23, 46, 69, 92, 138, 276\}$

2. $b = 342 = 2 \times 3^2 \times 19$ et $D_a = \{1, 2, 3, 6, 9, 18, 19, 38, 57, 112, 171, 342\}$

3. a. $d = \text{PGCD}(a ; b) = 2 \times 3 = 6$

b. $d = \text{PGCD}(a ; b) = \text{PGCD}(da' ; db') = d\text{PGCD}(a' ; b')$. Or $d \neq 0$ donc $d\text{PGCD}(a' ; b') = 1$ et a' et b' sont premiers entre eux.

c. $a' = 2 \times 23 = 46$, $b' = 3 \times 19 = 57$,
$m = da'b' = 2^2 \times 3^2 \times 19 \times 23 = 31464$.

d. $\frac{a}{b} = \frac{a'}{b'} = \frac{46}{57}$

$\frac{1}{a} + \frac{1}{b}\frac{1}{da'} + \frac{1}{db'} = \frac{b'}{da'b'} + \frac{a'}{da'b'} = \frac{b'+a'}{da'b'} = \frac{103}{31464}$.

101 **1.** p est premier donc p^2 admet 1, p, p^2 comme diviseurs. Soient x et y tels $x^2 - y^2 = p^2$.

2. a. si x est pair et y est impair alors, $x^2 - y^2$ est impair, idem pour x impair et y pair donc, que x et y ont même parité.

b. $(x-y)(x+y) = 4$ donc, $(x-y) = 1$ et $(x+y) = 4$, impossible ou $x - y = 2$ et $x + y = 2$ donc, $x = 2$ et $y = 0$.

3. a. $p \neq 2$ et p est premier donc, p est impair et $p^2 - 1$ pair.

b. $(x-y)(x+y) = p^2$ donc, $(x-y) = 1$ et $(x+y) = p^2$,

donc $x = \frac{p^2+1}{2}$ et $y = \frac{p^2-1}{2}$ ou $x - y = p$ et $x + y = p$

donc $x = p$ et $y = 0$. Les solutions sont $(\frac{p^2+1}{2}, \frac{p^2-1}{2})$ et $(p, 0)$.

102 **a.** $2^{11} - 1 = 2047$. On cherche les diviseurs premiers possibles et on trouve $2047 = 23 \times 89$.

b. $2^p = 2^p - 1 + 1$, donc $2^p \equiv 1[2^p - 1]$, donc par puissance, $2^{pq} \equiv 1[2^p - 1]$ et $1 \leqslant [2^p - 1]$, donc $2^{pq} - 1$ est divisible par $2^p - 1$. On montre de même que $2^{pq} - 1$ est divisible par $2^q - 1$.

c. On en déduit que si n est non premier, $n = pq$, $p > 1$, $q > 1$, $2^n - 1$ est divisible par $2^q - 1 > 1$ donc non premier. Par contraposée, si $2^n - 1$ est premier, alors n est premier. La réciproque est fausse, 11 est premier et $2^{11} - 1$ n'est pas premier.

103 Soit n un entier naturel. Soit $P(n)$ l'ensemble des entiers strictement positifs, inférieurs à n, premier avec n.

a. $P(2) = \{1\}$, donc $\varphi(2) = 1$. $P(3) = \{1, 2\}$, $\varphi(3) = 2$. $P(4) = \{1, 3\}$, $\varphi(4) = 2$. $P(5) = \{1, 2, 3, 4\}$, $\varphi(5) = 4$. $P(6) = \{1, 5\}$, $\varphi(6) = 2$. $P(7) = \{1, 2, 3, 4, 5, 6\}$, $\varphi(7) = 6$.

b.
```
Après Lire N        X = X +1          Affiche Dim (L1)
Efface liste L1     A = D
....                FinTanQue
```

c. p premier est premier avec tout nombre qui lui est inférieur donc $\varphi(p) = p - 1$

d. $n = pq$, p et q premiers distincts. Il y a q multiples de p inférieurs ou égaux à n et p multiples de q inférieurs ou égaux à n et un multiple de pq. Tous les autres nombres sont premiers avec pq. $\varphi(pq) = pq - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1)$.

e. Les nombres premiers avec p^n sont tous les nombres qui ne sont pas mutiples de p. Il y a p^{n-1} multiples de p inférieurs ou égaux à p^n. $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$

f. Si $n = p^r q^m$ avec p et q premiers distincts, on pourrait envisager $\varphi(n) = p^{r-1}(p-1)\, q^{m-1}(q-1)$

$\varphi(36) = 12$ et $36 = 2^2 \times 3^2$ et $12 = 2(2-1).\ 3(3-1)$ et la conjecture semble vérifiée.

4 Matrices

Appliquer les capacités attendues

11 **a.** La taille de la matrice est 1×4. Pour CASIO, TI et Maxima il faut d'abord indiquer ces dimensions avant d'entrer les coefficients.
Pour Xcas, on saisit A:=matrix([[1,–2,3,–4]]).
En JavaScript, on saisit A=[[1,–2,3,–4]].

b. La taille est 3×1. Pour Xcas, on saisit A:=matrix([[4],[–5],[6]]).
En JavaScript, on saisit A=[[4],[–5],[6]].

c. La taille est 3×2.
Pour Xcas, on saisit A:=matrix([[12,–15],[7,2],[–1,4]]).
En JavaScript, on saisit A=[[12,–15],[7,2],[–1,4]].

d. La taille est 2×4
Pour Xcas, on saisit A:=matrix([[1,2,3,4],[–5,–6,–7,–8]]).
En JavaScript, on saisit A=[[1,2,3,4],[–5,–6,–7,–8]].

17
```
Pour i = 1 à 6 faire
    Pour j = 1 à 3 faire
        A_ij = i + j ;
    FinPour
FinPour
```

23 Les matrices sont de même taille, $A + B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

29 **a.** Le nombre de colonne de A est égal au nombre de ligne de B, donc le produit AB est calculable et la matrice produit est de taille 1×1. On a donc : $AB = \begin{pmatrix} -42 \end{pmatrix}$.

b. Le nombre de colonne de A est égal à 3, qui est différent du nombre de lignes de B, égal à 1. AB n'est pas calculable.

37 Pour une matrice 2×2, on commence par calculer $ad - bc = 3 \times 2 + 5 \times 4 = 26 \neq 0$. Donc A admet un inverse. Notons $A^{-1} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ et on a donc $AA^{-1} = \begin{pmatrix} 4b + 3a & 4d + 3c \\ 2b - 5a & 2d - 5c \end{pmatrix}$.

On résout alors le système

$$\begin{cases} 4b + 3a = 1 \\ 4d + 3c = 0 \\ 2b - 5a = 0 \\ 2d - 5c = 1 \end{cases} \Leftrightarrow a = \frac{1}{13};\ b = \frac{5}{26};\ c = -\frac{2}{13};\ d = \frac{3}{26}.$$

44 **a.** Le système s'écrit $\begin{pmatrix} -4 & 3 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ et la matrice est inversible.

b. Il se résout donc ainsi : $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & 3 \\ -1 & 4 \end{pmatrix}\begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 13 \\ 18 \end{pmatrix}$.

Devoir de synthèse

80 **1.** B doit avoir un nombre de lignes égal à 7. Les bonnes réponses sont donc b. et c.

2. B doit avoir un nombre de colonnes égal à 5. Les bonnes réponses sont b. et d.

3. Les matrices doivent avoir la même taille : réponse a.

4. a. **5.** a.

81 **1.** Faux. **2.** Vrai. **3.** Faux.

4. Faux, par exemple A de taille 2×2 et B de taille 2×1.

5. Faux, par exemple A de taille 2×3 et B de taille 3×2.

6. Faux, il n'est pas spécifié que le système est linéaire.

82 $AB = \begin{pmatrix} -58 \\ -1 \end{pmatrix}$.

83 **1.** $(A + I_3)^3 = 0$.

2. $(A + I_3)^3 = A^3 + 3A^2 + 3A + I_3$.

3. $A^3 + 3A^2 + 3A + I_3 = A(A^2 + 3A + 3I_3) + I_3 \Leftrightarrow$
$A(-A^2 - 3A - 3I_3) = I_3$. Il existe donc une matrice $N = -A^2 - 3A - 3I_3$ telle que $AN = I_3$. Par unicité, $A^{-1} = -A^2 - 3A - 3I_3$.

84 $A = \begin{pmatrix} 1 & 0 & -1 & -2 \\ 3 & 2 & 1 & 0 \\ 5 & 4 & 3 & 2 \end{pmatrix}$.

85 **1.** Si $A = A^{-1}$, alors $A^2 = I_2$ en multipliant chaque membre de l'égalité par A. Réciproquement, si $AA = I_2$, alors A admet une matrice inverse qui est égale à A par unicité de l'inverse d'une matrice.

2. $A^2 = \begin{pmatrix} bc + a^2 & bd + ab \\ cd + ac & d^2 + bc \end{pmatrix}$. Le système est immédiat.

3. a. On procède par disjonction de cas.
Si $d = -a$, alors les 2e et 3e équations disparaissent et la 1re et 4e sont alors équivalentes entre elles.
Si $d \neq -a$, alors les 2e et 3e équations sont équivalentes à $b = c = 0$ et dans ce cas, les 1re et 4e sont équivalentes à $a^2 = d^2 = 1$.
b. Si $b = 0$, alors $a^2 = 1 \Leftrightarrow a = 1$ ou $a = -1$. Dans ce cas, les matrices possibles sont de la forme suivante :
$A = \begin{pmatrix} 1 & 0 \\ c & -1 \end{pmatrix}$ et $A = \begin{pmatrix} -1 & 0 \\ c & 1 \end{pmatrix}$, c étant un réel quelconque.

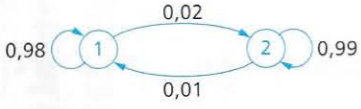
Si $b \neq 0$, alors $c = \dfrac{1 - a^2}{b}$ et la matrice A est de la forme :

$$A = \begin{pmatrix} a & b \\ \dfrac{1 - a^2}{b} & -a \end{pmatrix}$$

c. $a^2 = 1 \Leftrightarrow a = 1$ ou $a = -1$. De même pour d. Les matrices A possibles sont donc :

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

86 **1. a.**



b. $P = \begin{pmatrix} 0{,}98 & 0{,}01 \\ 0{,}02 & 0{,}99 \end{pmatrix}$. **2. a.** $u = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

b. On calcule $Pu = \begin{pmatrix} 0{,}01 \\ 0{,}99 \end{pmatrix}$, donc après une minute, le composant est en panne avec une probabilité de 1 %. On calcule ensuite $P^2u = \begin{pmatrix} 0{,}0197 \\ 0{,}9803 \end{pmatrix}$. La probabilité est d'environ 2 %.

5 Suites de matrices

Appliquer les capacités attendues

9 Le graphe comporte trois états donc la matrice de transition, notée M, sera carrée de taille 3.
Si l'on veut une matrice de transition stochastique selon les colonnes, m_{ij} est alors la probabilité de passer de l'état j à l'état i.

$$M = \begin{pmatrix} 0{,}3 & 0 & 0 \\ 0 & 0 & 0{,}8 \\ 0{,}7 & 1 & 0{,}2 \end{pmatrix}.$$

12 **1.** u étant stochastique, ses coordonnées sont positives donc les coordonnées du vecteur λu ont le signe de λ. De plus, M étant une matrice stochastique, les coordonnées de Mu sont positives. Donc λ est positif.
2. M est stochastique selon les lignes signifie que la somme des coefficients de chaque ligne est égale à 1. Ainsi, pour tout $i = 1, \ldots, n$, $m_{i1} + m_{i2} + \ldots + m_ip = \sum_{j=1}^{p} m_{ij} = 1$.

3. a. Pour tout entier i entre 1 et n, on a : $v_i = \sum_{j=1}^{p} m_{ij}u_j$.

b. Pour tout j entre 1 et p, on a $u_j \leqslant u_{i_0}$, donc $m_{ij}u_j \leqslant m_{ij}u_{i_0}$.

Ainsi : $v_i \leqslant \sum_{j=1}^{p} m_{ij}u_{i_0} = u_{i_0} \times \sum_{j=1}^{p} m_{ij} = u_{i_0}$.

c. Pour tout i, on a $v_i = \lambda u_i$, donc en particulier $v_{i_0} = \lambda u_{i_0}$, donc $\lambda u_{i_0} \leqslant u_{i_0}$ et on obtient le résultat voulu en divisant chaque membre de l'inégalité par u_{i_0}, qui est positif car u est un vecteur stochastique et non nul car sinon, étant la plus grande valeur, toutes les coordonnées de u seraient nulles, ce qui n'est pas possible pour un vecteur stochastique.

15 **a.** On choisit $u^{(0)} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et on calcule $M^2u^{(0)} \approx \begin{pmatrix} 0{,}55 \\ 0{,}45 \end{pmatrix}$, $M^5u^{(0)} \approx \begin{pmatrix} 0{,}52 \\ 0{,}48 \end{pmatrix}$, $M^{10}u^{(0)} \approx \begin{pmatrix} 0{,}52 \\ 0{,}48 \end{pmatrix}$. Une mesure stationnaire semble donc être $\pi = \begin{pmatrix} 0{,}52 \\ 0{,}48 \end{pmatrix}$.

b. On pose $\pi = \begin{pmatrix} a \\ b \end{pmatrix}$ doit résoudre l'équation
$\pi = M\pi \Leftrightarrow (M - I_2)\pi = 0 \Leftrightarrow \begin{pmatrix} -0{,}6 & 0{,}65 \\ 0{,}6 & -0{,}65 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = 0$.

Cette matrice est non inversible, mais on en extrait une équation que l'on complète par $a + b = 1$ et on obtient alors :

$$\begin{pmatrix} -0{,}6 & 0{,}65 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0{,}52 \\ 0{,}48 \end{pmatrix}.$$

18 On a $M = \begin{pmatrix} 0{,}4 & 0{,}65 \\ 0{,}6 & 0{,}35 \end{pmatrix}$.

1. On peut choisir $u^{(0)} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et on a alors

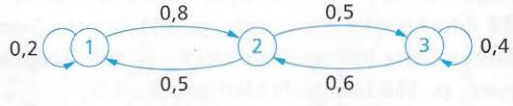
$$M^{10}u^{(0)} \approx M^{20}u^{(0)} \approx M^{30}u^{(0)} \approx \begin{pmatrix} 0{,}55 \\ 0{,}45 \end{pmatrix}.$$

2. a. Au bout de 10, 20 ou 30 unités de temps, la proportion de dextrose est d'environ 55 %.
b. La proportion limite du dextrose semble être de 55 % alors que celle du lévulose semble être de 45 %.

Devoir de synthèse

39 **1. a.** car on ne peut calculer que uM ou Mv et que $uM = \left(\sum_{k=1}^{n} u_k m_{kj}\right)_j = \left(\sum_{k=1}^{n} m_{kj}\right)_j$, or M étant stochastique selon les colonnes, pour tout j entre 1 et n, $\sum_{k=1}^{n} m_{kj} = 1$.
2. d. pour des raisons similaires.
3. a.

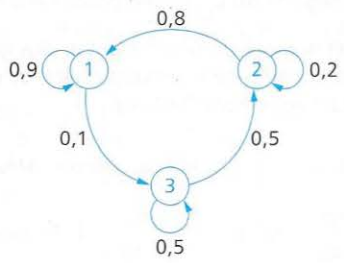
40



41 **1. a.** La matrice est stochastique selon les lignes.
b. $P = \begin{pmatrix} 0{,}6 & 0{,}1 \\ 0{,}4 & 0{,}9 \end{pmatrix}$. **2. a.** $P^{10}u \approx P^{20}u \approx P^{30}u \approx \begin{pmatrix} 0{,}2 \\ 0{,}8 \end{pmatrix}$.
On peut conjecturer qu'une mesure stationnaire de P est ce vecteur $\pi = \begin{pmatrix} 0{,}2 \\ 0{,}8 \end{pmatrix}$.

b. On pose $\pi = \begin{pmatrix} a \\ b \end{pmatrix}$ et on résout l'équation $\pi = P\pi \Leftrightarrow (P - I_2)\pi = 0$. Comme $P - I_2$ n'est pas inversible, on extrait l'équation $-0{,}4a + 0{,}1b = 0$ à laquelle on rajoute $a + b = 1$.
Le système à résoudre est alors $\begin{cases} -0{,}4a + 0{,}1b = 0 \\ a + b = 1 \end{cases}$ et ses solutions sont $a = 0{,}2$ et $b = 0{,}8$.
c. Simple vérification.

42 **1.**



2. a. $M = \begin{pmatrix} 0,9 & 0,8 & 0 \\ 0 & 0,2 & 0,5 \\ 0,1 & 0 & 0,5 \end{pmatrix}$. **b.** On prend $u = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ et on calcule

$$M^{10}u \approx M^{20}u \approx M^{30}u \approx \begin{pmatrix} 0,75 \\ 0,09 \\ 0,15 \end{pmatrix}.$$

3. a. L'équation matricielle est $M\pi = \pi \Leftrightarrow P\pi = 0$, avec

$$P = M - I_3 = \begin{pmatrix} -0,1 & 0,8 & 0 \\ 0 & -0,8 & 0,5 \\ 0,1 & 0 & -0,5 \end{pmatrix}.$$

b. P n'est pas inversible. On peut garder deux des trois équations du système et on doit rajouter l'équation $a + b + c = 1$, où a, b et c sont les coefficients de π.

c. $A = \begin{pmatrix} -0,1 & 0,8 & 0 \\ 0 & -0,8 & 0,5 \\ 1 & 1 & 1 \end{pmatrix}$. **d.** Il y a donc toujours environ 9,4 % de la population toujours malade.

43 **a.** Voir la démonstration de la propriété 2 p. 146.

b. Mu étant stochastique selon les colonnes, la somme des coordonnées du vecteur colonne $(1 - c)Mu$ est égale à $1 - c$. Le vecteur ε étant stochastique, la somme des cordonnées du vecteur $c\varepsilon$ est égale à c. Ainsi, la somme des coordonnées du vecteur v est égale à $1 - c + c = 1$.

44 **1.** $\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 0,3 & 0,85 \\ 0,7 & 0,15 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix}$. On note A la matrice utilisée.

2. On procède par récurrence.

La propriété est vraie au rang 0 car $a_0 + b_0 = 1$.

Supposons la propriété vraie au rang n et démontrons-là au rang $n + 1$. On effectue la somme membre à membre des deux égalités données et on obtient : $a_{n+1} + b_{n+1} = a_n + b_n = 1$.

3. La matrice semble admettre une mesure invariante puisque $A^{10}u \approx A^{20}u \approx A^{30}u \approx \begin{pmatrix} 0,55 \\ 0,45 \end{pmatrix}$, où $u = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}$. On démontre effectivement que la mesure invariante de A est $\pi = \begin{pmatrix} \frac{17}{31} \\ \frac{14}{31} \end{pmatrix}$ en résolvant l'équation matricielle $\begin{pmatrix} -0,7 & 0,85 \\ 1 & 1 \end{pmatrix} \pi = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Ainsi, en notant a et b les limites des suites (a_n) et (b_n), elles satisfont l'équation $\begin{pmatrix} a \\ b \end{pmatrix} = A \begin{pmatrix} a \\ b \end{pmatrix}$, c'est-à-dire que $\begin{pmatrix} a \\ b \end{pmatrix}$ est une mesure invariante de A, donc égale à π.

Crédits photographiques

p. 9 Daniel Deneuchatel ; **p. 12** h Photodisc/Thinkstock ; **p. 12** b Pascal Sittler/RŽa ; **p. 23** Lee/Leemage ; **p. 25** ullstein - Archiv Gerstenberg/akg-images ; **p. 30** Photo.com/Thinkstock ; **p. 39** SSPL/Science Museum/Leemage ; **p. 40** James King-Holmes/SPL/Cosmos ; **p. 43** SPL/Cosmos ; **p. 44** Ruth Black/Fotolia.com ; **p. 47** RIA Novosti/akg-images ; **p. 62** iStockphoto/Thinkstock ; **p. 68** Chris Butler/SPL/Cosmos ; **p. 74** Laurent Cerino/RŽa ; **p. 77** Jean-Francois Colonna/CMAP-Ecole Polytechnique www.lactamme.polytechnique.fr ; **p. 79** MP/Leemage ; **p. 94** Costa/Leemage ; **p. 102** Gareth Cattermole/Getty Images for Netflix/AFP ; **p. 105** Imagestate/Hoa-Qui/Gamma-Rapho ; **p. 128** MP/Leemage ; **p. 130** Costa/Leemage ; **p. 131** Jupiterimages/Photos.com/Getty Images/Thinkstock ; **p. 137** Muller/NY Public Library/SPL/Cosmos ; **p. 138** iStockphoto/Thinkstock ; **p. 141** Angelo Giampiccolo/Alamy/Photo12.com ; **p. 143** Burke/Triolo Productions/Brand X Pictures/Getty Images/Thinkstock ; **p. 151** Coquille de nautile iStockphoto/Thinkstock ; **p. 162** Solkoll ; **p. 167** Rapha'l Pasquier ; **p. 168** Microsoft Mathematics 4.0é

Iconographe : Lisa Buchaudon

Composition et schémas : STDI

IMPRIM'VERT®

Le papier sur lequel est imprimé cet ouvrage provient de forêts certifiées et gérées durablement.

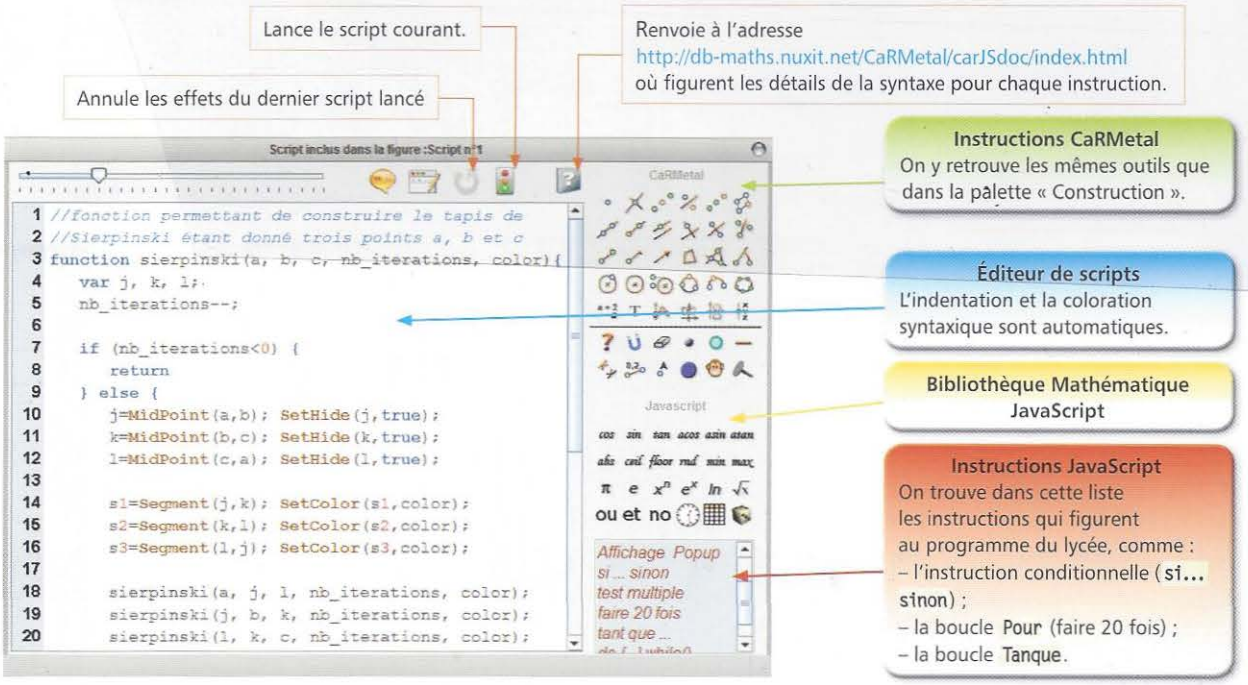
Imprimé en France par I.M.E. – 25110 Baume-les-Dames

N° d'édition : 006198-01 - Dépôt légal : avril 2012

Programmer avec CaRMetal

L'interface

Cette fenêtre est accessible depuis le menu « JavaScript » de la fenêtre principale du logiciel.



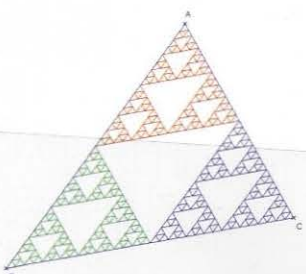
Ajouter une instruction

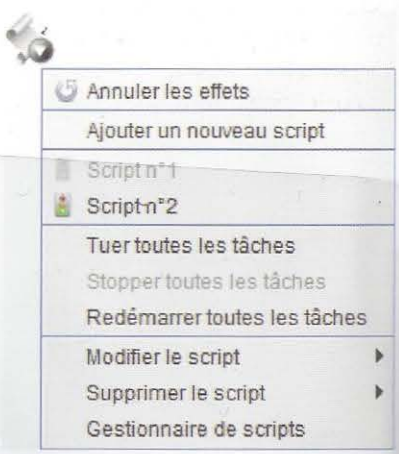
• Aucune syntaxe n'est à retenir : il suffit de cliquer sur une icône pour insérer l'instruction correspondante dans l'éditeur. On peut toutefois cliquer sur le bouton « Aide » pour obtenir quelques exemples. Quant à l'affectation, elle se fait à l'aide du symbole « = ».

• La déclaration des variables (non obligatoire) se fait à l'aide du mot-clef var.

Gérer ses scripts

Une autre icône fait son apparition en haut à gauche de la zone de construction dès qu'un premier script est ajouté à la figure. Un clic permet d'afficher le menu suivant depuis lequel on peut directement lancer/arrêter les exécutions de tous les scripts.

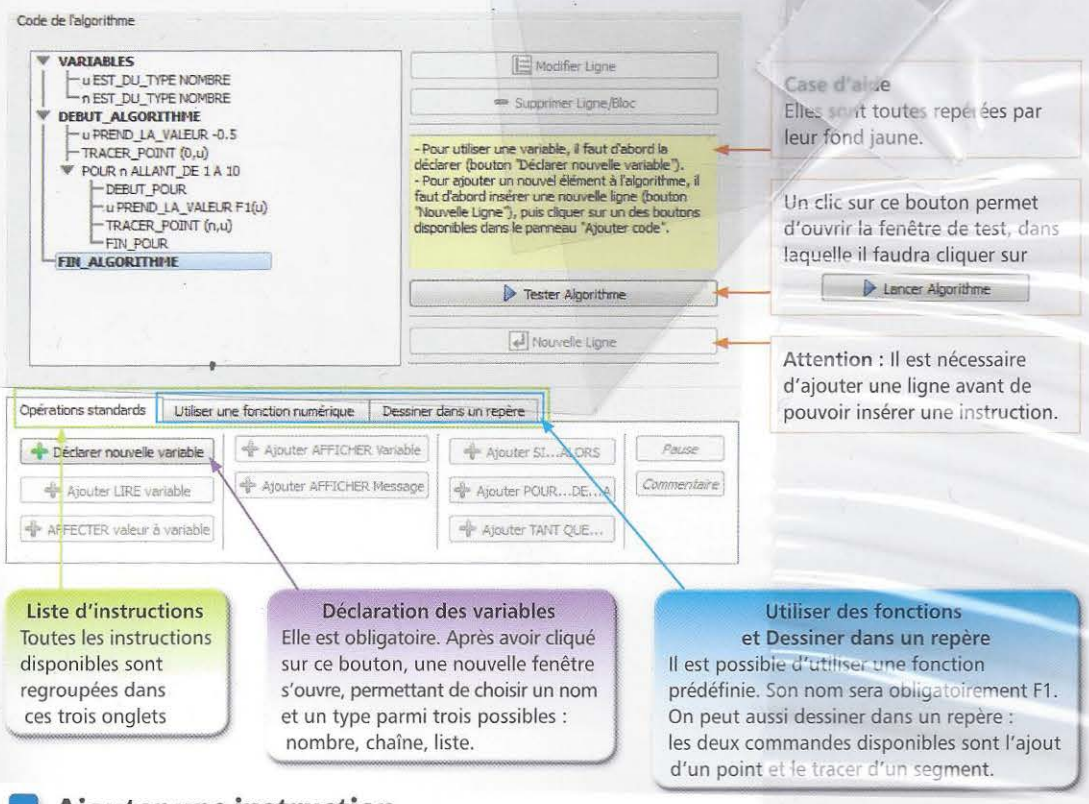




CaRMetal est un logiciel libre, téléchargeable gratuitement à l'adresse suivante : http://db-maths.nuxit.net/CaRMetal/ .

Programmer avec AlgoBox

L'interface

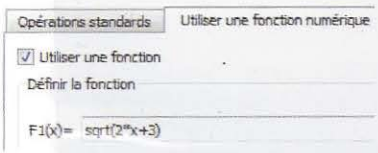


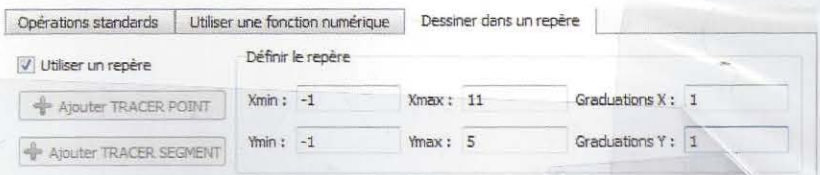
Ajouter une instruction

Aucune syntaxe n'est à retenir : il suffit de cliquer sur un bouton pour insérer l'instruction correspondante dans une ligne vierge. Si besoin, une aide avec des exemples fournis est présente, sur le fond jaune.

Utiliser les fonctions

Dans l'exemple donné, la fonction est utilisée pour définir une suite par une relation de récurrence :
$u_{n+1} = F1(u_n) = \sqrt{2u_n + 3}$ et de premier terme $u_0 = -0{,}5$.
On calcule les 11 premiers termes en utilisant la variable u puis on place les points de coordonnées $(n\ ;\ u)$.
Pour cet exemple, un bon paramétrage du repère est le suivant :



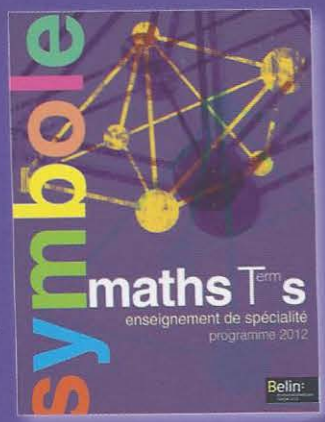


AlgoBox est un logiciel libre, téléchargeable gratuitement à l'adresse suivante : http://www.xm1math.net/algobox/ .

Syntaxe des principales instructions pour différents langages et logiciels de programmation

Instructions	Langage symbolique	Casio	TI	JavaScript/C/C++[1]	AlgoBox
Affectation	`n = 23 ;`	`23→N↵`	`23→N`	`n = 23;`	`n PREND_LA_VALEUR 23`
Demander une saisie	`Saisir(n) ;`	`"N="?→N↵`	`Prompt N`	`n=Input("Saisir n :");`	`LIRE n`
Afficher à l'écran	`Afficher(n) ;` `Afficher(« Bonjour ») ;`	`N↵` `"BONJOUR"↵`	`Disp N` `Disp "BONJOUR"`	`Println(n);` `Print("Bonjour");`	`AFFICHER n` `AFFICHER "Bonjour"`
Test	`Si x < 5 alors` `  Afficher(« x < 5 ») ;` `Sinon` `  Afficher(« x >= 5 ») ;` `FinSi`	`If X<5↵` `Then "X<5"↵` `Else "X>=5"↵`	`If X<5:Then` `Disp "X<5"` `Else` `Disp "X≥5"`	`if(x<5){` `  Println("x < 5");` `} else {` `  Println("x >= 5");` `}`	`SI (x<5) ALORS` `  DEBUT_SI` `  AFFICHER "x<5"` `  FIN_SI` `  SINON` `  DEBUT_SINON` `  AFFICHER "x>=5"` `  FIN_SINON`
Traduction des symboles	Égalité : == Plus petit : < et <= Plus grand : > et >= Non égalité : !=	Égalité : = Plus petit : < et ≤ Plus grand : > et ≥ Non égalité : ≠		Égalité : == Plus petit : < et <= Plus grand : > et >= Non égalité : !=	
Boucle TantQue	`x = 10 ;` `Tantque x< 27 faire` `  x = x + 10 ;` `  Afficher(x) ;` `FinTantque`	`10→X↵` `While X<27↵` `X+10→X↵` `X↵` `WhileEnd↵`	`10→X` `While X<27` `X+10→X` `Disp X` `End`	`x=10;` `while(x<27){` `  x=x+10;` `  Println(x);` `}`	`x PREND_LA_VALEUR 10` `TANT_QUE (x<27) FAIRE` `  DEBUT_TANT_QUE` `  x PREND_LA_VALEUR x+10` `  AFFICHER x` `  FIN_TANT_QUE`
Boucle Pour	`k = 2 ;` `Pour i allant de 0 à 9 faire` `  Afficher(k*i) ;` `FinPour`	`2→K↵` `For 0→I To 9↵` `K×I→P↵` `P↵` `Next`	`2→K` `For(I,0,9,1)` `K*I→P` `Disp P` `End`	`k=2;` `for (i=0; i<10; i=i+1){` `  Println(k*i);` `}`	`k PREND_LA_VALEUR 2` `POUR i ALLANT_DE 0 A 9` `  DEBUT_POUR` `  p PREND_LA_VALEUR k*i` `  AFFICHER p` `  FIN_POUR`

1. Il s'agit ici de captures réalisées dans le module JavaScript de CaRMetal. Les commandes de saisie ou d'affichage sont à adapter selon le langage.



Collection symbole

maths Tes

lesclésdubac

Une collection double pour réussir, qui s'adapte à chaque mode de préparation

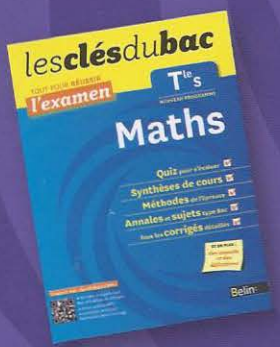


TOUT POUR RÉUSSIR *l'année*

Pour viser le bon dossier ou la mention au Bac en se préparant régulièrement et progressivement toute l'année:

- **Cours** complet et structuré
- **Méthodes** expliquées
- **Exercices** progressifs et minutés
- **Annales** et **sujets** type Bac
- Tous les **corrigés** détaillés

Et des prolongements en ligne gratuits



TOUT POUR RÉUSSIR *l'examen*

L'essentiel pour assurer le jour du Bac:

- **Synthèses** de cours
- **Quiz** pour s'évaluer
- **Méthodes** de l'épreuve
- **Annales** et **sujets** type Bac par thématique ou complets
- Tous les **corrigés** détaillés

Et des prolongements en ligne gratuits

Belin
ÉDITEUR INDÉPENDANT
DEPUIS 1777

www.editions-belin.com
ISBN 978-2-7011-6198-3
9 782701 161983
Code 006198