Terminale

Mathématiques expertes

Programme 2020

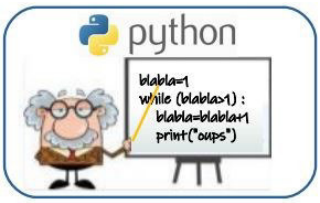
Fiches d'exercices et de cours à compléter

Auteur : Pierre Lux – version 2023

Toutes les corrections sont consultables en ligne

http://pierrelux.net

1 : Les nombres complexes : point de vue algébrique pages 1 à 10
2 : Les nombres complexes - point de vue géométrique pages 11 à 23
3 : Les nombres complexes - trigonométrie pages 24 à 33
4 : Les nombres complexes :équations polynomiales pages 34 à 45
5 : Les nombres complexes – utilisation pages 46 à 54
6 : Divisibilité et congruences pages 55 à 69
7 : PGCD – Nombres premiers entre eux pages 70 à 86
8 : Les nombres premiers pages 87 à 99
9 : Matrices – Opérations élémentaires pages 100 à 116
10 : Graphes pages 117 à 127
11 : Matrices – Quelques utilisations pages 128 à 141



LES NOMBRES COMPLEXES : POINT DE VUE ALGÉBRIQUE

1) DÉFINITION – FORME ALGÉBRIQUE

Définition :

On appelle **corps des nombres complexes**, et on note $\mathbb{C}$ un ensemble contenant $\mathbb{R}$ tel que :
- Il existe dans $\mathbb{C}$ un élément noté i tel que $i^2=-1$.
- Tout élément de $\mathbb{C}$ s'écrit sous la forme $a+bi$, où $a\in\mathbb{R}$ et $b\in\mathbb{R}$.
- $\mathbb{C}$ est muni d'une addition et d'une multiplication qui prolongent l'addition et la multiplication de $\mathbb{R}$, et qui suivent les mêmes règles de calcul.

Un nombre complexe sera souvent représenté par la lettre z.

Nombres complexes particuliers :

Soit un nombre complexe $z=a+bi$ avec $a\in\mathbb{R}$ et $b\in\mathbb{R}$.
- Si $b=0$, on a $z=a$, z est un réel. ($\mathbb{R}$ est contenu dans $\mathbb{C}$)
- Si $a=0$, on a $z=bi$, on dit que z est un imaginaire pur (on dit parfois simplement imaginaire).

Remarques :
- $\mathbb{R}$ correspond à l'ensemble des points sur une droite. Un nombre réel x correspond au point d'abscisse x sur la droite.
  On peut donc toujours comparer deux nombres réels :
  si x et y sont des réels, on a nécessairement $x\leqslant y$ ou $y\leqslant x$ (Le point d'abscisse x se trouve, sur la droite, "avant" ou "après" le point d'abscisse y)
- $\mathbb{C}$, ensemble des nombres $a+bi$ avec $a\in\mathbb{R}$ et $b\in\mathbb{R}$ correspond à l'ensemble des points d'un plan.
  Un nombre complexe $a+bi$ avec $a\in\mathbb{R}$ et $b\in\mathbb{R}$ correspond au point du plan de coordonnées $(a\,;b)$.
  On ne peut donc pas comparer deux nombres complexes : il n'y a pas de relation d'ordre dans $\mathbb{C}$.
  On ne peut donc pas dire qu'un nombre complexe z est inférieur à un nombre complexe z' ou qu'un nombre complexe z est positif.

Propriété :

L'écriture d'un nombre complexe sous la forme $z=a+bi$, où $a\in\mathbb{R}$ et $b\in\mathbb{R}$, est unique.

Preuve :

Considérons un nombre complexe z s'écrivant de deux façons : $z=a+bi$ et $z=a'+b'i$, avec a , b , a' , b' réels.
On a alors $a+bi=a'+b'i$ et on en déduit $a-a'=i(b'-b)$
Supposons que $b\neq b'$, on aurait alors $i=\dfrac{a-a'}{b'-b}$,
Ceci n'est pas possible puisque $i\notin\mathbb{R}$ alors que $\dfrac{a-a'}{b'-b}\in\mathbb{R}$
On ne peut donc pas avoir $b\neq b'$, ce qui signifie que $b=b'$.
Alors $b'-b=0$ et comme on sait que $a-a'=i(b'-b)$, on en déduit $a-a'=0$ c'est-à-dire $a=a'$.
On a donc obtenu $a=a'$ et $b=b'$. Les deux écritures de z sous la forme $a+bi$ et $a'+b'i$ sont donc identiques.

Définition :

Soit un nombre complexe z.
L'écriture $z=a+bi$, où $a\in\mathbb{R}$ et $b\in\mathbb{R}$, est appelée **forme algébrique** du nombre complexe z.
a est appelé **partie réelle** de z, et b **partie imaginaire** de z.
On note $a=\Re e(z)$ et $b=\Im m(z)$.

Remarques :
- La partie réelle de z est un nombre réel.
- La partie imaginaire de z est un nombre réel.

Propriété :

Deux complexes sont égaux si et seulement si ils ont même partie réelle et même partie imaginaire.
C'est-à-dire que si a , b , a' , b' sont des réels, on a

$$a+bi=a'+b'i \quad\Leftrightarrow\quad a=a' \text{ et } b=b'$$

Preuve :

Soit z et z' deux nombres complexes : $z=a+bi$ et $z'=a'+b'i$, avec a , b , a' , b' réels.
On a alors $a=\Re e(z)$, $a'=\Re e(z')$, $b=\Im m(z)$ et $b'=\Im m(z')$
Si $z=z'$, alors $a+bi=a'+b'i$ et comme la forme algébrique d'un nombre complexe est unique, on en déduit que $a=a'$ et $b=b'$.
Donc z et z' ont la même partie réelle et la même partie imaginaire.

Réciproquement :
Si z et z' ont la même partie réelle et la même partie imaginaire, alors $a=a'$ et $b=b'$
et par conséquent $a+bi=a'+b'i$, c'est-à-dire $z=z'$

Exemple : Soit $z=2+3i$ et $z'=i-5$. Calculer et écrire sous forme algébrique :

$z+z'=$ $\qquad$ $z-z'=$

$2z-3z'=$ $\qquad$ $z\cdot z'=$ $\qquad$ $z^2=$

2) DIVISION

Propriété :

Tout nombre complexe non nul z admet un unique inverse noté $\frac{1}{z}$.

Preuve :

On pose $z=x+iy$

Existence : On considère le nombre complexe $z'=\frac{x-iy}{x^2+y^2}$

On a : $zz'=$

Donc z' est bien un inverse de z.

Unicité : On considère z'' un autre inverse de z.

On a : $(z''-z')z=$

Comme $z\neq 0$, on a forcément $z''-z'=0$ et donc $z''=z'$

3) CONJUGUÉ

Définition :

Soit z un nombre complexe de forme algébrique $a+bi$.
On appelle **conjugué** de z le nombre complexe noté $\overline{z}$ tel que $\overline{z}=a-bi$.

Exemple : Soit $z=3+5i$ et $z'=-2+3i$. Calculer :

$\overline{z}=$ $\qquad$ $\overline{z}'=$ $\qquad$ $\overline{z}+\overline{z}'=$ $\qquad$ $z+z'=$

$\overline{z+z'}=$ $\qquad$ $\overline{z}\cdot\overline{z}'=$ $\qquad$ $zz'=$ $\qquad$ $\overline{zz'}=$

Propriétés :

Pour tous nombres complexes z et z', on a :

- $\overline{\overline{z}}=z$
- $z\cdot\overline{z}$ est un réel positif
- $\overline{z+z'}=\overline{z}+\overline{z}'$; $\overline{z-z'}=\overline{z}-\overline{z}'$; $\overline{zz'}=\overline{z}.\overline{z}'$; $\overline{z}^n=\overline{z^n}$ ($n\in\mathbb{N}^*$)
- Si $z'\neq 0$ $\quad \overline{\frac{1}{z'}}=\frac{1}{\overline{z}'}$; $\overline{\frac{z}{z'}}=\frac{\overline{z}}{\overline{z}'}$
- $\Re e(z)=\frac{z+\overline{z}}{2}$; $\Im m(z)=\frac{z-\overline{z}}{2i}$
- $\Im m(z)=0 \Leftrightarrow z\in\mathbb{R}\Leftrightarrow z=\overline{z}$
- $\Re e(z)=0 \Leftrightarrow z\in i\mathbb{R}\Leftrightarrow z=-\overline{z}$ (z est un imaginaire pur)

Preuve :

Soit les nombres complexes écrits sous la forme algébrique : $z=a+bi$ et $z'=a'+b'i$.

- $\overline{z}=a-bi$ donc $\overline{\overline{z}}=a+bi=z$
- $z\cdot\overline{z}=($

- $z+z'=a+bi+a'+b'i=(a+a')+(b+b')i$.

- $z-z'=a+bi-(a'+b'i)=(a-a')+(b-b')i$.

  Comme $(a-a')$ et $(b-b')$ sont des réels, on obtient : $\overline{z-z'}=(a-a')+(b-b')i=a-bi-a'+b'i=\overline{z}-\overline{z}'$

- $zz'=(a+bi)(a'+b'i)=aa'+ab'i+a'bi+bb'i^2=(aa'-bb')+(ab'+a'b)i$

  Comme $(aa'-bb')$ et $(ab'+a'b)$ sont des réels, on obtient : $\overline{zz'}=(aa'-bb')-(ab'+a'b)i$

  D'autre part $\overline{z}\cdot\overline{z}'=(a-bi)(a'-b'i)=aa'-ab'i-a'bi+bb'i^2=(aa'-bb')-(ab'+a'b)i=\overline{zz'}$

- $\overline{z}^n=\overline{z^n}$ se démontre facilement par récurrence en utilisant $\overline{zz'}=\overline{z}.\overline{z}'$ *exigible*

- Si $z'\neq 0$, $\frac{1}{z'}=\frac{1}{a'+b'i}=\frac{a'-b'i}{(a'+b'i)(a'-b'i)}=\frac{a'-b'i}{a'^2+b'^2}=\frac{a'}{a'^2+b'^2}+\frac{-b'}{(a'^2+b'^2)}i$

  Comme $\frac{a'}{a'^2+b'^2}$ et $\frac{-b'}{a'^2+b'^2}$ sont des réels, on obtient : $\overline{\frac{1}{z'}}=\frac{a'}{a'^2+b'^2}+i\frac{b'}{a'^2+b'^2}$

  D'autre part $\overline{z}'=a'-b'i$, donc $\frac{1}{\overline{z'}}=\frac{1}{a'-b'i}=\frac{a'+b'i}{(a'-b'i)(a'+b'i)}=\frac{a'+b'i}{a'^2+b'^2}=\frac{a'}{a'^2+b'^2}+\frac{b'}{a'^2+b'^2}i=\overline{\frac{1}{z'}}$

- *Si* $z'\neq 0$, $\overline{\frac{z}{z'}}=$

- $\frac{z+\overline{z}}{2}=$ $\qquad$ $\frac{z-\overline{z}}{2i}=$

- $z=\overline{z}\ \Leftrightarrow$

- $z=-\overline{z}\ \Leftrightarrow$

Remarque : La propriété $z\cdot\overline{z}\in\mathbb{R}^+$ sera utile pour trouver les formes algébriques d'inverses et de quotients.

Exemples : Méthode de l'expression conjuguée

- L'inverse de $1-i$ est :

- $\frac{1+i}{2-i}=$

4) LA FORMULE DU BINÔME DE NEWTON

Propriété : binome de Newton

Soit a et b deux nombres complexes. Pour tout entier naturel n , on a :

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$

Preuve :

On note $P(n)$: « $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$ », pour $n\in\mathbb{N}$

Initialisation :

Pour $n=0$, on a : $(a+b)^0=1$ et $\sum_{k=0}^{0}\binom{0}{k}a^k b^{0-k}=\binom{0}{0}a^0 b^0=1$

Donc P(0) est vraie.

Hérédité :

Supposons $P(n)$ vraie pour un entier naturel n fixé, c'est à dire $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$ (HR)

Montrons que $P(n+1)$ est vraie, c'est à dire $(a+b)^{n+1}=\sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}$

On a : $(a+b)^{n+1}=(a+b)(a+b)^n=(a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$ (d'après HR)

Ainsi $(a+b)^{n+1}=a\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}+b\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$

$$=\sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k}+\sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k}$$

On rentre a et b dans les sommes (on développe)

On coupe la somme en deux en isolant le dernier terme — On coupe la somme en deux en isolant le premier terme

$$=\sum_{k=0}^{n-1}\binom{n}{k}a^{k+1}b^{n-k}+\binom{n}{n}a^{n+1}b^0+\binom{n}{0}a^0 b^{n+1+0}+\sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k}$$

$$=\sum_{k=0}^{n-1}\binom{n}{k}a^{k+1}b^{n-k}+a^{n+1}+b^{n+1}+\sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k}$$

On pose $s=k+1$

$$=\sum_{s=1}^{n}\binom{n}{s-1}a^s b^{n-(s-1)}+a^{n+1}+b^{n+1}+\sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k}$$

On remplace s par k *(variable muette)*

$$=a^{n+1}+b^{n+1}+\sum_{k=1}^{n}\binom{n}{k-1}a^k b^{n+1-k}+\sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k}$$

$$=a^{n+1}+b^{n+1}+\sum_{k=1}^{n}\left(\binom{n}{k-1}+\binom{n}{k}\right)a^k b^{n+1-k}$$

Egalité utilisée dans le triangle de Pascal

$$=\binom{n+1}{n+1}a^{n+1}b^0+\binom{n+1}{0}a^0 b^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k}$$

$$=\binom{n+1}{0}a^0 b^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n+1-k}+\binom{n+1}{n+1}a^{n+1}b^0$$

Premier terme ($k=0$) — Dernier terme ($k=n+1$)

$$=\sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}$$

Donc $P(n+1)$ est vraie

Conclusion :

On en déduit que pour tout entier naturel n, on a $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$

Exemple :

$(1+i)^3=$

Forme algébrique :

On note souvent :
$z=a+bi$ où $a\in\mathbb{R}$ et $b\in\mathbb{R}$

On appelle **corps des nombres complexes**, et on note $\mathbb{C}$ un ensemble contenant $\mathbb{R}$ tel que :

- Il existe dans $\mathbb{C}$ un élément noté i tel que $i^2=-1$.
- Tout élément de $\mathbb{C}$ s'écrit sous la forme $a+bi$, où $a\in\mathbb{R}$ et $b\in\mathbb{R}$.
- $\mathbb{C}$ est muni d'une addition et d'une multiplication qui prolongent l'addition et la multiplication de $\mathbb{R}$, et qui suivent les mêmes règles de calcul.

L'écriture $z=a+bi$, où $a\in\mathbb{R}$ et $b\in\mathbb{R}$, est appelée **forme algébrique** du nombre complexe z.
a est appelé **partie réelle** de z, et b **partie imaginaire** de z.

On note : $a=\Re e(z)$ et $b=\Im m(z)$.

La partie réelle de z est un nombre réel.
La partie imaginaire de z est un nombre réel.

Nombres complexes particuliers :

- Si $b=0$, on a $z=a$, z est un réel. ($\mathbb{R}$ est contenu dans $\mathbb{C}$)
- Si $a=0$, on a $z=bi$, on dit que z est **un imaginaire pur** (on dit parfois simplement imaginaire).

Attention : On ne peut pas comparer deux nombres complexes : il n'y a pas de relation d'ordre dans $\mathbb{C}$.

Unicité :

L'écriture d'un nombre complexe sous la forme $z=a+bi$, où $a\in\mathbb{R}$ et $b\in\mathbb{R}$, est unique.

$a+bi=a'+b'i \Leftrightarrow a=a'$ et $b=b'$

Propriété :

Deux complexes sont égaux si et seulement si ils ont même partie réelle et même partie imaginaire.

Division :

Tout nombre complexe non nul z admet un unique inverse noté $\frac{1}{z}$.

Conjugué :

Soit z un nombre complexe de forme algébrique $a+bi$.
On appelle **conjugué** de z le nombre complexe noté $\overline{z}$ tel que $\overline{z}=a-bi$.

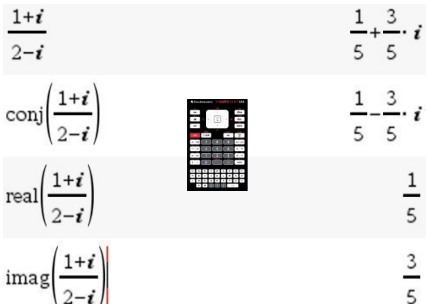
Propriétés :

Pour tous nombres complexes z et z', on a :

- $\overline{\overline{z}}=z$
- $z\cdot\overline{z}$ est un réel positif
- $\overline{z+z'}=\overline{z}+\overline{z'}$; $\overline{z-z'}=\overline{z}-\overline{z'}$; $\overline{zz'}=\overline{z}.\overline{z'}$; $\overline{z^n}=\overline{z}^n$ ($n\in\mathbb{N}^*$)
- Si $z'\neq 0$ $\overline{\left(\frac{1}{z'}\right)}=\frac{1}{\overline{z'}}$; $\overline{\left(\frac{z}{z'}\right)}=\frac{\overline{z}}{\overline{z'}}$
- $\Re e(z)=\frac{z+\overline{z}}{2}$; $\Im m(z)=\frac{z-\overline{z}}{2i}$
- $\Im m(z)=0 \Leftrightarrow z\in\mathbb{R}\Leftrightarrow z=\overline{z}$
- $\Re e(z)=0 \Leftrightarrow z\in i\mathbb{R}\Leftrightarrow z=-\overline{z}$ (z est un imaginaire pur)

Méthode de l'expression conjuguée :

$$\frac{1+i}{2-i}=\frac{(1+i)(2+i)}{(2-i)(2+i)}=\frac{2+i+2i-1}{4-i^2}=\frac{1+3i}{4+1}=\frac{1}{5}+\frac{3}{5}i$$



Avec une Ti-spire

Binôme de Newton

Soit a et b deux nombres complexes. Pour tout entier naturel n, on a :

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}$$

Exemple :

$$(1+i)^3=\sum_{k=0}^{3}\binom{3}{k}1^k i^{3-k}=\binom{3}{0}1^0 i^{3-0}+\binom{3}{1}1^1 i^{3-1}+\binom{3}{2}1^2 i^{3-2}+\binom{3}{3}1^3 i^{3-3}=i^3+3i^2+3i+1=-i-3+3i+1=-2+2i$$

Forme algébrique – conjugué – parties réelle et imaginaire

Ex 1-1 : ***Vrai ou faux***

1) Si $z=4i-3$, alors

a) Im(z)=-3

b) Im(z)=4

c) $\bar{z}=4i+3$

d) $-\bar{z}=4i+3$

e) $i\bar{z}=4-3i$

f) Re($\bar{z}$)=-3

2) Si $z=-3i$, alors z est un imaginaire pur.

3) Si $z=-2$, alors iz est un imaginaire pur.

4) Si $z=a+ib$ (où $a\in\mathbb{R}$, $b\in\mathbb{R}$) , alors

a) Re($z+3$)=Re(z)+3

b) Re(iz)= b

c) Im(z^2)= b^2

d) Im($2z$)= $2b$

Ex 1-2 : ***Parties réelle et imaginaire***

1) Déterminer les parties réelle et imaginaire de :

$3i$; -5 ; 0 ; i^3 ; $3i-2$

2) Soit $x\in\mathbb{R}$ et $z=(4-2x)+i(5-x)$.

a) Pour quelle valeur de x , z est-il réel ?

b) Pour quelle valeur de x , z est-il imaginaire pur ?

Ex 1-3 : ***Calculs dans les complexes***

1) Déterminer la forme algébrique des nombres :

$z_1=3+5-i+2(8-5i)$

$z_2=3(-2+5i)(3i-1)$

2) Déterminer les conjugués des nombres :

$z_3=5-4(i-3)$:

$z_4=3i(2-i)$:

3) Déterminer la forme algébrique des inverses des nombres :

-3 :

i :

$-5i$:

$1-2i$:

4) Écrire sous forme algébrique les nombres :

$\frac{3}{i}$

$\frac{2}{2i-1}$

$\frac{2-i}{2+3i}$

Ex 1-4 : ***Réels et imaginaires purs***

Soit $x\in\mathbb{R}$ et $y\in\mathbb{R}$.
Pour quelles valeurs de x et y les nombres ci-dessous sont réels ou imaginaires purs ?

$z_1=2x-4i+7$ et $z_2=3x-2i+4(x+iy)$

Ex 1-5 : ***Python : les commandes complexes***

Déterminer l'affichage en python correspondant aux instructions saisies.

```
z1=complex(-2,1)
z2=complex(1,2)
```

```
print(z1*z2.real)                    (-2-1j)
print(z1)                            1.0
print(z1.imag)                       (1+2j)
print(z2)                            (-2+1j)
print(z1+z2)                         (-1+3j)
print(z1+z2.real)                    (-1+1j)
print(z1.conjugate())                (-2+1j)
```

Ex 1-6 : ***Mettre sous forme algébrique - calculatrice***

Mettre les nombres complexes ci-dessous sous forme algébrique, puis vérifier avec la calculatrice :

1) $z_1=(4-5i)^2$

2) $z_2=(4-5i)(4+5i)$

3) $z_3=(4+5i)^2$

4) $z_4=2-i(3-4i)(1+i)$

5) $z_5=(1-2i)^3$

6) $z_6=i^4-i^3$

7) $z_7=\overline{(1-2i)^2}$

8) $z_8=\overline{1-i(2-5i)}$

9) $z_9=\dfrac{1}{4i-3}$

10) $z_{10}=\dfrac{1}{(5-i)(2-3i)}$

Ex 1-7 : ***Parties réelle et imaginaire en fonction de*** a ***et*** b

Soit $z=a+ib$ (où $a\in\mathbb{R}$, $b\in\mathbb{R}$).

Déterminer en fonction de a et b les parties réelles et imaginaires de :

1) $Z_1=z^2-2z$

2) $Z_2=\dfrac{z-i}{z+1}$

3) $Z_3=\dfrac{z-2+i}{z+1-i}$

Conjugué

Ex 1-8 : ***En fonction de*** $\bar{z}$

Écrire en fonction de $\bar{z}$ les conjugués des nombres suivants :

1) $Z_1=z-3i$

2) $Z_2=iz-4$

3) $Z_3=(z-2i)(iz+4)$

4) $Z_4=\dfrac{z-2+i}{z-3-i}$

Ex 1-9 : $z+\bar{z}$ ***et*** $z-\bar{z}$

Soit $z=\frac{3-2i}{5-i}$ et $z'=\frac{3+2i}{5+i}$

1) Sans calcul, justifier que $z+z'$ est un réel ?

2) Sans calcul, justifier que $z-z'$ est un imaginaire pur.

Ex 1-10 : $z\bar{z}$

Dans chacun des cas, calculer $z\bar{z}$:

1) $z=1+3i$

2) $z=\frac{1-2i}{2i+1}$

Ex 1-11 : ***Réel ou imaginaire pur : Calculer le conjugué***

Soit z un nombre complexe non nul.

En calculant le conjugué des nombres ci-dessous, déterminer si chacun de ces nombres est un nombre réel, un nombre imaginaire pur ou ni l'un ni l'autre.

$Z_1=z+\bar{z}$

$Z_2=\frac{z-\bar{z}}{z+\bar{z}}$ (où z n'est pas un imaginaire pur)

$Z_3=z^2+\bar{z}^2$

$Z_4=\frac{z^2-\bar{z}^2}{z\bar{z}+1}$

Suites et Fonctions dans les complexes

Ex 1-12 : ***Suites dans les complexes***

On considère la suite (u_n) à valeurs complexe définie par
$\begin{cases} u_0=1 \\ u_{n+1}=(1+i)u_n \end{cases}$

1) Calculer les trois premier termes de cette suite.

2) À quel type de suite réelle ressemble cette suite ?

3) Pourquoi peut-on aussi définir une telle suite dans les complexes.

4) Donner son écriture explicite.

5) Calculer u_7 .

Ex 1-13 : ***Une fonction dans les complexes***

Soit f la fonction définie de $\mathbb{C}$ dans $\mathbb{C}$ par $f(z)=z^2-3iz$.

1) Déterminer sous forme algébrique :

a) $f(i)$

b) $f(1-i)$

c) $f\left(\frac{1}{1+i}\right)$

2) Exprimer $\overline{f(z)}$ en fonction de f ($\bar{z}$)

Ex 1-14 : ***Une fonction dans les complexes - invariant***

Soit f la fonction définie de $\mathbb{C}$ dans $\mathbb{C}$ par $f(z)=z-2\bar{z}+2$.

1) On pose $z=x+iy$ où x et y sont des réels . Donner l'expression algébrique de $f(z)$ en fonction de x et de y .

2) On appelle invariant de f tout nombre complexe qui est égal à son image . Existe-t-il des invariants de f ?

Ex 1-15 : ***Une fonction dans les complexes - invariant***

Soit f la fonction définie pour tout complexe z différent de $2i$ par $f(z)=\frac{2z}{z-2i}$.

1) Calculer l'image de 2, puis celle de $1+i$.

2) Existe-t-il des invariants de f ?

Équations

Ex 1-16 : ***Équations du premier degré et équations de second degré élémentaires***

Résoudre dans $\mathbb{C}$ les équations ci-dessous :

1) $(2+4i)z+3-i=5z-i$

2) $(2-i)z+3-i=3\bar{z}-i$

3) $\frac{i}{z+2i}=4$

4) $z^2=-9$

5) $(z-2i)^2=-4$

6) $\frac{z-1}{iz+1}=-i$

7) $\frac{z-3-i}{z+2-i}=-2i$

Ex 1-17 : ***Système d'équation***

Résoudre dans $\mathbb{C}$ le système d'équations $\begin{cases}3z_1+z_2=2-5i\\ z_1-z_2=2+i\end{cases}$.

Ex 1-18 : ***Utiliser les parties réelles et imaginaires***

Soit $z=x+iy$ (où $x\in\mathbb{R}$, $y\in\mathbb{R}$).

Résoudre dans $\mathbb{C}$ les équations ci-dessous :

1) $z^2-\bar{z}=2$

2) $3z^2+z\bar{z}+6i\sqrt{2}=0$

Binôme de Newton

Ex 1-19 : ***Utiliser le triangle de Pascal***

En utilisant le triangle de Pascal, donner la forme algébrique des expressions ci-dessous :

1) $(1+2i)^3$

2) $(i+2)^4$

3) $(1-i)^5$

Ex 1-20 : ***Trouver un coefficient sans faire le développement***

1) Dans la formule de Newton avec $(x+y)^{12}$, peut-on trouver un terme en x^4y^6 . Si oui, quel est son coefficient ?

2) Même question avec x^4y^8

Ex 1-21 : ***Déterminer une somme***

Montrer que pour tout entier naturel n , $\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$

LES NOMBRES COMPLEXES : POINT DE VUE GÉOMÉTRIQUE

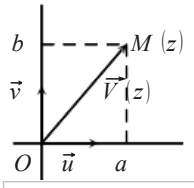
1) REPRÉSENTATION GÉOMÉTRIQUE

Définition :

On se place dans le plan rapporté à un repère orthonormal direct $(O\,;\vec{u}\,,\vec{v})$.

Au point M de coordonnées $(a\,;b)$, on peut associer le nombre complexe $z=a+bi$.
On dit que $z=a+bi$ est **l'affixe** de M ou que $M\,(a\,;b)$ est **l'image ponctuelle** de $z=a+bi$.

Au vecteur $\vec{V}$ de coordonnées $(a\,;b)$, on peut associer le nombre complexe $z=a+bi$.
On dit que $z=a+bi$ est **l'affixe** de $\vec{V}$ ou que $\vec{V}\,(a\,;b)$ est **l'image vectorielle** de $z=a+bi$.

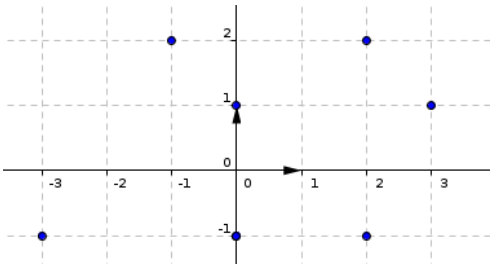


Lorsqu'on repère un point ou un vecteur par son affixe dans un repère orthonormal direct, on dit qu'on se place dans le plan complexe.

Exemple : Placer dans le plan complexe, les points d'affixes :

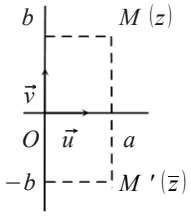
$z_1=2+2i$; $z_2=3+i$; $z_3=-1+2i$; $z_4=2-i$

$z_5=i$; $z_6=-i$; $z_7=1$; $z_8=-i-3$



Remarque :

Si M est le point d'affixe z , le point M' d'affixe $\bar{z}$ est



Propriétés :

Si M a pour affixe $z=a+bi$ et si M' a pour affixe $z'=a'+b'i$, avec a, b, a', b' réels, alors :

- le vecteur $\overrightarrow{MM'}$ a pour affixe $z'-z=(a'-a)+(b'-b)i$
- $OM=\|\overrightarrow{OM}\|=\sqrt{a^2+b^2}$
- $MM'=\|\overrightarrow{MM'}\|=\sqrt{(a'-a)^2+(b'-b)^2}$
- le milieu I de $[MM']$ a pour affixe $z_I=\dfrac{z+z'}{2}$

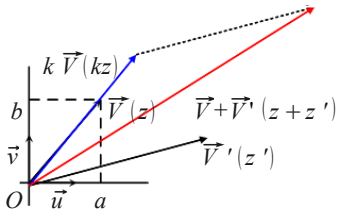
Preuve :

M a pour coordonnées $(a\,;b)$ et M' a pour coordonnées $(a'\,;b')$. Les résultats vus en 1ère sur les coordonnées permettent d'écrire :

- $\overrightarrow{MM'}$ a pour coordonnées $\begin{pmatrix}a'-a\\b'-b\end{pmatrix}$, donc $\overrightarrow{MM'}$ a pour affixe $(a'-a)+(b'-b)i=a'-a+b'i-bi=a'+b'i-(a+bi)=z'-z$
- le milieu I de $[MM']$ a pour coordonnées $\left(\dfrac{a+a'}{2}\,;\dfrac{b+b'}{2}\right)$, donc son affixe est :

Propriétés :

- Si $\vec{V}$ a pour affixe z et $\vec{V}'$ pour affixe z', alors $\vec{V}+\vec{V}'$ a pour affixe $z+z'$.
- Si k est un réel, alors $k\,\vec{V}$ a pour affixe kz.



Preuve :

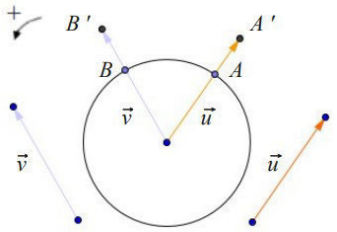
- Soit $a+bi$ et $a'+b'i$ les formes algébriques de z et z'.
  Le vecteur $\vec{V}$ a pour coordonnées $\begin{pmatrix}a\\b\end{pmatrix}$ et le vecteur $\vec{V}'$ a pour coordonnées $\begin{pmatrix}a'\\b'\end{pmatrix}$.

  On sait alors que le vecteur $\vec{V}+\vec{V}'$ a pour coordonnées $\begin{pmatrix}a+a'\\b+b'\end{pmatrix}$.
  Il a donc pour affixe :
  $a+a'+(b+b')i=a+a'+bi+b'i=a+bi+a'+b'i=z+z'$.

- Si k est un réel, alors on sait que $k\,\vec{V}$ a pour coordonnées $\begin{pmatrix}ka\\kb\end{pmatrix}$, donc $k\,\vec{V}$ a pour affixe :
  $ka+kbi=k\,(a+bi)=kz$.

2) MESURES DE L'ANGLE ORIENTÉ D'UN COUPLE DE VECTEURS NON NULS

Soit $\vec{u}$ et $\vec{v}$ deux vecteurs non nuls du plan orienté, O un point quelconque et C le cercle trigonométrique de centre O.
On considère A' et B' les points définis par $\overrightarrow{OA'}=\vec{u}$ et $\overrightarrow{OB'}=\vec{v}$.
Les demi-droites $[OA')$ et $[OB')$ coupent le cercle trigonométrique C respectivement en A et en B.
Les vecteurs $\overrightarrow{OA}=\frac{1}{\|\vec{u}\|}\vec{u}$ et $\overrightarrow{OB}=\frac{1}{\|\vec{v}\|}\vec{v}$ sont unitaires, respectivement colinéaires à $\vec{u}$ et $\vec{v}$ et de même sens qu'eux.



Définitions :

On appelle **mesures de l'angle orienté** $(\overrightarrow{OA}, \overrightarrow{OB})$ tous les réels de la forme :

- $l+2k\pi$ où l est la longueur de l'arc parcouru de A vers B dans le sens direct et où $k \in \mathbb{N}$
- $-l'-2k\pi$ où l' est la longueur de l'arc parcouru de A vers B dans le sens indirect et où $k' \in \mathbb{N}$.

Remarque : On peut exprimer toutes les mesures sous la forme $l+2k\pi$ où $k \in \mathbb{Z}$.

Les mesures en radian de l'angle orienté de vecteurs $(\vec{u}, \vec{v})$ sont celles de l'angle orienté de vecteurs unitaires $(\overrightarrow{OA}, \overrightarrow{OB})$ c'est à dire, celles de l'angle orienté de vecteurs unitaires $\left(\frac{1}{\|\vec{u}\|}\vec{u}, \frac{1}{\|\vec{v}\|}\vec{v}\right)$.

Il en résulte que si x est une mesure de $(\vec{u}, \vec{v})$, alors les autres mesures sont de la forme $x+2k\pi$, $k \in \mathbb{Z}$.
On dit que les angles orientés sont définis **modulo 2π**.

Notations :

- La notation usuelle est $(\widehat{\vec{u};\vec{v}})$, mais s'il n'y a aucun risque de confusion, on notera seulement $(\vec{u}, \vec{v})$ cet angle orienté.
- Par abus de langage, on confond un angle et ses mesures.
  On écrit, par exemple, $(\vec{u}, \vec{v})=\frac{\pi}{2}$ signifiant qu'**une** mesure de $(\vec{u}, \vec{v})$ est $\frac{\pi}{2}$; les autres mesures sont alors de la forme $\frac{\pi}{2}+2k\pi$, $k \in \mathbb{Z}$.
  On écrit aussi $(\vec{u}, \vec{v})=\frac{\pi}{2}+2k\pi$, $\boldsymbol{k \in \mathbb{Z}}$ ou encore $(\vec{u}, \vec{v})=\frac{\pi}{2}[2\pi]$

Définition :

Une seule des mesures de l'angle orienté de vecteurs $(\vec{u}, \vec{v})$ appartient à l'intervalle $]-\pi ; \pi]$.
On l'appelle **mesure principale** de l'angle orienté de vecteurs $(\vec{u}, \vec{v})$.

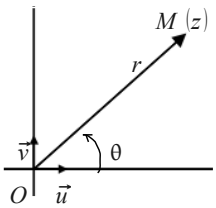
Remarque :
La valeur absolue de la mesure principale de l'angle orienté de vecteurs $(\vec{u}, \vec{v})$ est la mesure de l'angle géométrique formé par ces deux vecteurs.

3) FORME TRIGONOMÉTRIQUE

Coordonnées polaires :

Le plan est muni d'un repère orthonormal direct $(O ; \vec{u}, \vec{v})$.
Soit $M(a ; b)$ un point du plan (distinct de O).
On appelle **coordonnées polaires** de M, tout couple de nombres réels (r, θ) tel que :

$r=OM$ et $(\vec{u}, \overrightarrow{OM})=\theta+2k\pi$, $k \in \mathbb{Z}$



Remarque :
Soit M le point d'affixe x avec $x \in \mathbb{R}$, on a $r=OM=|x|$

Définition :

Tout nombre complexe non nul z peut-être écrit sous la forme :

$z=r(\cos\theta+i\sin\theta)$, avec $\theta \in \mathbb{R}$ et $r \in \mathbb{R}_+^*$.

On dit que $z=r(\cos\theta+i\sin\theta)$ avec $\theta \in \mathbb{R}$ et $r \in \mathbb{R}_+^*$ est une **forme trigonométrique** de z.

Propriété :

Si deux nombres complexes z et z' sont écrits sous forme trigonométrique $z = r(\cos\theta + i\sin\theta)$ et $z' = r'(\cos\theta' + i\sin\theta')$, on a :

$$z = z' \Leftrightarrow r(\cos\theta + i\sin\theta) = r'(\cos\theta' + i\sin\theta') \Leftrightarrow \begin{cases} r = r' \\ \theta = \theta'[2\pi] \end{cases}$$

Preuve : Considérons les points M et M' d'affixes respectives z et z'. On peut écrire :

$$z = z' \Leftrightarrow M = M' \Leftrightarrow$$

4) MODULE

Définition :

Soit le nombre complexe z de forme algébrique $a + bi$ et soit M le point d'affixe z.

On appelle **module** de z le nombre réel positif $r = OM = \sqrt{a^2 + b^2}$. On note $r = |z|$.

Remarque :

La notation $||z||$ ne risque pas de prêter à confusion avec la notation de la valeur absolue puisque lorsque x est un nombre réel, on a $r = OM = |x|$.
Pour un réel x , $|x|$ pourra être lu indifféremment "valeur absolue de x" ou "module de x".
Pour un nombre complexe non réel z , $|z|$ sera lu impérativement "module de z".

Exemple : - Calculer le module de $z_1 = 3 + 4i$:

- $z_2 = \sqrt{3} + i$:

Propriétés :

- Soit $\vec{V}$ un vecteur d'affixe z , on a $||\vec{V}|| = |z|$
- Soit A et B deux points d'affixes respectives z_A et z_B , on a $AB = |z_B - z_A|$

Preuve :
Si $\vec{V}$ est un vecteur d'affixe z, on a $\vec{V} = \overrightarrow{OM}$ avec M d'affixe z . Alors $||\vec{V}|| = ||\overrightarrow{OM}|| = OM = |z|$.
Si A et B sont les points d'affixes respectives z_A et z_B , le vecteur $\overrightarrow{AB}$ a pour affixe $z_B - z_A =$ ...

Propriétés :

- $|z| = 0 \Leftrightarrow z = 0$
- $|-z| = |z|$
- $|\bar{z}| = |z|$
- $|z + z'| \leqslant |z| + |z'|$
- $|z \cdot z'| = |z| \cdot |z'|$ et $|z^n| = |z|^n$ ($n \in \mathbb{N}$)
- si $z \neq 0$ $\left|\frac{1}{z}\right| = \frac{1}{|z|}$
- si $z' \neq 0$ $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$
- $z\bar{z} = |z|^2$ (on retrouve $z\bar{z} \in \mathbb{R}^+$)
- si $z \neq 0$ $\frac{1}{z} = \frac{\bar{z}}{|z|^2}$

Preuve :

- Soit M le point d'affixe z dans le plan rapporté au repère $(O ; \vec{u}, \vec{v})$. On peut écrire :
- Le point M' d'affixe $-z$ est symétrique du point M par rapport à l'origine O.

  La symétrie conservant les distances on a :

- Le point M'' d'affixe est symétrique du point M par rapport à l'axe $(O ; \vec{u})$.
  La symétrie conservant les distances on a : $OM'' = OM$ donc $|\bar{z}| = |z|$

- Soit $\vec{v}$ le vecteur d'affixe z et $\vec{v'}$ le vecteur d'affixe z'.
  On sait que le vecteur $\vec{v} + \vec{v'}$ a pour affixe $z + z'$.
  En utilisant l'inégalité triangulaire, on a $||\vec{v} + \vec{v'}|| \leqslant ||\vec{v}|| + ||\vec{v'}||$ donc $|z + z'| \leqslant |z| + |z'|$

- Si z a pour forme algébrique $z = a + bi$ et si z' a pour forme algébrique $z' = a' + b'i$, alors : *exigible*
  $zz' = (a + bi)(a' + b'i) = aa' + ab'i + a'bi + bb'i^2 = (aa' - bb') + (ab' + a'b)i$
  Comme $(aa' - bb')$ et $(ab' + a'b)$ sont des réels, on en déduit que :
  $|zz'| = \sqrt{(aa' - bb')^2 + (ab' + a'b)^2} = \sqrt{aa'^2 + bb'^2 + ab'^2 + a'b^2} = \sqrt{a^2(a'^2 + b'^2) + b^2(a'^2 + b'^2)} = \sqrt{(a^2 + b^2)(a'^2 + b'^2)} = \sqrt{a^2 + b^2}\sqrt{a'^2 + b'^2} = |z| \cdot |z'|$

- $|z^n| = |z|^n$ se montre facilement par récurrence en utilisant $|z \cdot z'| = |z| \cdot |z'|$ *exigible*

- si $z' \neq 0$ on a, d'après la propriété précédente :

$$|z| \times \left|\frac{1}{z}\right| = \left|z \times \frac{1}{z}\right| = |1| = 1 \text{ , donc } \left|\frac{1}{z}\right| = \frac{1}{|z|} \quad \text{et} \quad \left|\frac{z}{z'}\right| = \left|z \times \frac{1}{z'}\right| = |z| \times \left|\frac{1}{z'}\right| = |z| \frac{1}{|z'|} = \frac{|z|}{|z'|}$$

- $z \cdot \bar{z} =$

- si $z \neq 0$, $\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2}$

5) L'ENSEMBLE DES COMPLEXES DE MODULE 1

Définition et notation :

L'ensemble des nombres complexes de module 1 est noté $\mathbb{U}$

Remarques :

- $\mathbb{U} =$

- Dans le plan complexe, l'ensemble des points images des éléments de $\mathbb{U}$ est

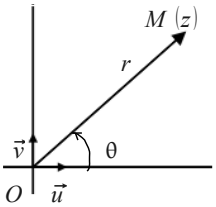
Propriétés de stabilité :

Soit z et z' deux nombres complexes appartenant à l'ensemble $\mathbb{U}$. On a :

- $zz' \in \mathbb{U}$ - $\frac{1}{z} \in \mathbb{U}$ ($z \neq 0$) - $\frac{z'}{z} \in \mathbb{U}$ ($z \neq 0$)

Preuve : Immédiat en utilisant les propriétés des modules

6) ARGUMENT



Définition :

Soit le nombre complexe non nul z de forme algébrique $a + bi$ et soit M le point d'affixe z.

On appelle **argument** de z tout nombre réel θ tel que $\theta = (\vec{u}, \overrightarrow{OM})[2\pi]$. On note $\theta = \arg(z)$

Remarque : θ n'est pas unique, il est défini à $2k\pi$ près $(k \in \mathbb{Z})$ c'est-à-dire modulo $[2\pi]$.

Propriétés :

Soit z et z' deux nombres complexes non nuls d'arguments respectifs θ et θ' . On a :

- $(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = \cos(\theta + \theta') + i\sin(\theta + \theta')$ $\quad \arg(zz') = \arg z + \arg z' \quad [2\pi]$
- $\frac{1}{\cos(\theta) + i\sin(\theta)} = \cos(\theta) + i\sin(-\theta)$ $\quad \arg\left(\frac{1}{z}\right) = -\arg z \quad [2\pi]$
- $\frac{\cos\theta + i\sin\theta}{\cos\theta' + i\sin\theta'} = \cos(\theta - \theta') + i\sin(\theta - \theta')$ $\quad \arg\left(\frac{z}{z'}\right) = \arg z - \arg z' \quad [2\pi]$
- $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$ pour tout $n \in \mathbb{Z}$ $\quad \arg(z^n) = n\arg z \quad [2\pi]$
- $\cos\theta - i\sin\theta = \cos(-\theta) + i\sin(-\theta)$ $\quad \arg(\bar{z}) = -\arg z \quad [2\pi]$
- $-(\cos\theta + i\sin\theta) = \cos(\theta + \pi) + i\sin(\theta + \pi)$ $\quad \arg(-z) = \arg z + \pi \quad [2\pi]$

Preuve :

- On a : $z = r(\cos\theta + i\sin\theta)$ avec $r \in \mathbb{R}^+$ et $z' = r'(\cos\theta' + i\sin\theta')$ avec $r' \in \mathbb{R}^+$.
  On montre facilement que : $(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = \cos(\theta + \theta') + i\sin(\theta + \theta')$.
  On peut en déduire : $zz' = rr'(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = rr'[\cos(\theta + \theta') + i\sin(\theta + \theta')]$.
  Comme rr' est un nombre réel positif, on a donc $\arg(zz') = \arg z + \arg z' \ [2\pi]$

- On montre facilement, en utilisant l'expression conjuguée, que : $\dfrac{1}{\cos(\theta)+i\sin(\theta)}=\cos(-\theta)+i\sin(-\theta)$

  On peut en déduire que : $\dfrac{1}{z}=\dfrac{1}{r}\times\dfrac{1}{\cos\theta+i\sin\theta}=\dfrac{1}{r}\times(\cos(-\theta)+i\sin(-\theta))$

  Comme $\dfrac{1}{r}$ est un nombre réel positif, on a donc $\arg\left(\dfrac{1}{z}\right)=-\theta=-\arg z \quad [2\pi]$.

- On a :

  $\dfrac{\cos\theta+i\sin\theta}{\cos\theta'+i\sin\theta'}=(\cos\theta+i\sin\theta)\dfrac{1}{\cos\theta'+i\sin\theta'}=(\cos\theta+i\sin\theta)\times(\cos(-\theta')+i\sin(-\theta'))=\cos(\theta-\theta')+i\sin(\theta-\theta')$

  Alors $\dfrac{z}{z'}=\dfrac{r}{r'}\times\dfrac{\cos\theta+i\sin\theta}{\cos\theta'+i\sin\theta'}=\dfrac{r}{r'}\times(\cos(\theta-\theta')+i\sin(\theta-\theta'))$

  Comme $\dfrac{r}{r'}$ est un nombre réel positif, on a donc $\arg\left(\dfrac{z}{z'}\right)=\theta-\theta'=\arg z-\arg z'$

- Soit $P(n)$ la proposition : $(\cos\theta+i\sin\theta)^n=\cos(n\theta)+i\sin(n\theta)$.

  Pour $n=0$, on a :

  $(\cos\theta+i\sin\theta)^0=1$ et $\cos(0\times\theta)+i\sin(0\times\theta)=\cos(0)+i\sin(0)=1+0i=1$, donc $P(0)$ est vraie.

  Supposons $P(n)$ vérifiée pour un entier naturel n, c'est-à-dire $(\cos\theta+i\sin\theta)^n=\cos(n\theta)+i\sin(n\theta)$.

  Alors en multipliant les deux membres par $\cos\theta+i\sin\theta$, on obtient :

  $(\cos\theta+i\sin\theta)^{n+1}=[\cos(n\theta)+i\sin(n\theta)](\cos\theta+i\sin\theta)=\cos(n\theta+\theta)+i\sin(n\theta+\theta)=\cos((n+1)\theta)+i\sin((n+1)\theta)$

  $P(n+1)$ est alors justifiée.

  On a donc démontré par récurrence que pour tout $n\in\mathbb{N}$, $(\cos\theta+i\sin\theta)^n=\cos(n\theta)+i\sin(n\theta)$.

  Lorsque l'on considère un entier négatif, que l'on peut noter $-n$ avec $n\in\mathbb{N}$, on peut écrire, en utilisant les propriétés déjà démontrées :

  $(\cos\theta+i\sin\theta)^{-n}=\dfrac{1}{(\cos\theta+i\sin\theta)^n}=\dfrac{1}{\cos(n\theta)+i\sin(n\theta)}=\cos(-n\theta)+i\sin(-n\theta)$

  La proposition est donc vérifiée pour tout $n\in\mathbb{Z}$. $z^n=[r(\cos\theta+i\sin\theta)]^n=r^n(\cos\theta+i\sin\theta)^n=r^n[\cos(n\theta)+i\sin(n\theta)]$

  On peut écrire $z^n=[r(\cos\theta+i\sin\theta)]^n=r^n(\cos\theta+i\sin\theta)^n=r^n[\cos(n\theta)+i\sin(n\theta)]$

  Comme r^n est un réel positif, on a donc pour tout $n\in\mathbb{Z}$: $\arg(z^n)=n\arg z \quad [2\pi]$

- Sachant que $\cos(-\theta)=\cos\theta$ et $\sin(-\theta)=-\sin\theta$, on peut écrire : $\cos\theta-i\sin\theta=\cos(-\theta)+i\sin(-\theta)$

  Alors $\bar{z}=r(\cos\theta-i\sin\theta)=r[\cos(-\theta)+i\sin(-\theta)]$.

  Comme r est un réel positif, on en déduit $\arg(\bar{z})=-\theta=-\arg z \quad [2\pi]$

- Sachant que $\cos(\theta+\pi)=-\cos\theta$ et $\sin(\theta+\pi)=-\sin\theta$, on peut écrire : $-(\cos\theta+i\sin\theta)=-\cos\theta-i\sin\theta=\cos(\theta+\pi)+i\sin(\theta+\pi)$

  Alors $-z=-r(\cos\theta+i\sin\theta)=r[\cos(\theta+\pi)+i\sin(\theta+\pi)]$.

  Comme r est un réel positif, on en déduit $\arg(-z)=\theta+\pi=\arg z+\pi \quad [2\pi]$

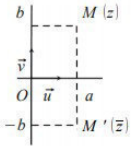
Propriétés :

Soit $z=r(\cos\theta+i\sin\theta)$ un nombre complexe écrit sous forme trigonométrique. $\bar{z}$ et $-z$ ont pour formes trigonométriques :

$$\bar{z}=r(\cos(-\theta)+i\sin(-\theta)) \qquad \text{et} \qquad -z=r(\cos(\theta+\pi)+i\sin(\theta+\pi))$$

Représentation géométrique :

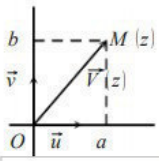
Si M est le point d'affixe z , le point M ' d'affixe $\bar{z}$ est le symétrique de M par rapport à l'axe des abscisses.



On se place dans le plan rapporté à un repère orthonormal direct $(O\,;\vec{u},\vec{v})$.

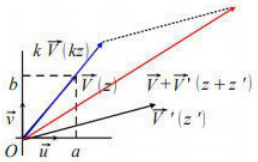
Au point M de coordonnées $(a\,;b)$, on peut associer le nombre complexe $z=a+bi$.
$z=a+bi$ est **l'affixe** de M et $M\,(a\,;b)$ est **l'image ponctuelle** de $z=a+bi$.

Au vecteur $\vec{V}$ de coordonnées $(a\,;b)$, on peut associer le nombre complexe $z=a+bi$.
$z=a+bi$ est **l'affixe** de $\vec{V}$ et $\vec{V}\,(a\,;b)$ est **l'image vectorielle** de $z=a+bi$.



Lorsqu'on repère un point ou un vecteur par son affixe dans un repère orthonormal direct, on dit qu'on se place dans le plan complexe.

Propriétés :

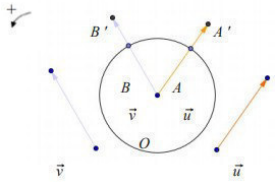


Si M a pour affixe $z=a+b\,i$ et si M' a pour affixe $z'=a'+b'\,i$, avec a,b,a',b' réels, alors :

- le vecteur $\overrightarrow{MM'}$ a pour affixe $z'-z=(a'-a)+(b'-b)\,i$
- $OM=\|\overrightarrow{OM}\|=\sqrt{a^2+b^2}$
- $MM'=\|\overrightarrow{MM'}\|=\sqrt{(a'-a)^2+(b'-b)^2}$
- le milieu I de $[MM']$ a pour affixe $z_I=\dfrac{z+z'}{2}$
- Si $\vec{V}$ a pour affixe z et $\vec{V}'$ pour affixe z', alors $\vec{V}+\vec{V}'$ a pour affixe $z+z'$.
- Si k est un réel, alors $k\,\vec{V}$ a pour affixe kz.

Angle orienté :

Soit $\vec{u}$ et $\vec{v}$ deux vecteurs non nuls du plan orienté, O un point quelconque et C le cercle trigonométrique de centre O.



On appelle **mesures de l'angle orienté** $(\overrightarrow{OA},\overrightarrow{OB})$ tous les réels de la forme :

- $l+2k\pi$ où l est la longueur de l'arc parcouru de A vers B dans le sens direct et où $k\in\mathbb{N}$
- $-l'+2k\pi$ où l' est la longueur de l'arc parcouru de A vers B dans le sens indirect et où $k'\in\mathbb{N}$.

Remarque : On peut exprimer toutes les mesures sous la forme $l+2k\pi$ où $k\in\mathbb{Z}$.

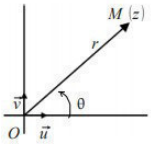
Les mesures en radian de l'angle orienté de vecteurs $(\vec{u},\vec{v})$ sont celles de l'angle orienté de vecteurs unitaires $(\overrightarrow{OA},\overrightarrow{OB})$.

Il en résulte que si x est une mesure de $(\vec{u},\vec{v})$, alors les autres mesures sont de la forme $x+2k\pi$, $k\in\mathbb{Z}$.
On dit que les angles orientés sont définis modulo 2π.

Une seule des mesures de l'angle orienté de vecteurs $(\vec{u},\vec{v})$ appartient à l'intervalle $]-\pi;\pi]$.
On l'appelle **mesure principale** de l'angle orienté de vecteurs $(\vec{u},\vec{v})$.

(r,θ) est un couple de **coordonnées polaires**

Forme trigonométrique :



$r=\sqrt{a^2+b^2}$
$a=r\cos\theta$
$b=r\sin\theta$

Tout nombre complexe non nul $z=a+ib$ peut-être écrit sous la forme :

$$z=r(\cos\theta+i\sin\theta)\,,\quad \text{avec } \theta\in\mathbb{R} \text{ et } r\in\mathbb{R}_+^*$$

On dit que $z=r(\cos\theta+i\sin\theta)$ avec $\theta\in\mathbb{R}$ et $r\in\mathbb{R}_+^*$ est une **forme trigonométrique** de z.

Propriété :

Si deux nombres complexes z et z' sont écrits sous forme trigonométrique $z=r(\cos\theta+i\sin\theta)$ et $z'=r'(\cos\theta'+i\sin\theta')$, on a :

$$z=z' \;\Leftrightarrow\; r(\cos\theta+i\sin\theta)=r'(\cos\theta'+i\sin\theta') \;\Leftrightarrow\; \begin{cases} r=r' \\ \theta=\theta'\,[2\pi] \end{cases}$$

Module :

On appelle **module** de z le nombre réel positif $r=OM=\sqrt{a^2+b^2}$. On note $r=|z|$.

Propriétés :

- Soit $\vec{V}$ un vecteur d'affixe z, on a $\|\vec{V}\|=|z|$
- Soit A et B deux points d'affixes respectives z_A et z_B, on a $AB=|z_B-z_A|$
- $|z|=0\Leftrightarrow z=0$
- $|-z|=|z|$
- $|\bar{z}|=|z|$
- $|z+z'|\leqslant|z|+|z'|$
- $|z\cdot z'|=|z|\cdot|z'|$ et $|z^n|=|z|^n$ ($n\in\mathbb{N}$)
- si $z\neq0$ $\left|\dfrac{1}{z}\right|=\dfrac{1}{|z|}$
- si $z'\neq0$ $\left|\dfrac{z}{z'}\right|=\dfrac{|z|}{|z'|}$
- $z\,\bar{z}=|z|^2$ (on retrouve $z\,\bar{z}\in\mathbb{R}^+$)
- si $z\neq0$ $\dfrac{1}{z}=\dfrac{\bar{z}}{|z|^2}$

L'ensemble des nombres complexes de module 1 :

$$\mathbb{U}=\{z\in\mathbb{C}\,/\,|z|=1\}$$

L'ensemble des nombres complexes de module 1 est noté $\mathbb{U}$

Dans le plan complexe, cet ensemble est le cercle trigonométrique.

Propriétés :

Soit z et z' deux nombres complexes appartenant à l'ensemble $\mathbb{U}$. On a :

- $zz'\in\mathbb{U}$
- $\dfrac{1}{z}\in\mathbb{U}$ ($z\neq0$)
- $\dfrac{z'}{z}\in\mathbb{U}$ ($z\neq0$)

Argument :

θ n'est pas unique, il est défini à $2k\pi$ près $(k\in\mathbb{Z})$ c'est-à-dire modulo $[2\pi]$.

On appelle **argument** de z (avec z **non nul**) tout nombre réel θ tel que $\theta=(\vec{u},\overrightarrow{OM})\,[2\pi]$. On note $\theta=\arg(z)$

Propriétés :

Soit z et z' deux nombres complexes non nuls d'arguments respectifs θ et θ'. On a :

- $(\cos\theta+i\sin\theta)(\cos\theta'+i\sin\theta')=\cos(\theta+\theta')+i\sin(\theta+\theta')$ — $\arg(zz')=\arg z+\arg z'\;[2\pi]$
- $\dfrac{1}{\cos(\theta)+i\sin(\theta)}=\cos(\theta)+i\sin(-\theta)$ — $\arg\left(\dfrac{1}{z}\right)=-\arg z\;[2\pi]$
- $\dfrac{\cos\theta+i\sin\theta}{\cos\theta'+i\sin\theta'}=\cos(\theta-\theta')+i\sin(\theta-\theta')$ — $\arg\left(\dfrac{z}{z'}\right)=\arg z-\arg z'\;[2\pi]$
- $(\cos\theta+i\sin\theta)^n=\cos(n\theta)+i\sin(n\theta)$ pour tout $n\in\mathbb{Z}$ — $\arg(z^n)=n\arg z\;[2\pi]$
- $\cos\theta-i\sin\theta=\cos(-\theta)+i\sin(-\theta)$ — $\arg(\bar{z})=-\arg z\;[2\pi]$
- $-(\cos\theta+i\sin\theta)=\cos(\theta+\pi)+i\sin(\theta+\pi)$ — $\arg(-z)=\arg z+\pi\;[2\pi]$
- $\bar{z}=r(\cos(-\theta)+i\sin(-\theta))$ et $-z=r(\cos(\theta+\pi)+i\sin(\theta+\pi))$

Affixes de points et de vecteurs

On se place dans un repère orthonormé $(O;\vec{u},\vec{v})$.

Ex 2-1 : ***Calculs d'affixes***

1) Déterminer les affixes des points suivants :
$A(2;0)$, $B(0;-5)$ et $C(-2;3)$

2) Déterminer les affixes des vecteurs suivants :
$-3\vec{u}$; $5\vec{u}$; $3\vec{u}-5\vec{v}$

3) Déterminer les affixes des vecteurs $\overrightarrow{AB}$ et $\overrightarrow{CD}$:
$A(2;5)$, $B(1;3)$, $C(3;0)$ et $D(-3;2)$

Ex 2-2 : ***Vecteurs colinéaires***

1) Soit $\vec{t}$ d'affixe $3-i$, $A(3,-1)$ et $B(x,3)$.

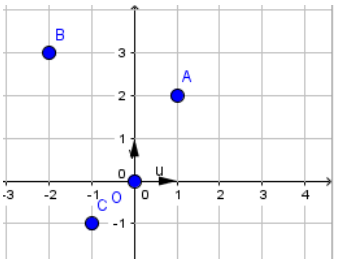
Pour quelle valeur de x , $\vec{t}$ est-il colinéaire à $\overrightarrow{AB}$?

2) Soit $A(3;4)$, $B(1,2)$, $C(a;0)$ et $D(4;-b)$.

Pour quelles valeurs de a et b , ABCD est-il un parallélogramme ?

Ex 2-3 : ***Lire et calculer des affixes***

1) Lire les affixes des points A, B et C.



2) Lire les affixes des vecteurs :
$\overrightarrow{AB}$, $\overrightarrow{AC}$ et $\overrightarrow{CB}$

3) Déterminer les affixes des milieux des côtés su triangle ABC.

Ex 2-4 : ***Affixe et parallélogramme***

Soit A, B et C les points d'affixes $z_A=5-i$, $z_B=4-3i$ et $z_C=-2+2i$.

1) Déterminer l'affixe du vecteur $\overrightarrow{AB}$.

2) Déterminer l'affixe de D tel que ABCD soit un parallélogramme.

3) Vérifier que ses diagonales ont le même milieu.

Ex 2-5 : ***Affixes de vecteurs et droites***

Soit A, B, C et D les points d'affixes $z_A=4+i$, $z_B=3-2i$, $z_C=-4+3i$ et $z_D=-1+9i$.

Déterminer les affixes des vecteurs $\overrightarrow{AB}$ et $\overrightarrow{DC}$.

Que peut-on dire des droites (AB) et (CD) ?

Ex 2-6 : ***Affixes, centre de gravité et points alignés***

Soit A, B et C les points d'affixes $z_A=3+2i$, $z_B=4-3i$ et $z_C=-2+2i$.

1) Déterminer l'affixe du centre de gravité G de ABC.
(Le centre de gravité G vérifie $\overrightarrow{GA}+\overrightarrow{GB}+\overrightarrow{GC}=\overrightarrow{0}$)

2) Déterminer l'affixe du milieu I de [BC] et montrer que les points A,I et G sont alignés.

Ex 2-7 : ***Affixes et centre de gravité***

Soit A, B, C et D les points d'affixes $z_A=3i$, $z_B=4+i$, $z_C=2-3i$ et $z_D=-2-i$.

1) Déterminer les affixes des vecteurs $\overrightarrow{AB}$ et $\overrightarrow{DC}$. Que peut-on en déduire ?

2) Soit G tel que $2\overrightarrow{GA}-\overrightarrow{GB}+2\overrightarrow{GC}=\overrightarrow{0}$. Déterminer l'affixe de G.

3) Montrer que G est le centre de gravité de ACD.

Ex 2-8 : ***Ensembles de points***

Dans le plan complexe muni d'un repère orthonormé $(O;\vec{u},\vec{v})$, déterminer dans chacun des cas l'ensemble des points M d'affixe $z=x+iy$

1) $3z+5i\bar{z}=7-2i$

2) $(1-2i)z+(1+2i)\bar{z}=z\bar{z}$

3) $z^2+\bar{z}\in\mathbb{R}$

4) $(1+z)(i+\bar{z}) \in i\mathbb{R}$

5) $\dfrac{z+1-2i}{z-3+2i} \in \mathbb{R}$

6) $\dfrac{z+1-2i}{z-3+2i} \in i\mathbb{R}$

Modules

Ex 2-9 : ***Calculs***

Déterminer le module des nombres complexes ci-dessous :

$z_1 = 2-3i$

$z_2 = 3+4i$

$z_3 = -4i$

$z_4 = -3$

Ex 2-10 : ***Calculs***

1) Soit z un nombre complexe de module r .
Déterminer $|-z|$ et $|iz|$.

2) Déterminer les longueurs AB et CD avec $z_A = 2+3i$, $z_B = 1+4i$, $z_C = 3i$ et $z_D = 5-2i$.

3) Déterminer le module des nombres :
-2 ; 5 ; $3i$; $-2i$; $-1-i$; $\sqrt{3}+i$; $\sqrt{3}-3i$

Ex 2-11 : ***Appliquer les formules***

Déterminer le module des nombres complexes ci-dessous :

$z_1 = (1+i)(2-3i)$

$z_2 = (5+2i)+(3-i)$

$z_3=\frac{2+i}{1-i}$

$z_4=(1-i)^4$

Ex 2-12 : ***L'ensemble*** $\mathbb{U}$

Montrer que les nombres complexes ci-dessous appartiennent à l'ensemble $\mathbb{U}$.

$z_1=\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i$, $z_2=i$, $z_3=\frac{\sqrt{5}}{3}+\frac{2}{3}i$, $\frac{z_1}{z_2}$

Ex 2-13 : ***Ensembles de points***

Dans chacun des cas, déterminer géométriquement l'ensemble des points M dont l'affixe z vérifie :

1) $|z-3-2i|=5$

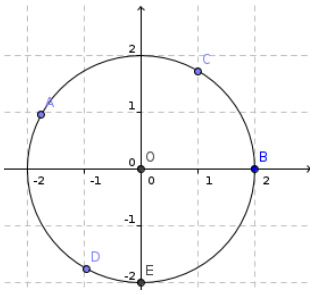
2) $|z-2-i|=|z+5-i|$

3) $|z+i|=|z-1|$

Arguments

Ex 2-14 : ***Lecture graphique***

Lire le module et un argument des affixes des points de la figure :



Ex 2-15 : ***S'aider de la représentation graphique***

Dans le plan complexe muni d'un repère orthonormé $(O;\vec{u},\vec{v})$, représenter, puis déterminer le module et un argument des nombres :

$z_1=-1+i$, $z_2=-1-i$, $z_3=-4$, $z_4=3i$

Ex 2-16 : ***Avec la calculatrice***

En utilisant la calculatrice déterminer un argument des nombres complexes ci-dessous :

-2 ; $-2i$; $-1-i$; $\sqrt{3}+i$; $\sqrt{3}-3i$

Ex 2-17 : ***Appliquer les formules***

Soit z un nombre complexe de module r et d'argument θ .
Déterminer en fonction de θ les arguments ci-dessous :

$\arg(-z)$, $\arg(iz)$, $\arg(z^5)$ et $\arg\left(-\frac{i}{z}\right)$

Ex 2-18 :

Soit z un nombre complexe de module 1 et d'argument $\frac{7\pi}{8}\ [2\pi]$.

Déterminer le module et un argument de :
$z_1=2z$, $z_2=iz$, $z_3=-3z$, $z_4=-3iz$, $z_5=\bar{z}$

Ex 2-19 : ***Représenter graphiquement***

Dans le plan complexe muni d'un repère orthonormé $(O;\vec{u},\vec{v})$, représenter les points M d'affixe z tels que :

1) $\arg(z)=\frac{\pi}{3}\ [2\pi]$

2) $\arg(z)=\frac{-2\pi}{3}\ [2\pi]$

3) $\begin{cases}\arg(z)=\frac{\pi}{4}[2\pi]\\ |z|=3\end{cases}$

Forme trigonométrique

Ex 2-20 :

Déterminer une forme trigonométrique des nombres complexes ci-dessous :

$z_1=-3i$

$z_2=4-4i$

$z_3=-\sqrt{3}+3i$

Ex 2-21 : ***Forme trigonométrique ou pas ?***

Les nombres complexes ci-dessous sont-ils écrits sous forme trigonométrique ?

1) $z_1=3\left(\cos\left(\frac{\pi}{4}\right)-i\sin\left(\frac{\pi}{4}\right)\right)$

2) $z_2=-3\left(\cos\left(\frac{\pi}{4}\right)+i\sin\left(\frac{\pi}{4}\right)\right)$

3) $z_3=3\left(\cos\left(\frac{\pi}{4}\right)+i\sin\left(\frac{\pi}{4}\right)\right)$

4) $z_4=3\left(\cos\left(\frac{\pi}{3}\right)+i\sin\left(\frac{\pi}{4}\right)\right)$

Ex 2-22 : ***De la forme trigonométrique à la forme algébrique***

Déterminer la forme algébrique des nombres complexes ci-dessous :

1) $z_1=2\left(\cos\left(\frac{\pi}{2}\right)+i\sin\left(\frac{\pi}{2}\right)\right)$

2) $z_2=3\left(\cos\left(\frac{-\pi}{3}\right)+i\sin\left(\frac{-\pi}{3}\right)\right)$

3) $z_3=3\left(\cos\left(\frac{\pi}{4}\right)+i\sin\left(\frac{\pi}{4}\right)\right)$

Ex 2-23 : ***Écrire sous forme trigonométrique***

Écrire les nombres complexes ci-dessous sous forme trigonométrique

1) $z_1=3\left(\cos\left(\frac{\pi}{4}\right)-i\sin\left(\frac{\pi}{4}\right)\right)$

2) $z_2=-3\left(\cos\left(\frac{\pi}{4}\right)+i\sin\left(\frac{\pi}{4}\right)\right)$

3) $z_3=3\left(\cos\left(\frac{-\pi}{3}\right)+i\sin\left(\frac{\pi}{3}\right)\right)$

Avec des suites

Ex 2-24 : ***Conjecture avec Python***

Soit la suite (z_n) de nombres complexes définie par :

$$\begin{cases} z_0=2 \\ z_{n+1}=\left(\frac{\sqrt{3}}{2}-\frac{i}{2}\right)z_n \end{cases}$$

1) Calculer z_1 , z_2 , z_3 et z_4 .

2) On considère le programme ci-dessous écrit en Python :

```
1  from math import sqrt
2
3  def suite(n):
4      z=complex(2,0)
5      for k in range(1,n+1):
6          z=z*complex(sqrt(3)/2,-1/2)
7          r=abs(z)
8      return(r)
9
10 print(suite(10))
11 print(suite(20))
12 print(suite(30))
```

complex(a,b) permet de définir le nombre complexe $a+ib$

abs(z) retourne le module du nombre complexe z

Le programme affiche :

```
>>>
1.999999999999999
1.9999999999999978
1.999999999999997
```

a) Que renvoie la fonction suite() ?

b) Que peut-on conjecturer ?

c) Démontrer cette conjecture.

3) Démontrer que pour tout entier naturel n , on a :

$$\arg(z_n) = \frac{-n\pi}{6} \quad [2\pi]$$

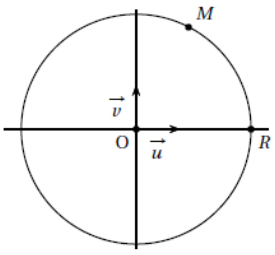
4) Démontrer que pour tout entier naturel k , z_{6k+3} est un imaginaire pur.

Ex 2-25 : ***Baccalauréat S – Antilles-Guyane 22 juin 2015 – ex 3***

Complexes – suite géométrique – géométrie - inégalité triangulaire

On appelle $\mathbb{C}$ l'ensemble des nombres complexes.

Dans le plan complexe muni d'un repère orthonormé $\left(O, \vec{u}, \vec{v}\right)$ on a placé un point M d'affixe z appartenant à $\mathbb{C}$, puis le point R intersection du cercle de centre O passant par M et du demi-axe $\left[O ; \vec{u}\right)$.



1. Exprimer l'affixe du point R en fonction de z.
2. Soit le point M' d'affixe z' définie par

$$z' = \frac{1}{2}\left(\frac{z+|z|}{2}\right).$$

Reproduire la figure sur la copie et construire le point M'.

Partie B

On définit la suite de nombres complexes (z_n) par un premier terme z_0 appartenant à $\mathbb{C}$ et, pour tout entier naturel n, par la relation de récurrence :

$$z_{n+1} = \frac{z_n + |z_n|}{4}.$$

Le but de cette partie est d'étudier si le comportement à l'infini de la suite $(|z_n|)$ dépend du choix de z_0.

1. Que peut-on dire du comportement à l'infini de la suite $(|z_n|)$ quand z_0 est un nombre réel négatif ?
2. Que peut-on dire du comportement à l'infini de la suite $(|z_n|)$ quand z_0 est un nombre réel positif ?
3. On suppose désormais que z_0 n'est pas un nombre réel.
   a. Quelle conjecture peut-on faire sur le comportement à l'infini de la suite $(|z_n|)$?
   b. Démontrer cette conjecture, puis conclure.*

NOMBRES COMPLEXES ET TRIGONOMÉTRIE

1) TRIGONOMÉTRIE

A) FORMULES D'ADDITION

Propriétés :

$\forall\, a \in \mathbb{R}$ et $\forall\, b \in \mathbb{R}$, on a :

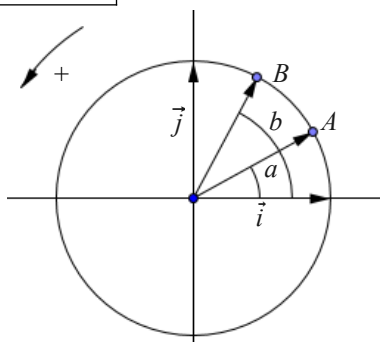
$\cos(a-b) = \cos a \cos b + \sin a \sin b$; $\cos(a+b) = \cos a \cos b - \sin a \sin b$

$\sin(a-b) = \sin a \cos b - \sin b \cos a$; $\sin(a+b) = \sin a \cos b + \sin b \cos a$

Preuve :

- $\cos(a-b) = \cos a \cos b + \sin a \sin b$

On considère le cercle trigonométrique C de centre O muni du repère orthonormal direct $(O\,;\vec{i}\,;\vec{j})$.
On note A et B les points de C, définis par $(\vec{i}\,,\overrightarrow{OA}) = a$ et $(\vec{i}\,,\overrightarrow{OB}) = b$.



Les coordonnées de A et de B sont respectivement

D'autre part, on a :

$(\overrightarrow{OA}\,,\overrightarrow{OB}) = ($

(la propriété utilisée est la relation de Chasles)

Calculons alors de deux manières le produit scalaire $\overrightarrow{OA}\cdot\overrightarrow{OB}$:

- *avec les coordonnées* :
- *en utilisant* $\cos(\overrightarrow{OA}\,,\overrightarrow{OB})$:

Ainsi $\cos(a-b) = \cos a \cos b + \sin a \sin b$

Pour les trois autres formules, il suffit d'appliquer $\cos(a-b) = \cos a \cos b + \sin a \sin b$ après les modifications suivantes :

$\cos(a+b) = \cos(a-(-b))$ …

$\sin(a+b) = \cos\left(\frac{\pi}{2} - (a+b)\right) = \cos\left(\left(\frac{\pi}{2} - a\right) - b\right) = \ldots$

$\sin(a-b) = \sin(a+(-b)) =$ …

Exemple :

En remarquant que $\frac{\pi}{12} = \frac{\pi}{3} - \frac{\pi}{4}$, on peut calculer les valeurs exactes de $\cos\frac{\pi}{12}$ et $\sin\frac{\pi}{12}$.

- $\cos\frac{\pi}{12} =$
- $\sin\frac{\pi}{12} = s$

B) FORMULES DE DUPLICATION ET DE LINÉARISATION

Propriétés :

FORMULES DE DUPLICATION	*FORMULES DE LINÉARISATION*
$\forall\, a \in \mathbb{R}$, on a : • $\sin 2a = 2\sin a \cos a$ • $\cos 2a = \cos^2 a - \sin^2 a$ $= 2\cos^2 a - 1$ $= 1 - 2\sin^2 a$	• $\cos^2 a = \frac{1+\cos(2a)}{2}$ • $\sin^2 a = \frac{1-\cos(2a)}{2}$

Preuve :

En prenant $b=a$, dans les formules précédentes on obtient $\sin 2a = 2\sin a \cos a$ et $\cos 2a = \cos^2 a - \sin^2 a$.

En utilisant la relation $\cos^2 a + \sin^2 a = 1$, on obtient $\cos 2a = 2\cos^2 a - 1$ et $\cos 2a = 1 - 2\sin^2 a$

On en déduit les deux dernières formules.

2) NOTATION EXPONENTIELLE D'UN NOMBRE COMPLEXE

D'après les résultats précédemment démontrés, l'argument du produit de deux nombres complexes est égal à la somme des arguments de ces deux nombres . C'est-à-dire que la fonction $f : \theta \longmapsto \cos\theta + i\sin\theta$ est telle que $f(\theta+\theta') = f(\theta)\times f(\theta')$.

Elle vérifie donc l'équation fonctionnelle caractéristique de la fonction exponentielle.

Notation : Pour $\theta \in \mathbb{R}$, on note $\cos\theta + i\sin\theta = e^{i\theta}$ et par conséquent pour $r \in \mathbb{R}_+^*$, on a $r(\cos\theta + i\sin\theta) = r\,e^{i\theta}$
Cette notation est appelée **notation exponentielle**.

Propriétés :

Les résultats déjà vus s'écrivent, avec la notation exponentielle :

$e^{i\theta}\times e^{i\theta'} = e^{i(\theta+\theta')}$ $\qquad \dfrac{1}{e^{i\theta}} = e^{i(-\theta)} = e^{-i\theta}$ $\qquad \dfrac{e^{i\theta}}{e^{i\theta'}} = e^{i(\theta-\theta')}$

$(e^{i\theta})^n = e^{in\theta} = e^{ni\theta}$, $n \in \mathbb{Z}$ $\qquad \overline{e^{i\theta}} = e^{-i\theta}$ $\qquad -e^{i\theta} = e^{i(\theta+\pi)}$

Remarques :

- La propriété $e^{i\theta}\times e^{i\theta'} = e^{i(\theta+\theta')}$, facile à retenir, permet de retrouver les **formules d'addition** :

En effet, on a d'une part : $e^{i(\theta+\theta')} = \cos(\theta+\theta') + i\sin(\theta+\theta')$

Et d'autre part : $e^{i\theta}\times e^{i\theta'} = (\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = \ldots = (\cos\theta\cos\theta' - \sin\theta\sin\theta') + i\sin\theta\cos\theta' + \cos\theta\sin\theta'$

En identifiant les parties réelles et imaginaires, on obtient :

et

- La propriété $(e^{i\theta})^2 = e^{2i\theta}$ permet, en procédant de la même façon, de retrouver les **formules de duplication** :

$\cos 2\theta = \cos^2\theta - \sin^2\theta$ et $\sin 2\theta = 2\sin\theta\cos\theta$

3) FORMULES DE MOIVRE ET D'EULER

On montre facilement :

Propriété : FORMULES D'EULER

Pour tout réel θ , on a :

$$\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2} \quad \text{et} \quad \sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2i}$$

Remarque :

Il est souvent utile de retenir les formules ainsi :

Propriété : FORMULE DE MOIVRE

Pour tout réel θ , et pour tout entier naturel n on a :

$$(e^{i\theta})^n = e^{ni\theta} \quad \Leftrightarrow \quad (\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Formules d'addition :

$\forall a \in \mathbb{R}$ et $\forall b \in \mathbb{R}$, on a :

$\cos(a-b) = \cos a \cos b + \sin a \sin b$ $\qquad$ $\cos(a+b) = \cos a \cos b - \sin a \sin b$

$\sin(a-b) = \sin a \cos b - \sin b \cos a$ $\qquad$ $\sin(a+b) = \sin a \cos b + \sin b \cos a$

Formules de duplication :

$\forall a \in \mathbb{R}$, on a :

- $\sin 2a = 2 \sin a \cos a$
- $\cos 2a = \cos^2 a - \sin^2 a$
  $= 2\cos^2 a - 1$
  $= 1 - 2\sin^2 a$

Formules de linéarisation :

$\forall a \in \mathbb{R}$, on a :

- $\cos^2 a = \dfrac{1+\cos(2a)}{2}$
- $\sin^2 a = \dfrac{1-\cos(2a)}{2}$

Notation exponentielle d'un nombre complexe :

Pour $\theta \in \mathbb{R}$, on note $\cos\theta + i\sin\theta = e^{i\theta}$ et par conséquent pour $r \in \mathbb{R}_+^*$, on a $r(\cos\theta + i\sin\theta) = r\,e^{i\theta}$
Cette notation est appelée **notation exponentielle**.

Propriétés :

Les résultats déjà vus s'écrivent, avec la notation exponentielle :

$e^{i\theta} \times e^{i\theta'} = e^{i(\theta+\theta')}$ $\qquad$ $\dfrac{1}{e^{i\theta}} = e^{i(-\theta)} = e^{-i\theta}$ $\qquad$ $\dfrac{e^{i\theta}}{e^{i\theta'}} = e^{i(\theta-\theta')}$

$(e^{i\theta})^n = e^{in\theta} = e^{ni\theta}$, $n \in \mathbb{Z}$ $\qquad$ $\overline{e^{i\theta}} = e^{-i\theta}$ $\qquad$ $-e^{i\theta} = e^{i(\theta+\pi)}$

- La propriété $e^{i\theta} \times e^{i\theta'} = e^{i(\theta+\theta')}$, facile à retenir, permet de retrouver les **formules d'addition** :

En effet, on a d'une part : $e^{i(\theta+\theta')} = \cos(\theta+\theta') + i\sin(\theta+\theta')$

Et d'autre part :

$e^{i\theta} \times e^{i\theta'} = (\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = \ldots = (\cos\theta\cos\theta' - \sin\theta\sin\theta') + i\sin\theta\cos\theta' + \cos\theta\sin\theta'$

En identifiant les parties réelles et imaginaires, on obtient :

$\cos(\theta+\theta') = \cos\theta\cos\theta' - \sin\theta\sin\theta'$ et $\sin(\theta+\theta') = \sin\theta\cos\theta' + \cos\theta\sin\theta'$

- La propriété $(e^{i\theta})^2 = e^{2i\theta}$ permet, en procédant de la même façon, de retrouver les **formules de duplication** :

$\cos 2\theta = \cos^2\theta - \sin^2\theta$ et $\sin 2\theta = 2\sin\theta\cos\theta$

Formules d'Euler :

Pour tout réel θ, on a :

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \quad \text{et} \quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

Il est souvent utile de retenir les formules ainsi :

$$e^{i\theta} + e^{-i\theta} = 2\cos\theta \quad \text{et} \quad e^{i\theta} - e^{-i\theta} = 2i\sin\theta$$

Formule de Moivre :

Pour tout réel θ, et pour tout entier naturel n on a :

$$(e^{i\theta})^n = e^{ni\theta} \Leftrightarrow (\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

Trigonométrie

Ex 1 : ***En fonction de*** $\cos x$ ***et*** $\sin x$

Exprimer en fonction de $\cos x$ et $\sin x$.

a) $\cos\left(x-\frac{\pi}{3}\right)$

b) $\sin\left(x-\frac{\pi}{4}\right)$

c) $\cos\left(\frac{4\pi}{3}-x\right)$

d) $\sin\left(-\frac{5\pi}{6}-x\right)$

Ex 2 : $\cos(2a)$, $\sin(2a)$

1) Peut-on avoir :

a) $\cos(2a)=2\cos(a)$

b) $\sin(2a)=2\sin(a)$

2) On donne $\cos a=\frac{\sqrt{6}+\sqrt{2}}{4}$ (où $a\in\left[0;\frac{\pi}{2}\right]$).

En calculant $\cos(2a)$, trouver a .

Ex 3 : ***Équations***

Trouver les solutions réelles des équations ci-dessous :

a) $\sin(2x)=\cos x$

b) $3\cos(2x)+2\sin^2 x=0$

Ex 4 : ***Simplification***

Simplifier $P=\cos x\cos\left(\frac{x}{2}\right)\cos\left(\frac{x}{4}\right)\sin\left(\frac{x}{4}\right)$

Ex 5 : ***Valeur exacte de*** $\cos\left(\frac{7\pi}{12}\right)$ ***et*** $\sin\left(\frac{7\pi}{12}\right)$

a) Exprimer $\frac{7\pi}{12}$ en fonction de $\frac{\pi}{4}$ et de $\frac{\pi}{3}$.

b) Déterminer la valeur exacte de $\cos\left(\frac{7\pi}{12}\right)$ et celle de $\sin\left(\frac{7\pi}{12}\right)$.

La notation exponentielle

Ex 6 : ***Mettre sous forme exponentielle***

Mettre sous forme exponentielle les nombres complexes :

$z_1=-\sqrt{3}+i$

$z_2=-2-2i$

$z_3=-\frac{1}{2}(\sqrt{3}+i)$

$z_4=3-i\sqrt{3}$

$z_5=4+4i$

En déduire les formes exponentielles de z_1z_2 , de $z_3z_4z_5$ et de $\frac{z_2}{z_3}$.

Ex 7 : ***Mettre sous forme algébrique***

Mettre sous forme algébrique les nombres complexes :

$z_1=4e^{\frac{i\pi}{2}}$

$z_2=e^{i\pi}$

$z_3=2e^{i\frac{3\pi}{4}}$

Ex 8 : ***Mettre sous forme exponentielle***

Les questions sont indépendantes.

1) On pose $z=3-i\sqrt{3}$

a) Déterminer l'écriture exponentielle de z .

b) En déduire les écritures exponentielles de :

$z_1=3z$

$z_2=iz$

$z_3=-2z$

$z_4=-4iz$

2) Soit $z = r\,e^{i\theta}$ (où $r>0$).

Déterminer l'écriture exponentielle de :

$-z$

iz

$-iz$

$\bar{z}$

$-i\bar{z}$

3) Soit $a \in \mathbb{R}$. Déterminer l'écriture exponentielle des nombres suivants :

$\cos a - i \sin a$

$\sin a + i \cos a$

$-\sin a + i \cos a$

Ex 9 : Valeur exacte de $\cos\left(\frac{\pi}{12}\right)$ et de $\sin\left(\frac{\pi}{12}\right)$

Soit $z_1 = \dfrac{\sqrt{6} - i\sqrt{2}}{2}$ et $z_2 = 1 + i$.

1) Déterminer les formes exponentielles de z_1 et de z_2 .

2) En déduire celle de $Z = z_1 z_2$

3) Déterminer la forme algébrique de Z.

4) En déduire la valeur exacte de $\cos\left(\frac{\pi}{12}\right)$ et de $\sin\left(\frac{\pi}{12}\right)$

Ex 10 : ***Retrouver des formules de trigonométrie***

En utilisant la forme exponentielle, exprimer les expressions suivantes en fonction de $\cos x$ et de $\sin x$.

$\cos\left(\frac{\pi}{2} + x\right)$

$\sin\left(\frac{\pi}{2} - x\right)$

Ex 11 : ***Un calcul pas si compliqué ...***

Déterminer le module et un argument de $\left(\dfrac{3 + i\sqrt{3}}{2 - 2i}\right)^4$.

Formules d'Euler et formule de Moivre

Ex 12 : ***Reconnaître les formules d'Euler***

Soit x un nombre réel.

Écrire sous forme algébrique les nombres complexes ci-dessous :

$a=3\left(e^{ix}+e^{-ix}\right)$

$b=e^{-ix}-e^{ix}$

$c=e^{i7x}+e^{-i7x}$

$d=e^{i2x}-e^{-2ix}$

Ex 13 : ***Simplification d'écriture***

Simplifier l'écriture du nombre suivant : $b=\left(e^{i\theta}-e^{-i\theta}\right)^2-\left(e^{i\theta}+e^{-i\theta}\right)^2$

Ex 14 : ***Utilisation du demi-angle : un grand classique***

Soit $\theta\in]0;2\pi[$.

1) En factorisant par $e^{i\frac{\theta}{2}}$, déterminer le module et un argument de $a=1+e^{i\theta}$.

2) Faire de même pour $b=1-e^{i\theta}$.

3) Montrer que $\frac{a}{b}$ est un imaginaire pur.

Ex 15 : ***Linéarisation et formules d'Euler :*** $\cos^5 x$

Soit $n\in\mathbb{N}$. Linéariser $\cos^n x$, c'est l'écrire en fonction de sommes de $\cos(px)$ où $p\in\mathbb{N}$.

1) Développer $(a+b)^5$.

2) En utilisant les formules d'Euler, montrer que :

$$\cos^5 x = \frac{1}{32}\left(e^{5ix}+5e^{3ix}+10e^{ix}+10e^{-ix}+5e^{-3ix}+e^{-5ix}\right)$$

3) En utilisant à nouveau les formules d'Euler, en déduire la linéarisation de $\cos^5 x$.

La linéarisation est un outil important pour déterminer des primitives.

<u>Ex 16 :</u> *Linéarisation et formules d'Euler :* $\sin^4 x$

1) Développer $(a+b)^4$ et en déduire le développement de $(a-b)^4$.

2) En utilisant les formules d'Euler, montrer que :

$$\sin^4 x = \frac{1}{16}\left(e^{i4x}-4e^{i2x}+6-4e^{-i2x}+e^{-i4x}\right)$$

3) En utilisant à nouveau les formules d'Euler, en déduire la linéarisation de $\sin^4 x$.

Ex 17 : ***Linéarisation et formules d'Euler :*** $\sin^3 x$

Linéariser $\sin^3 x$. (l'écrire en fonction de sommes de $\sin(px)$ où $p \in \mathbb{N}$)

Ex 18 : ***Déterminer des sommes trigonométriques très connues***

1) Montrer que $\cos(n\theta)=\Re e\left(\left(e^{i\theta}\right)^n\right)$ et $\sin(n\theta)=\Im m\left(\left(e^{i\theta}\right)^n\right)$

2) On pose $C_n=\sum_{k=0}^{n}\cos(k\theta)$ et $S_n=\sum_{k=0}^{n}\sin(k\theta)$

Montrer en utilisant la question 1) et les formules d'Euler que :

$$C_n=\cos\left(n\frac{\theta}{2}\right)\frac{\sin\left((n+1)\frac{\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)} \quad \text{et} \quad S_n=\sin\left(n\frac{\theta}{2}\right)\frac{\sin\left((n+1)\frac{\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}$$

Avec des suites

Ex 19 : ***D'après Baccalauréat S – Pondichéry 8 avril 2014 – ex 3***

Complexes – suite géométrique – algorithme – géométrie

Le plan complexe est muni d'un repère orthonormé $(O, \vec{u}, \vec{v})$.
Pour tout entier naturel n, on note A_n le point d'affixe z_n défini par :

$$z_0 = 1 \quad \text{et} \quad z_{n+1} = \left(\frac{3}{4}+\frac{\sqrt{3}}{4}i\right)z_n.$$

On définit la suite (r_n) par $r_n = |z_n|$ pour tout entier naturel n.

1. Donner la forme exponentielle du nombre complexe $\frac{3}{4}+\frac{\sqrt{3}}{4}i$.
2. a. Montrer que la suite (r_n) est géométrique de raison $\frac{\sqrt{3}}{2}$.
   b. En déduire l'expression de r_n en fonction de n.
   c. Que dire de la longueur OA_n lorsque n tend vers $+\infty$?
3. On considère l'algorithme suivant :

```
from math import sqrt
R=1
n=0
p=float(input("p="))
while (R>p):
    n=n+1
    R=sqrt(3)/2*R
print(n)
```

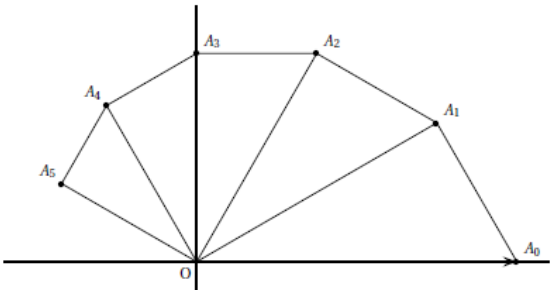
a. Quelle est la valeur affichée par l'algorithme pour $P = 0,5$?

b. Pour $P = 0,01$ on obtient $n = 33$. Quel est le rôle de cet algorithme ?

4. a. Démontrer que le triangle OA_nA_{n+1} est rectangle en A_{n+1}.

b. On admet que $z_n = r_n e^{i\frac{n\pi}{6}}$.
Déterminer les valeurs de n pour lesquelles A_n est un point de l'axe des ordonnées.

c. Compléter la figure donnée en annexe, à rendre avec la copie, en représentant les points A_6, A_7, A_8 et A_9.
Les traits de construction seront apparents.



LES NOMBRES COMPLEXES : ÉQUATIONS POLYNOMIALES

1) ÉQUATION DU SECOND DEGRÉ À COEFFICIENTS RÉELS

Propriété :

L'équation $az^2+bz+c=0$, où a, b et c sont des réels (avec $a\neq 0$) admet dans $\mathbb{C}$ deux solutions (éventuellement confondues).
Soit $\Delta=b^2-4ac$ le discriminant de l'équation. Δ est un nombre réel.

- si $\Delta \geqslant 0$, les deux solutions sont réelles : $z_1=\dfrac{-b-\sqrt{\Delta}}{2a}$ et $z_2=\dfrac{-b+\sqrt{\Delta}}{2a}$
- si $\Delta<0$, les deux solutions sont des nombres complexes non réels, conjugués l'un de l'autre :

$$z_1=\frac{-b-i\sqrt{-\Delta}}{2a} \quad \text{et} \quad z_2=\frac{-b+i\sqrt{-\Delta}}{2a}$$

Le trinôme az^2+bz+c peut alors se factoriser sous la forme $az^2+bz+c=a(z-z_1)(z-z_2)$.

Preuve :

On considère l'équation $az^2+bz+c=0$, où a, b et c sont des réels (avec $a\neq 0$)

On peut écrire $az^2+bz+c=a\left(z^2+\dfrac{b}{a}z+\dfrac{c}{a}\right)=a\left(\left(z+\dfrac{b}{2a}\right)^2-\dfrac{b^2}{4a^2}+\dfrac{c}{a}\right)=a\left(\left(z+\dfrac{b}{2a}\right)^2-\dfrac{b^2-4ac}{4a^2}\right)=a\left(\left(z+\dfrac{b}{2a}\right)^2-\dfrac{\Delta}{4a^2}\right)$

- si $\Delta>0$, l'équation a deux solutions réelles, et deux seulement .

  Comme $\mathbb{R}\subset\mathbb{C}$, l'équation a donc deux solutions complexes et deux seulement qui sont : $z_1=\dfrac{-b-\sqrt{\Delta}}{2a}$ et $z_2=\dfrac{-b+\sqrt{\Delta}}{2a}$

- si $\Delta=0$, l'équation a une solution réelle $z=-\dfrac{b}{2a}$

- si $\Delta<0$, $-\Delta>0$ et on peut écrire :
  on obtient alors :

La démonstration fait apparaître la factorisation du trinôme az^2+bz+c sous la forme $az^2+bz+c=a(z-z_1)(z-z_2)$.

On en déduit que l'équation $az^2+bz+c=0$ a deux solutions complexes qui sont : $z_1=\dfrac{-b-i\sqrt{-\Delta}}{2a}$ et $z_2=\dfrac{-b+i\sqrt{-\Delta}}{2a}$

Ces deux solutions sont des nombres complexes non réels, conjugués l'un de l'autre.

2) POLYNÔMES

Définitions :

Soit un entier naturel n et a_0 , a_1 , …, a_n des réels.
Une **fonction polynôme à coefficients réels** (ou **polynôme**), est une fonction souvent notée P définie sur $\mathbb{C}$ qui admet une unique écriture sous la forme :

$$P(z)=a_nz^n+a_{n-1}z^{n-1}+\ldots+a_1z+a_0$$

Le **polynôme nul** est le polynôme P défini pour tout nombre complexe z par $P(z)=0$.

Si P n'est pas le polynôme nul, n est le **degré** de P

On appelle **racine** du polynôme P tout nombre complexe z_0 tel que $P(z_0)=0$.

Exemples :

$P_1(z)=5$

$P_2(z)=5z^4-2z^2+1$

$P_3(z)=12z^7$

Remarque :

On admet (ce qui est du bon sens) qu'un polynôme est le polynôme nul si et seulement si tous ses coefficients sont nuls.

3) FACTORISATION DES POLYNÔMES

Définition :

On dit qu'un polynôme P est factorisable (ou divisible) par $z-a$ s'il existe un polynôme Q tel que pour tout $z\in\mathbb{C}$:

$$P(z)=(z-a)Q(z)$$

Exemple :

$P(z)=4z^2-25$

Propriété :

Soit un complexe a et n un entier naturel .
Pour tout $z\in\mathbb{C}$, z^n-a^n est factorisable par $z-a$ et :

$$z^n-a^n=(z-a)(z^{n-1}+a\,z^{n-2}+a^2\,z^{n-3}+\ldots+a^{n-2}\,z+a^{n-1})=(z-a)\sum_{k=0}^{n-1}a^k\,z^{n-1-k}$$

Preuve : ***exigible***

Si $a=0$, la propriété est évidente.

Supposons maintenant $a\neq 0$.

Dans les complexes, les propriétés calculatoires sont identiques à celles que nous avons dans $\mathbb{R}$.

On en déduit donc que la formule permettant de calculer la somme des termes consécutifs d'une suite géométrique reste vraie dans $\mathbb{C}$.

Pour tout nombre complexe q , on a donc :

En remplaçant q par $\frac{z}{a}$ dans l'égalité précédente, on obtient :

$$\left(\frac{z}{a}\right)^n-1=$$

$$\Rightarrow \quad \frac{z^n}{a^n}-1=$$

$$\Rightarrow \quad \frac{z^n-a^n}{a^n}=\left(\frac{z-a}{a}\right)\left(\frac{a^{n-1}}{a^{n-1}}+\frac{a^{n-2}z}{a^{n-1}}+\frac{a^{n-3}z^2}{a^{n-1}}+\ldots+\frac{z^{n-1}}{a^{n-1}}\right)$$

$$\Rightarrow \quad \frac{z^n-a^n}{a^n}=\frac{(z-a)(a^{n-1}+a^{n-2}z+a^{n-3}z^2+\ldots+z^{n-1})}{a\,a^{n-1}}$$

$$\Rightarrow \quad \frac{z^n-a^n}{a^n}=\frac{(z-a)(a^{n-1}+a^{n-2}z+a^{n-3}z^2+\ldots+z^{n-1})}{a^n}$$

$$\Rightarrow \quad z^n-a^n=(z-a)(a^{n-1}+a^{n-2}z+a^{n-3}z^2+\ldots+z^{n-1})$$

Propriété :

Soit un complexe a .
Un polynôme P est factorisable par $z-a$ si et seulement si a est une racine de P .

Preuve : *exigible*

Si P est factorisable par $z-a$, il est immédiat que a est une racine de P .

Montrons la réciproque :

Soit P un polynôme à coefficients réels de degré n .

On peut donc écrire P sous la forme $P(z)=a_n z^n+a_{n-1}z^{n-1}+\ldots+a_1 z+a_0$ où a_0 , a_1 , …, a_n sont des réels.

On a alors

$P(z)-P(a)=$

Or d'après la propriété précédente, il existe des polynômes Q_n , Q_{n-1} , …, Q_2 tels que :

$z^n-a^n=(z-a)Q_n$, $z^{n-1}-a^{n-1}=(z-a)Q_{n-1}$, … , $z^2-a^2=(z-a)Q_2$

On en déduit que :

$P(z)-P(a)=$

Ainsi $P(z)-P(a)$, c'est à dire $P(z)$ (étant donné que $P(a)=0$) est bien factorisable par $z-a$

4) DEGRÉ ET RACINES

Propriété :

Un polynôme non nul P , de degré n , admet au plus n racines.

Preuve : *exigible*

Soit la propriété $H(n)$: «L'équation $P(z)=0$, où P est un polynôme de degré n a un nombre de solutions inférieur ou égal à n » , où $n\in\mathbb{N}^*$

Montrons cette propriété par récurrence.

Initialisation :

Toute équation du premier degré du type $az+b=0$ a au plus une solution . Donc $H(1)$ est vraie.

Hérédité :

On suppose $H(n)$ vraie pour un entier naturel n supérieur ou égal à 1 fixé , c'est à dire :

L'équation $P(z)=0$, où P est un polynôme de degré n a un nombre de solutions inférieur ou égal à n . (HR)

Montrons que $H(n+1)$ est vraie, c'est à dire :

- Si P n'a pas de racines, alors l'équation $P(z)=0$ a bien sûr moins de $n+1$ solutions.

- Si P a eu moins une racine complexe a , alors il existe un polynôme Q de degré n tel que

Conclusion :

$H(n)$ est vraie pour tout $n\in\mathbb{N}^*$.

Équation du second degré à coefficients réels :

L'équation $az^2+bz+c=0$, où a, b et c sont des réels (avec $a\neq 0$) admet dans $\mathbb{C}$ deux solutions (éventuellement confondues).

Soit $\Delta=b^2-4ac$ le discriminant de l'équation. Δ est un nombre réel.

- si $\Delta\geqslant 0$, les deux solutions sont réelles : $z_1=\dfrac{-b-\sqrt{\Delta}}{2a}$ et $z_2=\dfrac{-b+\sqrt{\Delta}}{2a}$
- si $\Delta<0$, les deux solutions sont des nombres complexes non réels, conjugués l'un de l'autre :

$$z_1=\frac{-b-i\sqrt{-\Delta}}{2a} \quad \text{et} \quad z_2=\frac{-b+i\sqrt{-\Delta}}{2a}$$

Le trinôme az^2+bz+c peut alors se factoriser sous la forme $az^2+bz+c=a(z-z_1)(z-z_2)$.

Avec une Ti-spire

cSolve(5·z²−10+15·z·i=0,z)

z=−i or z=−2·i

cFactor(5·z²−10+15·z·i,z)

5·(z+i)·(z+2·i)

Polynôme :

Soit un entier naturel n et a_0, a_1, …, a_n des réels.
Une **fonction polynôme à coefficients réels** (ou **polynôme**), est une fonction souvent notée P définie sur $\mathbb{C}$ qui admet une unique écriture sous la forme :

$$P(z)=a_n z^n+a_{n-1}z^{n-1}+\ldots+a_1 z+a_0$$

On admet (ce qui est du bon sens) qu'un polynôme est le polynôme nul si et seulement si tous ses coefficients sont nuls.

Le **polynôme nul** est le polynôme P défini pour tout nombre complexe z par $P(z)=0$.

Si P n'est pas le polynôme nul, n est le **degré** de P

On appelle **racine** du polynôme P tout nombre complexe z_0 tel que $P(z_0)=0$.

Factorisation des polynômes :

Un polynôme P est **factorisable** (ou divisible) par $z-a$ s'il existe un polynôme Q tel que pour tout $z\in\mathbb{C}$:

$$P(z)=(z-a)Q(z)$$

Propriété :

Soit un complexe a et n un entier naturel .
Pour tout $z\in\mathbb{C}$, z^n-a^n est factorisable par $z-a$ et :

$$z^n-a^n=(z-a)(z^{n-1}+a z^{n-2}+a^2 z^{n-3}+\ldots+a^{n-2}z+a^{n-1})=(z-a)\sum_{k=0}^{n-1}a^k z^{n-1-k}$$

Propriété :

Soit un complexe a .
Un polynôme P est factorisable par $z-a$ si et seulement si a est une racine de P .

Avec une Ti-spire

cFactor(z⁴+3·z³−9·z²+3·z−10,z)

(z−2)·(z+5)·(z−i)·(z+i)

Degré et racines :

Un polynôme non nul P , de degré n , admet au plus n racines.

Équations

Ex 4-1 : ***Équations du second degré***

Résoudre dans $\mathbb{C}$ les équations ci-dessous .

1) $z^2-2z+2=0$

2) $2z^2-2z+3=0$

3) $2z^2-2z-3=0$

4) $z+\frac{1}{z}=1$

5) $z+\frac{1}{z}=\sqrt{3}$

6) $\frac{z-1}{z+2}=z$

Ex 4-2 : ***Équation de degré 3 : factorisation immédiate***

Résoudre dans $\mathbb{C}$ l'équation $3z^3-2z^2+z=0$ (E)

Ex 4-3 : ***Équation de degré 4 : se ramener à un équation du second degré***

Résoudre dans $\mathbb{C}$ l'équation $z^4+5z^2+6=0$ (E).

Ex 4-4 : ***Avec l'inverse : se ramener à un équation du second degré***

Résoudre dans $\mathbb{C}$ l'équation $\frac{1}{z^2}+\frac{1}{z}+2=0$.

Ex 4-5 : ***Système***

Résoudre dans $\mathbb{C}$ le système $\begin{cases} z+z'=6 \\ zz'=12 \end{cases}$

Ex 4-6 : ***Équation de degré 4 : images des solutions sur un cercle***

Soit $f(z)=z^4-\sqrt{2}z^3-4\sqrt{2}z-16$.

1) Trouver deux réels a et b tels que $f(z)=(z^2+4)(z^2+az+b)$.

2) Résoudre dans $\mathbb{C}$ l'équation $f(z)=0$.

3) Soit A, B , C et D les images des solutions de l'équation précédente. Montrer que ces points sont sur un même cercle dont on déterminera le centre et le rayon.

Ex 4-7 : ***Somme et produit des racines***

1) Soit z_1 et z_2 les solutions de l'équation à coefficients réels $az^2+bz+c=0$.

Montrer que $z_1+z_2=-\frac{b}{a}$ et $z_1z_2=\frac{c}{a}$.

2) Soit z_1 et z_2 deux nombres de produit $P \neq 0$ et de somme S.
Montrer que z_1 et z_2 sont solutions de l'équation $x^2 - Sx + P = 0$.

3) Soit z_1 et z_2 les solutions de l'équation $2z^2 - 3z + 3 = 0$.
Sans résoudre l'équation, calculer le module de $z_1^{-1} + z_2^{-1}$.

Factorisation

Ex 4-8 : ***Factoriser des polynômes du second degré***

Factoriser les polynômes ci-dessous dans $\mathbb{C}$:

1) $P(z) = z^2 + 9$

2) $Q(z) = 2z^2 + 2z + 1$

3) $R(z) = 3z^2 + \sqrt{3}z + 1$

Ex 4-9 : ***Factoriser un polynôme de degré 3***

Soit $P(z) = z^3 + 6z^2 + 13z + 10$

1) Calculer $P(-2)$

2) En déduire une factorisation de $P(z)$ dans les réels.

Ex 4-10: ***Factoriser un polynôme de degré 3***

Soit $Q(z) = 8z^3 - 1$. En factorisant, résoudre l'équation $Q(z) = 0$ dans $\mathbb{C}$.

Ex 4-11 : ***Factoriser un polynôme de degré 4***

Soit $P(z)=z^4-5z^3+7z^2-5z+6$.

1) Démontrer que pour tout complexe z , on a : $P(\overline{z})=\overline{P(z)}$

2) Déterminer une racine imaginaire pure évidente de P.

3) Quelle autre racine la question 1 permet-elle de trouver ?

4) Factoriser $P(z)$ dans les réels.

Ex 4-12 : ***Factoriser un polynôme de degré 4***

Soit $P(z)=z^4+6z^3+15z^2+18z$

1) Déterminer un réel a tel que $P(z)=(z^2+3z)^2+a(z^2+3z)$

2) Factoriser $P(z)$ dans les réels et résoudre l'équation $P(z)=0$ dans $\mathbb{C}$

Ex 4-13 : ***Factoriser un polynôme de degré 4***

Soit $P(z)=z^4-2z^3+12z^2-8z+32$

1) Démontrer que $2i$ et $-2i$ sont des racines de P.

2) Justifier que $P(z)$ peut être factorisé par z^2+4 .

3) Déterminer l'ensemble des racines de P dans les complexes.

Avec des coefficients complexes

Ex 4-14 : ***Racines carrées d'un nombre complexe***

Soit un nombre complexe $c=a+ib$ où a et b sont des réels.

On cherche les éventuels nombres complexes vérifiant l'équation $z^2=c$ (E)

1) Cas où $b=0$:

a) Que peut-on dire de la nature de c ?

b) Déterminer l'ensemble des nombres complexes solutions de (E).

2) Cas où $b \neq 0$:

On pose $z = x + iy$ où x et y sont des réels.

a) Montrer que si x et y existent alors : $\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$

b) Montrer que $x^2 + y^2 = \sqrt{a^2 + b^2}$

c) En déduire x^2 et y^2 .

d) Que peut-on dire du signe de x et y si $b > 0$?

En déduire que (E) a deux solutions et exprimer les solutions en fonction de a et b .

e) En procédant de la même façon, traiter le cas $b < 0$.

Ex 4-15 : ***Application de l'exercice précédent***

1) Déterminer les solutions de l'équation $z^2 = -2 + 2i\sqrt{3}$ (E_1)

2) Soit le polynôme $P(z) = z^4 + 4z^2 + 16$

a) Combien P a-t-il de racines au maximum ?

b) Résoudre l'équation $Z^2 + 4Z + 16 = 0$ (E).

c) En déduire l'ensemble des racines de P.

d) Justifier que les racines obtenues sont constituées de deux paires de racines conjuguées.

Ex 4-16 : ***Factoriser un polynôme de degré 3***

Soit $R(z) = z^3 - (1+i)z + z - 1 - i$

1) Trouver une racine évidente de R.

2) En déduire une factorisation de R dans $\mathbb{C}$.

Ex 4-17: ***Équation de degré 3 à coefficients complexes***

Soit $P(z)=z^3-(16-i)z^2+(89-16i)z+89i$.

1) Calculer $P(-i)$.

2) Trouver deux nombres réels a et b tels que $P(z)=(z+i)(z^2+az+b)$.

3) Résoudre dans $\mathbb{C}$ l'équation $P(z)=0$.

Sur tout le chapitre des complexes

Ex 4-18 : ***Baccalauréat S – Antilles-Guyane 11 septembre 2014 – ex 4***

Complexes – équations – ensembles de points

On note $\mathbb{C}$ l'ensemble des nombres complexes.
Le plan complexe est muni d'un repère orthonormé $(O, \vec{u}, \vec{v})$. On prendra comme unité 2 cm sur chaque axe.
Le graphique sera fait sur une feuille de papier millimétré et complété au fur et à mesure des questions.

On considère la fonction f qui à tout nombre complexe z associe

$$f(z) = z^2 + 2z + 9.$$

1. Calculer l'image de $-1+i\sqrt{3}$ par la fonction f.
2. Résoudre dans $\mathbb{C}$ l'équation $f(z) = 5$.
   Écrire sous forme exponentielle les solutions de cette équation.
   Construire alors sur le graphique, à la règle et au compas, les points A et B dont l'affixe est solution de l'équation (A étant le point dont l'affixe a une partie imaginaire positive).
   On laissera les traits de construction apparents.
3. Soit λ un nombre réel. On considère l'équation $f(z) = \lambda$ d'inconnue z.
   Déterminer l'ensemble des valeurs de λ pour lesquelles l'équation $f(z) = \lambda$ admet deux solutions complexes conjuguées.
4. Soit (F) l'ensemble des points du plan complexe dont l'affixe z vérifie

$$|f(z) - 8| = 3.$$

   Prouver que (F) est le cercle de centre $\Omega(-1\ ;\ 0)$ et de rayon $\sqrt{3}$.
   Tracer (F) sur le graphique.
5. Soit z un nombre complexe, tel que $z = x + iy$ où x et y sont des nombres réels.
   a. Montrer que la forme algébrique de $f(z)$ est

$$x^2 - y^2 + 2x + 9 + i(2xy + 2y).$$

   b. On note (E) l'ensemble des points du plan complexe dont l'affixe z est telle que $f(z)$ soit un nombre réel.
   Montrer que (E) est la réunion de deux droites D_1 et D_2 dont on précisera les équations.
   Compléter le graphique de l'annexe en traçant ces droites.
6. Déterminer les coordonnées des points d'intersection des ensembles (E) et (F).

Ex 4-19 : ***Baccalauréat S – Asie 16 juin 2015 – ex 4***

Complexes – le nombre j – géométrie

Le plan est muni du repère orthonormé direct $\left(O, \vec{u}, \vec{v}\right)$.

On donne le nombre complexe $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Le but de cet exercice est d'étudier quelques propriétés du nombre j et de mettre en évidence un lien de ce nombre avec les triangles équilatéraux.

Partie A : propriétés du nombre j

1. **a.** Résoudre dans l'ensemble $\mathbb{C}$ des nombres complexes l'équation

$$z^2 + z + 1 = 0.$$

   b. Vérifier que le nombre complexe j est une solution de cette équation.

2. Déterminer le module et un argument du nombre complexe j, puis donner sa forme exponentielle.
3. Démontrer les égalités suivantes :
   a. $j^3 = 1$;
   b. $j^2 = -1 - j$.
4. On note P, Q, R les images respectives des nombres complexes 1, j et j^2 dans le plan.
   Quelle est la nature du triangle PQR ? Justifier la réponse.

Partie B

Soit a, b, c trois nombres complexes vérifiant l'égalité $a + jb + j^2c = 0$.
On note A, B, C les images respectives des nombres a, b, c dans le plan.

1. En utilisant la question A - 3. b., démontrer l'égalité : $a - c = j(c - b)$.
2. En déduire que AC = BC .
3. Démontrer l'égalité : $a - b = j^2(b - c)$.
4. En déduire que le triangle ABC est équilatéral.*

LES NOMBRES COMPLEXES : UTILISATION

1) INTERPRÉTATION GÉOMÉTRIQUE DE $\frac{c-a}{b-a}$

On se place dans le plan rapporté à un repère orthonormal direct $(O\,;\vec{u}\,,\vec{v})$.

Propriétés :

Soit A, B , C et D quatre points distincts d'affixes respectives a , b , c et d . On a :

- $\left|\frac{c-a}{b-a}\right|=\frac{\text{AC}}{\text{AB}}$
- $\arg\left(\frac{c-a}{b-a}\right)=(\overrightarrow{\text{AB}}\,,\overrightarrow{\text{AC}})\ [2\pi]$

Preuve :

- On a bien $a\neq b$ car les points sont distincts . On a alors :
  $\left|\frac{c-a}{b-a}\right|=$

- La preuve de la deuxième propriété nécessite de connaître quelques propriétés des angles orientés de vecteurs qui sont faciles à mettre en place en faisant un schéma.

Soit $\vec{u}$, $\vec{v}$ et $\vec{w}$ trois vecteurs non nuls du plan orienté . On a :
- Relation de Chasles : $(\vec{u}\,,\vec{v})+(\vec{v}\,,\vec{w})=(\vec{u}\,,\vec{w})\ [2\pi]$
- $(\vec{u}\,,\vec{v})=-(\vec{v}\,,\vec{u})\ [2\pi]$

$$\arg\left(\frac{c-a}{b-a}\right)=\arg(c-a)-\arg(b-a)=(\vec{u}\,,\overrightarrow{\text{AC}})-(\vec{u}\,,\overrightarrow{\text{AB}})\ [2\pi]$$
$$=-(\vec{u}\,,\overrightarrow{\text{AB}})+(\vec{u}\,,\overrightarrow{\text{AC}})\ [2\pi]$$
$$=(\overrightarrow{\text{AB}}\,,\vec{u})+(\vec{u}\,,\overrightarrow{\text{AC}})\ [2\pi]$$
$$=(\overrightarrow{\text{AB}}\,,\overrightarrow{\text{AC}})\ [2\pi]$$ (D'après la relation de Chasles)

Remarques :

Soit A, B , C et D quatre points distincts d'affixes respectives a , b , c et d . On a :

- A appartient à la médiatrice de [BC] si et seulement si

- Les points A, B et C sont alignés si et seulement si

- Les droites (AB) et CD) sont perpendiculaires si et seulement si

2) RACINES *n*-ièmes DE l'UNITÉ

On se place dans le plan rapporté à un repère orthonormal direct $(O\,;\vec{u}\,,\vec{v})$.

Définition :

Soit n un entier naturel non nul.
On appelle racine *n*-ième de l'unité, tout nombre complexe z vérifiant $z^n=1$.

1 est bien sûr toujours une racine *n*-ième de l'unité

Remarque :

Les racines *n*-ième de l'unité sont les racines du polynôme $\text{P}(z)=z^n-1$

Propriété et définition :

Soit n un entier naturel non nul.
L'équation $z^n=1$ admet exactement n racines *n*-ièmes de l'unité distinctes.
Il s'agit des nombres complexes $e^{i\frac{2k\pi}{n}}$ où $k\in\{0,1,2,\dots,n-1\}$

On note U_n l'ensemble des racines *n*-ièmes de l'unité

Preuve :

Soit n un entier naturel non nul et un complexe $z=r\,\mathrm{e}^{i\theta}$ où $r\in\mathbb{R}_+^*$ et $\theta\in\mathbb{R}$. On a :

$z^n=1 \quad \Leftrightarrow$

Ainsi tous les nombres complexes $\mathrm{e}^{i\frac{2k\pi}{n}}$ où $k\in\mathbb{Z}$ sont solutions de l'équation $z^n=1$.

En particulier les nombres complexes $\mathrm{e}^{i\frac{2k\pi}{n}}$ où $k\in\{0,1,2,\dots,n-1\}$ sont bien sûr solutions.

Soit K un entier quelconque.
En effectuant la division euclidienne de K par n , on obtient.

On retrouve donc une solution de la forme $\mathrm{e}^{i\frac{2k\pi}{n}}$ où $k\in\{0,1,2,\dots,n-1\}$ et on en déduit le résultat attendu.

Propriété :

Soit n un entier naturel non nul.
Les points images des éléments de U_n appartiennent au cercle trigonométrique.

Pour $n\geqslant 3$, les points images des éléments de U_n sont les sommets d'un polygone régulier à n sommets.

Ce qui est trivial, car ils ont pour module 1.

Quelques cas particuliers :

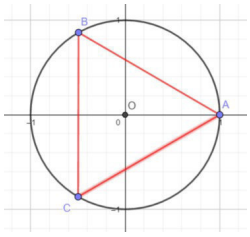
- Les racines 2-ièmes (ou racines carrées) de l'unité sont les nombres complexes tels que $z^2=1$.

  Dans ce cas on trouve facilement -1 et 1 . On a

- Les racines 3-ièmes de l'unité sont les nombres complexes tels que $z^3=1$.
  Les solutions sont les nombres complexes :

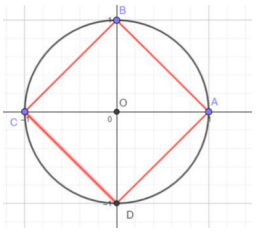
  On note :
  $j=\mathrm{e}^{i\frac{2\pi}{3}}$. On a alors $\bar{j}=\mathrm{e}^{i\frac{4\pi}{3}}$. Ainsi

  Les points images des éléments de U_3 ts du triangle équilatéral ABC.



- Les racines 4-ièmes de l'unité sont les nombres complexes tels que $z^4=1$.

  Dans ce cas on peut factoriser facilement pour déterminer les racines de l'unité :



  Les points images des éléments de U_4 sont les sommets du carré ABCD.

Interprétation géométrique de :

$$\frac{c-a}{b-a}$$

On se place dans le plan rapporté à un repère orthonormal direct $(O;\vec{u},\vec{v})$.

Soit A, B , C et D quatre points distincts d'affixes respectives a , b , c et d . On a :

- $\left|\frac{c-a}{b-a}\right|=\frac{AC}{AB}$
- $\arg\left(\frac{c-a}{b-a}\right)=(\overrightarrow{AB},\overrightarrow{AC})\ [2\pi]$

Remarques importantes :

- A appartient à la médiatrice de [BC] si et seulement si $\left|\frac{c-a}{b-a}\right|=1$
- Les points A, B et C sont alignés si et seulement si $\arg\left(\frac{c-a}{b-a}\right)=0\ [\pi]$, ce qui revient à dire que $\frac{c-a}{b-a}$ est **un réel**.
- Les droites (AB) et CD) sont perpendiculaires si et seulement si $\arg\left(\frac{c-a}{b-a}\right)=\frac{\pi}{2}\ [\pi]$, ce qui revient à dire que $\frac{c-a}{b-a}$ est un **imaginaire pur**.

Racines *n*-ième de l'unité :

Les racines *n*-ième de l'unité sont les racines du polynôme $P(z)=z^n-1$

Soit n un entier naturel non nul.
On appelle **racine *n*-ième de l'unité**, tout nombre complexe z vérifiant $z^n=1$.

1 est bien sûr toujours une racine *n*-ième de l'unité

Soit n un entier naturel non nul.
L'équation $z^n=1$ admet exactement n racines *n*-ièmes de l'unité distinctes.
Il s'agit des nombres complexes $e^{i\frac{2k\pi}{n}}$ où $k\in\{0,1,2,\dots,n-1\}$

On note U_n l'ensemble des racines *n*-ièmes de l'unité .

$$U_n=\left\{e^{i\frac{2k\pi}{n}},k\in\{0,1,2,\dots n-1\}\right\}$$

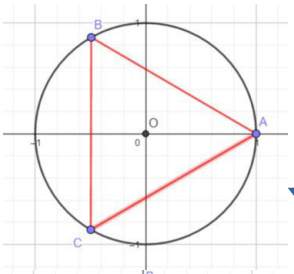
Propriété :

Soit n un entier naturel non nul.
Les points images des éléments de U_n appartiennent au cercle trigonométrique.

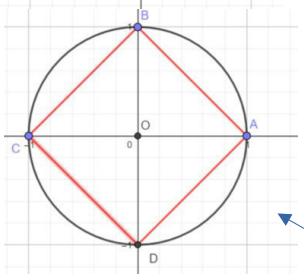
Pour $n\geqslant 3$, les points images des éléments de U_n sont les sommets d'un polygone régulier à n sommets.

Quelques cas particuliers :

- **Les racines 2-ièmes (ou racines carrées) de l'unité** sont les nombres complexes tels que $z^2=1$.
  Dans ce cas on trouve facilement -1 et 1 . On a $U_2=\{-1;1\}$



- **Les racines 3-ièmes de l'unité** sont les nombres complexes tels que $z^3=1$.
  Les solutions sont les nombres complexes : $e^{i\frac{2\times0\times\pi}{3}}=e^0=1$, $e^{i\frac{2\times1\times\pi}{3}}=e^{i\frac{2\pi}{3}}$ et $e^{i\frac{2\times2\times\pi}{3}}=e^{i\frac{4\pi}{3}}$
  On note : $j=e^{i\frac{2\pi}{3}}$.
  On a alors $\bar{j}=e^{i\frac{4\pi}{3}}$. Ainsi $U_3=\{1,j,\bar{j}\}$
  Les points images des éléments de U_3 sont les sommets du triangle équilatéral ABC.



- **Les racines 4-ièmes de l'unité** sont les nombres complexes tels que $z^4=1$.
  Dans ce cas on peut factoriser facilement pour déterminer les racines de l'unité :

$$z^4=1 \Leftrightarrow z^4-1=0 \Leftrightarrow (z^2-1)(z^2+1)=0 \Leftrightarrow (z-1)(z+1)(z-i)(z+i)=0$$

  Ainsi $U_4=\{1;i;-1;-i\}$

  Les points images des éléments de U_4 sont les sommets du carré ABCD.

Dans toute la fiche d'exercice, le plan complexe est muni d'un repère orthonormé direct $(O; \vec{u}, \vec{v})$

Interprétation géométrique du module et de l'argument

Ex 5-1 : ***Comprendre la formule de l'argument d'un quotient***

Dans chacun des cas déterminer une mesure en radian de $(\overrightarrow{OA}, \overrightarrow{OB})$ où A et B sont deux points du plan complexe.

1) $A(-4)$ et $B(-2i)$

2) $A(\sqrt{3}+i)$ et $B(1-i\sqrt{3})$

3) $A(4+6i)$ et $B(-3+2i)$

Ex 5-2 : ***Comprendre la formule de l'argument d'un quotient***

Dans chacun des cas déterminer une mesure en radian de $(\overrightarrow{AB}, \overrightarrow{AC})$ où A, B et C sont trois points du plan complexe, puis déduire des calculs le rapport $\frac{AC}{AB}$.

1) $A(3+2i)$, $B(6+4i)$ et $C(1+5i)$

2) $A(2-5i)$, $B(3-6i)$ et $C(4-7i)$

3) $A(3-i)$, $B(5-i)$, et $C(5-3i)$

Ex 5-3 : ***Valider ou infirmer une conjecture géométrique***

Dans le plan complexe, on considère les points $A(3+4i)$, $B(-5-6i)$ et $C(11-2i)$.

1) Placer ces trois points, et conjecturer la nature du triangle ABC.

2) Écrire sous forme algébrique $\frac{z_C - z_A}{z_B - z_A}$, puis valider ou infirmer la conjecture précédente.

Ex 5-4 : ***Valider ou infirmer une conjecture géométrique***

Dans le plan complexe, on considère les points $A(1+5i)$, $B(7,5+4,5i)$, $C(7-2i)$ et $D(0,5-1,5i)$.

1) Placer ces quatre points, et conjecturer la nature du quadrilatère ABCD.

2) Valider ou infirmer la conjecture précédente.

Ex 5-5 : ***Ensemble de points, arguments et angles orientés de vecteurs***

Soit A,B,C et D les points d'affixes $z_A=1$, $z_B=i$, $z_C=-1$ et $z_D=-i$.

Dans chacun des cas, déterminer l'ensemble des points d'affixe z vérifiant la condition donnée et tracer cet ensemble dans un repère.

1) $\arg(z-i)=-\frac{\pi}{2}+2k\pi$ (où $k\in\mathbb{Z}$)

2) $\arg\left(\frac{z-i}{z-1}\right)=2k\pi$ (où $k\in\mathbb{Z}$)

3) $\arg\left(\frac{z+i}{z+1}\right)=\pi+2k\pi$ (où $k\in\mathbb{Z}$)

4) $\frac{z+i}{z-1}$ soit un imaginaire pur.

Ex 5-6 : ***Vecteurs orthogonaux, points alignés,*** $\Re e(z'\bar{z})$ ***et*** $\Im m(z'\bar{z})$

Soit M et M′ d'affixes $z=x+iy$ et $z'=x'+iy'$ où x , y , x' et y' sont des nombres réels. En utilisant $\frac{z'}{z}$, montrer que :

1) $\overrightarrow{OM}$ et $\overrightarrow{OM'}$ sont orthogonaux si, et seulement si , $\Re e(z'\bar{z})=0$

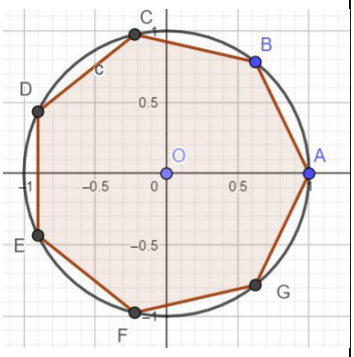
2) O , M et M′ sont alignés si, et seulement si $\Im m(z'\bar{z})=0$

Racines n-ième de l'unité

Ex 5-7 : ***Heptagone et affixe des sommets***

Soit l'heptagone régulier ABCDEFG

Donner l'affixe de chacun de ses sommets sous forme exponentielle.



Ex 5-8 : ***Représenter les solutions de*** U_n

Résoudre dans $\mathbb{C}$ les équations ci-dessous, puis tracer le polygone dont les sommets ont pour affixes ces solutions.

1) $z^8=1$

2) $z^{12}=1$

Ex 5-9 : ***Utiliser les racines n-ièmes de l'unité pour résoudre une équation***

Résoudre dans $\mathbb{C}$ les équations c-dessous **:**

1) $(z-i)^4=1$

2) $z^5=4\sqrt{2}$

3) $z^6=(2-i)^6$

Ex 5-10 : ***Utiliser les racines n-ièmes de l'unité pour résoudre une équation***

On considère dans $\mathbb{C}$ l'équation $z^4-28+96i=0\,(\mathrm{E})$.

1) Montrer que $z_0=3-i$ est une solution de (E)

2) En déduire que l'équation (E) est équivalente à l'équation $z^4={z_0}^4$

3) Résoudre (E).

Ex 5-11 : ***Utiliser les racines n-ièmes de l'unité pour résoudre une équation***

1) Résoudre dans $\mathbb{C}$ l'équation $z^4=1$.

2) Soit z un nombre complexe . On pose $z=\frac{u-1}{u+1}$ (avec $u\neq -1$) .

Exprimer u en fonction de z .

3) En déduire les solutions dans $\mathbb{C}$ de l'équation $(u-1)^4=(u+1)^4$.

Ex 5-12 : ***Somme des racines n-ièmes de l'unité***

1) Soit $\omega\in \mathrm{U}_7$ tel que $\omega\neq 1$.

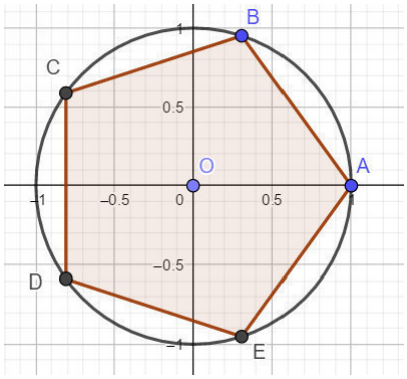
Montrer que $\omega^k\in \mathrm{U}_7$ pour tout $k\in\{0,1,\dots,6\}$

On admet la réciproque, ce qui signifie que l'ensemble U_7 est constitué des complexes ω^k avec $k\in\{0,1,\dots,6\}$ où ω est un élément quelconque de U_7 .

2) Justifier que la somme des éléments de U_7 est nulle.

Ex 5-13 : ***Construction à la règle non graduée et au compas d'un pentagone régulier***

Le but de l'exercice est de construire à la règle non graduée et au compas le pentagone régulier ci-contre.



1) On considère les points K(-1) et $\mathrm{J}\left(\frac{i}{2}\right)$.

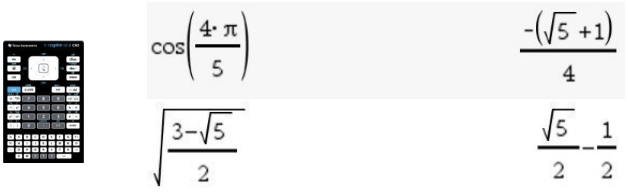
Le cercle de centre J et de rayon $\frac{1}{2}$ coupe le segment [KJ] en L.

Calculer les longueurs KJ et KL.

2) Donner sous forme exponentielle l'affixe de C.

3) Montrer que $KC^2 = 2 + 2\cos\left(\frac{4\pi}{5}\right)$

4) La calculatrice affiche :



En utilisant les résultats de la calculatrice, montrer que $KC = KL$

5) Dans le plan complexe, construire à la règle non graduée et au compas un pentagone régulier.

Fonctions dans les complexes

Ex 5-14 :

Soit I le point d'affixe $2i$ et f la fonction qui à tout point M d'affixe z, associe le point M' d'affixe z' tel que $z' = iz$.

1) a) Déterminer l'affixe du point A' , l'image par f du point A d'affixe $1+\sqrt{2}+i$.

b) Montrer que A, I et A' sont alignés.

2) a) Montrer que les points M du plan tels que M, I et M' soient alignés sont sur le cercle Γ de centre Ω d'affixe $1+i$ et de rayon $\sqrt{2}$.

b) Montrer que $A \in \Gamma$.

c) Déterminer l'ensemble Γ' décrit par le point M' lorsque le point M décrit Γ .

3) Soit B le point d'affixe $2+2i$ et B' son image par f .
a) Montrer que $(AB) \perp (A'B')$

b) Soit C le point d'intersection des droites (AB) et $(A'B')$.

Calculer $\frac{z_B - z_A}{z_A}$ puis en déduire la nature du quadrilatère $OACA'$.

Ex 5-15 :

Soit les points A et B d'affixes respectives 2 et -2 et f la fonction qui à tout point M (différent de A) d'affixe z, associe le point M' d'affixe z' tel que $z' = \frac{z(z-2)}{z-2}$.

1) a) Déterminer l'affixe du point P' image par f du point P d'affixe $1+i$.

b) Montrer que $(AP) // (BP')$.

c) Montrer que $(AP) \perp (PP')$.

2) Déterminer l'ensemble des points invariants par f.

On cherche maintenant à généraliser les propriétés 1b) et 1c) pour obtenir une construction de l'image M' d'un point M quelconque du plan.

3) a) Montrer que pour tout nombre complexe z, $(z-2)(\bar{z}-2) \in \mathbb{R}$.

b) En déduire que pour tout nombre complexe distinct de 2, $\frac{z'+2}{z-2} \in \mathbb{R}$.

c) Montrer que $(AM) // (BM')$.

4) Soit M un point quelconque tel que $M \notin (AB)$. Généraliser le résultat de la question 1c)

5) Soit M un point distinct de A. déduire des questions précédentes une construction du point M' image de M par f.
Réaliser une figure pour le point Q d'affixe $3-2i$.

DIVISIBILITÉ ET CONGRUENCES

1) ENSEMBLES $\mathbb{N}$ et $\mathbb{Z}$

L'ensemble $\{0;1;2;\ldots\}$ est appelé ensemble des **entiers naturels** . Il est noté $\mathbb{N}$.
L'ensemble $\{\ldots;-3;-2;-1;0;1;2;3;\ldots\}$ est appelé ensemble des **entiers relatifs (ou entiers)** . Il est noté $\mathbb{Z}$.

Remarques :

- $\mathbb{N}$ est une partie de $\mathbb{Z}$:
- La somme et le produit de deux entiers naturels sont des entiers naturels.
- La somme et le produit de deux entiers relatifs sont des entiers relatifs.

Propriété : *admise*

Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

Une partie non vide de $\mathbb{Z}$ n'a pas nécessairement de plus petit élément.

Exemples :

- Soit A = { 8 ; 12 ; 14 ; 21 }
- Soit B l'ensemble des entiers naturels impairs. B est une partie de $\mathbb{N}$.

2) DIVISIBILITÉ

Définition :

Soit a et b deux entiers relatifs .

S'il existe un entier relatif k tel que $b = k \times a$, on dit que b est un **multiple** de a ou que a est un **diviseur** de b .
On dit aussi que b est **divisible** par a et que a **divise** b . (on ne dit jamais que b multiplie a)

Pour indiquer que a divise b, on note $a \mid b$.

Exemple :
De l'égalité $54 = 6 \times 9$, on peut déduire :

Remarque :
L'ensemble des multiples de 3 est l'ensemble des nombres de la forme $3 \times k$ avec $k \in \mathbb{Z}$. Cet ensemble est noté $3\mathbb{Z}$.

Propriétés :

- Soit a et b deux entiers relatifs . Si a divise b et si $b \neq 0$, alors $|a| \leq |b|$.
- Tout entier relatif $b \neq 0$ a un nombre fini de diviseurs.

On peut traduire la première propriété en termes de multiples :
Si n est un multiple non nul de p, alors $|n| \geq |p|$.

Preuve :

- Soit a et b deux entiers relatifs tels que a divise b et $b \neq 0$.
  Puisque a divise b, on peut écrire $b = ak$ avec $k \in \mathbb{Z}$, donc $|b| = |ak| = |a| \times |k|$
  Comme $b \neq 0$, on a $k \neq 0$, donc $|k| \geq 1$ et par conséquent $|b| \geq |a|$.

- Soit b un entier relatif non nul.
  Si a est un diviseur de b, on a vu que $|a| \leq |b|$, donc $-|b| \leq a \leq |b|$
  a peut donc prendre au maximum $2 \times |b| + 1$ valeurs et le nombre de diviseurs de b est fini (inférieur à $2 \times |b| + 1$)

Propriété :

Soit a, b et c trois entiers relatifs.
Si a divise b, alors a divise bc.

On peut traduire la propriété en termes de multiples :
Si b est un multiple de a, alors bc est un multiple de a.

Preuve :

Remarque :
Tout multiple d'un multiple de a est un multiple de a.

Propriété:

Soit a, b et c trois entiers relatifs.
Si a divise b et si a divise c alors a divise $b + c$ et a divise $b - c$.

Plus généralement, si a divise b et si a divise c alors a divise tout nombre de la forme $bu + cv$ où u et v sont des entiers relatifs.

On peut traduire la propriété en termes de multiples :
Si b et c sont des multiples de a, alors $bu + cv$ est un multiple de a.

Preuve :
Si a divise b, on peut écrire $b = a \times k$ avec $k \in \mathbb{Z}$.
Si a divise c, on peut écrire $c = a \times k'$ avec $k' \in \mathbb{Z}$.
Alors pour tous les entiers relatifs u et v, on peut écrire :

Comme $ku + k'v$ est un élément de $\mathbb{Z}$, on en déduit que a divise $bu + cv$.

Propriétés :

Soit a, b, c des entiers relatifs.

- 1, -1, a, $-a$ sont des diviseurs de a.
- Si a divise b alors $-a$ divise b , a divise $-b$ et $-a$ divise $-b$.
- Si a divise b et si b divise a , alors $a = b$ ou $a = -b$. (c'est-à-dire que $|a| = |b|$)
- Si a divise b et si b divise c, alors a divise c.
- Si a divise b alors pour tout entier relatif c, ac divise bc.

3) DIVISION EUCLIDIENNE

Propriété d'Archimède :

Soit b un entier naturel non nul.
Pour tout entier naturel a, il existe un entier naturel n tel que $a < nb$.

Preuve :
b étant un entier naturel non nul, on a $b \geq 1$, donc $(a + 1)b \geq a + 1 > a$.
Il suffit donc de prendre $n = a + 1$ pour que nb soit strictement supérieur à a .
Il existe donc un entier naturel n tel que $a < nb$

Remarque :
Cela revient à dire que l'ensemble des multiples de b ($b \neq 0$) n'est pas majoré par a, et ceci pour tout $a \in \mathbb{N}$.
On en déduit que l'ensemble des multiples de b ($b \neq 0$) n'est pas majoré.

Exemple :
$b = 3$; $a = 52$ pour $n \geq 18$, on $a < nb$.

Rappel : Technique de la division d'entiers naturels
On peut écrire $43 = 8 \times 5 + 3$.
43 s'appelle le **dividende**, 5 **le diviseur**, 8 **le quotient** et 3 **le reste**.

43	5
3	8

On a $3 < 5$.
Le reste doit toujours être strictement inférieur au diviseur.

Remarque :
Les multiples de 5 sont 0, 5, 10, 15, 20, 25, 30, 35, 40, 45 et on choisit $40 = 8 \times 5$ car $45 > 43$.
Pour chercher le quotient d'une division, on cherche en pratique les multiples du diviseur et on choisit celui qui précède immédiatement le multiple supérieur au dividende.

Division euclidienne dans $\mathbb{N}$:

Soit a un entier naturel et b un entier naturel non nul.

Il existe un unique couple (q ; r) d'entiers naturels tel que : $a = bq + r$ et $r < b$.

a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.
On dit que le couple unique (q ; r) est le résultat de la division euclidienne de a par b.

Preuve :
Soit a un entier naturel et b un entier naturel non nul.

- Existence du couple $(q\ ;\ r)$

Considérons l'ensemble E des entiers naturels n tels que $a < bn$. $E = \{n \in \mathbb{N}\ /\ a < bn\}$.
Puisque b est non nul, on sait d'après la propriété d'Archimède que l'ensemble E est non vide.
E est donc une partie non vide de $\mathbb{N}$, E a donc un plus petit élément.
Ce plus petit élément p n'est pas nul, car 0 n'appartient pas à E.
On a donc $p \geq 1$. Posons $q = p - 1$. Alors $q \in \mathbb{N}$.
D'autre part $q \notin E$. (le plus petit élément de E est p et $q < p$)
Puisque $q \notin E$, on a $bq \leq a$ et comme $p \in E$, on a aussi $a < bp$ c'est-à-dire $a < b(q + 1)$.
On a donc trouvé un entier naturel q tel que $bq \leq a < b(q + 1)$.
Posons $r = a - bq$. On a $r \in \mathbb{N}$ et $a = bq + r$.
D'autre part : $bq \leq a < b(q + 1) \Leftrightarrow bq \leq a < bq + b \Leftrightarrow 0 \leq a - bq < b \Leftrightarrow 0 \leq r < b$.
Il existe donc un couple $(q\ ;\ r)$ d'entiers naturels tel que $a = bq + r$ et $r < b$.

- Unicité du couple $(q\ ;\ r)$

Supposons qu'il existe un deuxième couple $(q'\ ;\ r')$ vérifiant les mêmes conditions.
On a alors : $bq + r = bq' + r' \Leftrightarrow b(q - q') = r' - r$.
Or, on a : $0 \leq r < b \Leftrightarrow -b < -r \leq 0$
Et $0 \leq r' < b$
On en déduit que : $-b < r' - r < b \Leftrightarrow |r' - r| < b$

Par ailleurs on a vu que $r' - r = b(q - q')$, donc $r' - r$ est un multiple de b .
Si $r' - r$ était non nul, alors on aurait $|r' - r| \geq |b|$ c'est-à-dire $|r' - r| \geq b$ ce qui est en contradiction avec l'inégalité démontrée précédemment.
On a donc nécessairement $r' - r = 0$ et par conséquent $b(q' - q) = 0$, donc $q' - q = 0$
On obtient alors $r' = r$ et $q' = q$.
Le couple $(q\ ;\ r)$ est donc unique.

Remarques :

- Si $r = 0$, alors

- Le reste d'une division euclidienne par 2 est

- Tout nombre pair s'écrit sous la forme

- Tout nombre impair s'écrit sous la forme

Exemple :
Division euclidienne de 31 par 7 :

Remarque : Division euclidienne de 1715 par 71 avec une calculatrice ou un tableur.

La plupart des calculatrices permettent d'obtenir directement le quotient et le reste d'une division euclidienne.

- **Avec une TI nspire:**

$\text{floor}\left(\frac{1715}{71}\right)$ 24

$\text{remain}(1715,71)$ 11

- **Avec un tableur :**

Le quotient est obtenu par ENT() (partie entière)
Le reste est obtenu par MOD(;)

	A	B	C	D
1			=ENT(A2/B2)	=MOD(A2;B2)
2	1715	71	24	11
3				

Division euclidienne d'un entier relatif :

Soit a un entier relatif et b un entier naturel non nul.
Il existe un unique couple $(q\ ;\ r)$, $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que : $a = bq + r$ et $r < b$
a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.
On dit que le couple unique $(q\ ;\ r)$ est le résultat de la division euclidienne de a par b.

Preuve :
Soit a un entier relatif et b un entier naturel non nul.
Si a est un entier positif ou nul, la propriété a déjà été justifiée.

Considérons un entier a négatif.

- Existence du couple $(q\,;r)$

a étant négatif, on considère son opposé $-a$ qui est un entier naturel.
D'après le résultat démontré sur les entiers naturels,
il existe un unique couple $(q\,;r)$, $q \in \mathbb{N}$ et $r \in \mathbb{N}$ tel que : $-a = bq + r$ et $r < b$
Donc $a = -bq - r = b(-q) - r$.

- Si $r = 0$, alors $-r = 0$ donc $-r \in \mathbb{N}$, et le couple $(-q\,;-r)$ répond à la question
- Si $r \neq 0$, le couple $(-q\,;-r)$ ne répond pas à la question car $-r \in \mathbb{N}$.
  On peut alors écrire $a = b(-q - 1) + b - r$
  On pose $q' = -q - 1$ et $r' = b - r$
  $q' \in \mathbb{Z}$; vérifions que $r' \in \mathbb{N}$.
  b et r étant des entiers, $b - r$ est un entier, donc $b - r \in \mathbb{Z}$.
  De plus $r \neq 0$ et $0 \leq r < b$, donc :
  $$0 < r < b \Rightarrow -b < -r < 0 \Rightarrow b - b < b - r < b \Rightarrow 0 < b - r < b$$
  On a donc $b - r \in$ et $b - r <$ b . Le couple $(-q\text{-}1\,;b - r)$ répond donc à la question.

- Unicité du couple $(q\,;r)$

L'unicité du couple se démontre exactement de le même façon que pour une division euclidienne dans $\mathbb{N}$.

Exemple :
La division euclidienne de -514 par 35 s'écrit :

Remarque :
Dans le cas d'entiers négatifs, les fonctions des calculatrices ne donnent pas toujours les résultats attendus, elles peuvent donner un reste négatif.
Il faudra donc faire preuve de vigilance dans leur utilisation et savoir rétablir le résultat correct.

4) CONGRUENCES

Définition

Soit p un entier naturel et a et b deux entiers relatifs.
On dit que a est congru à b modulo p, si a et b ont le même reste dans la division euclidienne par p.

On note : $a \equiv b\ [p]$ ou
$a \equiv b$ (modulo p) ou $a \equiv b\ (p)$

Remarques :

- $a \equiv b\ [p] \Leftrightarrow$
- $a \equiv 0\ [p]$ si et seulement si
- Si $a \equiv r\ [b]$ et si $0 \leq r < b$, alors

Propriétés

- $a \equiv b\ [p] \Leftrightarrow b - a$ est multiple de p
- Si $a \equiv b\ [p]$ et si $b \equiv c\ [p]$ alors $a \equiv c\ [p]$
- Si $a \equiv b\ [p]$ et si $a' \equiv b'\ [p]$
  alors $a + a' \equiv b + b'\ [p]$; $a - a' \equiv b - b'\ [p]$; $aa' \equiv bb'\ [p]$; $a^n \equiv b^n\ [p]$ $n \in \mathbb{N}^*$
- Si $a \equiv b\ [p]$ alors pour tout $c \in \mathbb{Z}$ $a + c \equiv b + c\ [p]$; $a - c \equiv b - c\ [p]$; $ac \equiv bc\ [p]$

Preuve :

- Supposons que $a \equiv b\ [p]$ alors a et b ont le même reste r dans la division euclidienne par p.
  On peut donc écrire $a = p \times k + r$ et $b = p \times k' + r$ avec $k \in \mathbb{Z}$, $k' \in \mathbb{Z}$, $r \in \mathbb{N}$ et $0 \leq r < p$
  Donc $b - a = p \times k' + r - (p \times k + r) = p \times k' - p \times k = p(k' - k)$
  $k' - k$ étant un entier relatif , on en déduit que $b - a$ est multiple de p.

  Réciproquement, Supposons que $b - a$ est multiple de p, on peut écrire $b - a = k \times p$ avec $k \in \mathbb{Z}$
  Notons q et r le quotient et le reste de la division euclidienne de b par p. On a donc :
  $$b = p \times q + r \Leftrightarrow b - a = p \times q + r - a \Leftrightarrow k \times p = p \times q + r - a \Leftrightarrow a = p \times q + r - kp \Leftrightarrow a = p(q - k) + r$$
  $q - k$ est un entier relatif et r un entier naturel tel que $0 \leq r < p$ (puisque r est le reste de la division euclidienne de b par p)
  On en déduit que r est le reste de la division euclidienne de a par p.
  Donc a et b ont le même reste dans la division euclidienne par p et par conséquent $a \equiv b\ [p]$

- Si $a \equiv b \ [p]$, alors a et b ont le même reste dans la division euclidienne par p.
  Si $b \equiv c \ [p]$, alors b et c ont le même reste dans la division euclidienne par p.
  On en déduit que a et c ont le même reste dans la division euclidienne par p et par conséquent $a \equiv c \ [p]$

- Si $a \equiv b \ [p]$ et si $a' \equiv b' \ [p]$, alors $b - a$ est un multiple de p et $b' - a'$ est un multiple de p.
  On en déduit, d'après les propriétés des multiples que :
  $(b - a) + (b' - a')$ et $(b - a) - (b' - a')$ sont des multiples de p
  C'est-à-dire $(b + b') - (a + a')$ et $(b - b') - (a - a')$ sont des multiples de p
  Donc $a + a' \equiv b + b' \ [p]$ et $a - a' \equiv b - b' \ [p]$

- Puisque $b - a$ est un multiple de p , $a'(b - a)$ est un multiple de p.
  Puisque $b' - a'$ est un multiple de p , $b(b' - a')$ est un multiple de p.
  On en déduit que $a'(b - a) + b(b' - a')$ est un multiple de p.
  C'est-à-dire $a'b - a'a + bb' - ba'$ est un multiple de p.
  On a alors $bb' - aa'$ est un multiple de p , c'est-à-dire $aa' \equiv bb' \ [p]$

- Soit la proposition $P(n)$: « $a^n \equiv b^n \ [p]$ », pour $n \in \mathbb{N}^*$

  Initialistion :
  Pour $n = 1$, on a $a^1 = a$ et $b^1 = b$ et on sait que $a \equiv b \ [p]$ donc P(1) est vraie
  Hérédité :
  Supposons P(n) vraie pour un entier $n \geq 1$ fixé, c'est à dire $a^n \equiv b^n \ [p]$ (HR)
  Montrons que $P(n+1)$ est vraie, c'est à dire $a^{n+1} \equiv b^{n+1} \ [p]$

  La proposition $P(n+1)$ est donc vraie.
  Conclusion :
  Donc $a^n \equiv b^n \ [p]$ pour tout $n \in \mathbb{N}^*$

-

- De même on peut écrire $b - a = (b - c) - (a - c)$.
  Donc $a - c \equiv b - c \ [p]$ pour tout $c \in \mathbb{Z}$
  D'autre part, puisque $b - a$ est un multiple de p , pour tout $c \in \mathbb{Z}$, $c(b - a)$ est un multiple de p,
  c'est-à-dire que $bc - ac$ est un multiple de p donc $ac \equiv bc \ [p]$

<u>Remarque :</u>
La relation de congruence est compatible avec l'addition, la soustraction et la multiplication.

<u>Attention :</u>

La relation de congruence n'est pas compatible avec la division ni avec la racine carrée.

On ne pourra en aucun cas simplifier dans une congruence comme on simplifie dans une égalité:

Entiers et entiers naturels :
$\mathbb{N} \subset \mathbb{Z}$

L'ensemble $\{0;1;2;\ldots\}$ est appelé ensemble des **entiers naturels** . Il est noté $\mathbb{N}$.
L'ensemble $\{\ldots;-3;-2;-1;0;1;2;3;\ldots\}$ est appelé ensemble des **entiers relatifs (ou entiers)** . Il est noté $\mathbb{Z}$.

Propriétés :

Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

Une partie non vide de $\mathbb{Z}$ n'a pas nécessairement de plus petit élément.

- La somme et le produit de deux entiers naturels sont des entiers naturels.
- La somme et le produit de deux entiers relatifs sont des entiers relatifs.

Divisibilité :
Pour indiquer que a divise b, on note $a \mid b$.

Soit a et b deux entiers relatifs .
S'il existe un entier relatif k tel que $b = k \times a$, on dit que b est un **multiple** de a ou que a est un **diviseur** de b .
On dit aussi que b est **divisible** par a et que a **divise** b . (on ne dit jamais que b multiplie a)

Propriétés :

Soit a,b et c trois entiers relatifs

- Si a divise b et si $b \neq 0$, alors $|a| \leq |b|$.
- Tout entier relatif $b \neq 0$ a un nombre fini de diviseurs.
- Si a divise b, alors a divise bc.
- Si a divise b et si a divise c alors a divise toute combinaisons linéaires $bu + cv$ (donc $b+c$ et $b-c$) où u et v sont des entiers relatifs.
- $1, -1, a, -a$ sont des diviseurs de a.
- Si a divise b alors $-a$ divise b , a divise $-b$ et $-a$ divise $-b$.
- Si a divise b et si b divise a , alors $a = b$ ou $a = -b$. (c'est-à-dire que $|a| = |b|$)
- Si a divise b et si b divise c, alors a divise c.
- Si a divise b alors pour tout entier relatif c, ac divise bc.

On peut traduire ces propriétés en termes de multiples . Par exemple : Si b est un multiple de a, alors bc est un multiple de a.

Division euclidienne d'un entier naturel:

Soit a un entier naturel et b un entier naturel non nul.
Il existe un unique couple $(q\,;r)$ d'entiers naturels tel que : $a = bq + r$ et $r < b$.
a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.
On dit que le couple unique $(q\,;r)$ est le résultat de la division euclidienne de a par b.

Remarque :

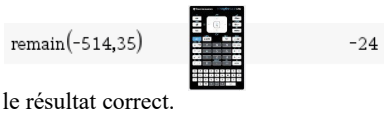
- Si $r = 0$, alors a est divisible par b.
- Le reste d'une division euclidienne par 2 est soit 0 soit 1.
- Tout nombre pair s'écrit sous la forme $2k$ avec $k \in \mathbb{Z}$.
- Tout nombre impair s'écrit sous la forme $2k+1$ avec $k \in \mathbb{Z}$.

Avec une TI-nspire:

Division euclidienne d'un entier :

Soit a un entier relatif et b un entier naturel non nul.
Il existe un unique couple $(q\,;r)$, $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que : $a = bq + r$ et $r < b$

Attention :
Dans le cas d'entiers négatifs, les fonctions des calculatrices ne donnent pas toujours les résultats attendus, elles peuvent donner un reste négatif.
Il faudra donc faire preuve de vigilance dans leur utilisation et savoir rétablir le résultat correct.



Congruence :
On note : $a \equiv b \ [p]$
ou $a \equiv b$ (modulo p)
ou $a \equiv b \ (p)$

Soit p un entier naturel et a et b deux entiers relatifs.
On dit que a est congru à b modulo p, si a et b ont le même reste dans la division euclidienne par p.

Remarque :

- $a \equiv b \ [p] \Leftrightarrow b \equiv a \ [p]$
- $a \equiv 0 \ [p]$ si et seulement si a est divisible par p
- *Si* $a \equiv r \ [b]$ et si $0 \leq r < b$, alors r est le reste de la division euclidienne de a par b

Propriétés :
La relation de congruence est compatible avec l'addition, la soustraction et la multiplication.

- $a \equiv b \ [p] \Leftrightarrow b - a$ est multiple de p
- Si $a \equiv b \ [p]$ et si $b \equiv c \ [p]$ alors $a \equiv c \ [p]$
- Si $a \equiv b \ [p]$ et si $a' \equiv b' \ [p]$ alors
  $a + a' \equiv b + b' \ [p]$; $a - a' \equiv b - b' \ [p]$; $aa' \equiv bb' \ [p]$; $a^n \equiv b^n \ [p]$ $n \in \mathbb{N}^*$
- *Si* $a \equiv b \ [p]$ alors pour tout $c \in \mathbb{Z}$ $a + c \equiv b + c \ [p]$; $a - c \equiv b - c \ [p]$; $ac \equiv bc \ [p]$

Attention :

La relation de congruence n'est pas compatible avec la division ni avec la racine carrée.
Par exemple $44 \equiv 8 \ [6]$, mais on ne peut pas diviser par 4 pour affirmer que 11 est congru à 2 modulo 6.
ou encore $4 \equiv 16 \ [12]$, mais on ne peut pas prendre la racine carrée pour affirmer que 2 est congru à 4 modulo 12
On ne pourra en aucun cas simplifier dans une congruence comme on simplifie dans une égalité:

Une congruence du type $2x \equiv 2y \ [p]$ ne pourra pas être simplifiée par 2

Divisibilité

Ex 6-1 : ***Trouver des multiples***

1) Déterminer le nombre de multiples de 19 compris entre 1000 et 3000.

2) Déterminer le nombre de multiples de 47 compris entre -2000 et 1000.

Ex 6-2 : ***Sommes de nombres pairs et impairs***

1) Montrer que la somme d'un nombre pair et d'un nombre impair est un nombre impair.

2) Montrer que la somme de deux nombres pairs est un nombre pair.

Ex 6-3 : ***Somme de nombres impairs consécutifs***

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

Ex 6-4 : ***Multiple de 3***

Soit a et b deux entiers tels que a est un multiple de 9 et b est un multiple de 15.

Montrer que $a+b$ est un multiple de 3.

Ex 6-5 :

Soit a et b deux entiers.

1) Montrer que si a est un diviseur de $a+b$, alors a est un diviseur de b .

2) Montrer que si a est un diviseur de b , alors a^2 est un diviseur de b^2 .

Ex 6-6 :

Existe-t-il un entier naturel multiple de 14 et diviseur de 100 ?

Ex 6-7 :

Montrer que si 13 est un diviseur de a, alors 13 est un diviseur de a^2.

Ex 6-8 :

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

Ex 6-9 :

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

Ex 6-10 : Vrai ou faux

Justifier ou donner un contre-exemple.

1) Si un entier a divise un entier b et un entier c, alors a^2 divise bc.

2) Si le carré d' un entier a divise un entier b, alors a divise $\sqrt{b}$.

3) Si un entier m, divise un entier a, il existe alors un entier n tel que $a=m\times n$. Ainsi, un entier naturel a a toujours un nombre pair de diviseurs positifs.

Ex 6-11 : $\overline{aaaaaa}$

On note $\overline{aaaaaa}$ le nombre formé de 6 chiffres a.

1) Montrer que pour tout chiffre a, $\overline{aaaa}$ est divisible par 101.

2) Montrer que pour tout chiffre a et b, $\overline{aaabbb}$ est divisible par 37.

Ex 6-12 : ***Montrer une divisibilité en utilisant la récurrence***

Montrer que pour tout entier naturel n, $10^n-(-1)^n$ est un multiple de 11.

Divisibilité et équation dans les entiers

Ex 6-13 :

Résoudre dans $\mathbb{Z}^2$ l'équation $x^2=y^2+17$ (E).

Ex 6-14 :

Résoudre dans $\mathbb{Z}^2$ l'équation $3xy-y^2=25$

Ex 6-15 :

Résoudre dans $\mathbb{Z}^2$ l'équation $3x+24y=17$

Division euclidienne

Ex 6-16 :

1) Effectuer la division euclidienne de $a=1257$ par $b=13$.

2) En déduire la division euclidienne de 1257 par 32.

3) En déduire la division euclidienne de -1257 par 96

Ex 6-17 : QCM

Cocher la (ou les) bonne(s) réponse(s)
Le reste de la division d'un entier par 4 peut être :

a) 5 b) 1 c) -2 d) 2,5 e) 4

Ex 6-18 :

1) Soit $a=4k+5$ ($k\in\mathbb{N}^*$).
Quel est le reste de la division euclidienne de a par 4 ?

2) On sait que le reste de la division euclidienne d'un entier naturel b par 5 est 3 . Comment peut-on écrire b ?

Ex 6-19 :

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

Ex 6-20 :

Soit a et b deux entiers naturels.
Dans la division euclidienne de a par 11, le reste est 8.
Dans la division euclidienne de b par 11, le reste est 3.
Donner le reste de la division euclidienne de :

1) $a+b$ par 11

2) a^2 par 11

Ex 6-21 :

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

Ex 6-22 : ***Division euclidienne de a(n) par b(n)***

Soit un entier naturel n .
Déterminer suivant les valeurs de n , le reste de la division euclidienne de $9n+17$ par $2n+3$.

Ex 6-23 : ***Partitionnement des entiers naturels***

1) Quelles sont les valeurs possibles du reste de la division euclidienne d'un entier naturel par 3 ?

2) Justifier que tout entier a peut s'écrire sous l'une des formes suivantes : $3k$, $3k+1$ ou $3k+2$ (où $k\in\mathbb{N}$)

3) Montrer que tout entier peut s'écrire sous l'un des formes suivantes : $4k$, $4k+1$, $4k+2$ ou $4k+3$ (où $k\in\mathbb{N}$)

4) Montrer que le produit de 4 entiers consécutifs est divisible par 4.

5) Que peut-on dire du produit de n ($n \in \mathbb{N}^*$)entiers consécutifs ?

Congruences

Ex 6-24 : ***Simplifier des congruences***

Pour chaque valeur de a , trouver un entier b tel que :

$$b \equiv a[5] \text{ et } -2 \leqslant b \leqslant 2$$

1) $a=11$

2) $a=29$

3) $a=-12$

4) $a=-105$

Ex 6-25 : ***Produit nul et congruence***

Soit a , b et n trois entiers naturels tels que $a \equiv b[n]$.

1) Montrer que si $a \equiv 0[n]$, alors $a \times b \equiv 0[n]$

2) Montrer que $4 \times 9 \equiv 0[6]$

3) Peut-on dire que si $a \times b \equiv 0[n]$, alors $a \equiv 0[n]$ ou $b \equiv 0[n]$?

Ex 6-26 : ***Calculer un reste avec des congruences***

Déterminer le reste dans la division euclidienne par 7 de :

1) $841^{120} \times 99^{35}$

2) $100^{85} - 44^{85}$

Ex 6-27 : ***Calculer un reste avec des congruences***

Montrer sans calcul, ni calculatrice que :

1) $17^{51} - 3^{51} \equiv 0[14]$

2) $13^{30} - 9^{30} \equiv 0[11]$

Ex 6-28 : ***Calculer un reste avec des congruences***

Soit a et b deux entiers tels que $a \equiv 3[5]$ et $b \equiv 4[5]$
Déterminer le reste de la division euclidienne de $11a^2 + 3b^2$ par 5.

Ex 6-29 : ***Calculer un reste avec des congruences***

1) Déterminer le reste de la division euclidienne de 2017^{2431} par 5.

2) Déterminer le reste de la division euclidienne de 2110^{2011} par 7.

Ex 6-30 : ***Utiliser un tableau de congruences***

En complétant le tableau ci-dessous, déterminer les différents restes possibles de la division euclidienne de x^4 par 5.

$x[5]$	-2	-1	0	1	2
$x^2[5]$					
$x^4[5]$					

Ex 6-31 : ***Résoudre dans $\mathbb{Z}$ une équation module n***

Résoudre dans $\mathbb{Z}$:

1) $\begin{cases} x \equiv 4[7] \\ 0 < x < 30 \end{cases}$

2) $7x \equiv 3[11]$

3) $5x \equiv 3[10]$

4) $5x \equiv 5[10]$

5) $5x + 24 \equiv 55[7]$

6) $9x - 24 \equiv 6x - 46[17]$

Ex 6-32 : ***Résoudre une équation avec les congruences***

On considère dans $\mathbb{Z}^2$: $3x^2 - 5y^2 = 16$ (E)

1) Montrer que si un couple $(x, y) \in \mathbb{Z}^2$ est solution de l'équation (E), alors $3x^2 \equiv 1[5]$.

2) Déterminer les restes de la division de $3x^2$ par 5 et conclure.

Ex 6-33 :

Montrer que pour tout entier $n \geqslant 1$, le nombre $N = 3 \times 5^{2n-1} + 2^{3n-2}$ est un multiple de 17

Ex 6-34:

Soit $n \in \mathbb{Z}$ et $N = n^3 - 3n + 5$

1) Déterminer les entiers n tels que $N \equiv 0 [7]$

2) Déterminer les entiers n tels que $N \equiv 1 [7]$

Ex 6-35 :

Déterminer suivant les valeurs de l'entier naturel n , le reste de la division euclidienne de 2^n par 5.

En déduire le reste de la division euclidienne de 2^{227505} par 5.

Ex 6-36 :

Montrer que $N = n(2n+1)(7n+1)$ est divisible par 6 pour tout entier naturel $n \neq 0$.

Ex 6-37 : ***Baccalauréat S nouvelle Calédonie mars 2016 – ex 4***

Congruences – cryptographie – suites

Les parties A et B peuvent être traitées de manière indépendante

Partie A

Afin de crypter un message, on utilise un chiffrement affine.
Chaque lettre de l'alphabet est associée à un nombre entier comme indiqué dans le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Soit x le nombre associé à la lettre à coder. On détermine le reste y de la division euclidienne de $7x + 5$ par 26, puis on en déduit la lettre associée à y (c'est elle qui code la lettre d'origine).
Exemple :
M correspond à $x = 12$
$7 \times 12 + 5 = 89$
Or $89 \equiv 11$ [26] et 11 correspond à la lettre L, donc la lettre M est codée par la lettre L.

1. Coder la lettre L.
2. a. Soit k un entier relatif. Montrer que si $k \equiv 7x$ [26] alors $15k \equiv x$ [26].
   b. Démontrer la réciproque de l'implication précédente.
   c. En déduire que $y \equiv 7x + 5$ [26] équivaut à $x \equiv 15y + 3$ [26].
3. À l'aide de la question précédente décoder la lettre F.

Partie B

On considère les suites (a_n) et (b_n) telles que a_0 et b_0 sont des entiers compris entre 0 et 25 inclus et pour tout entier naturel n, $a_{n+1} = 7a_n + 5$ et $b_{n+1} = 15b_n + 3$.
Montrer que pour tout entier naturel n, $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$.
On admet pour la suite du problème que pour tout entier naturel n,
$b_n = \left(b_0 + \frac{3}{14}\right) \times 15^n - \frac{3}{14}$.

Partie C

Déchiffrer un message codé avec un chiffrement affine ne pose pas de difficulté (on peut tester les 312 couples de coefficients possibles). Afin d'augmenter cette difficulté de décryptage, on propose d'utiliser une clé qui indiquera pour chaque lettre le nombre de fois où on lui applique le chiffrement affine de la partie A. Par exemple pour coder le mot MATH avec la clé 2-2-5-6, on applique « 2 » fois le chiffrement affine à la lettre M (cela donne E), « 2 » fois le chiffrement à la lettre A, « 5 » fois le chiffrement à la lettre T et enfin « 6 » fois le chiffrement à la lettre H.
Dans cette partie, on utilisera la clé 2-2-5-6.
Décoder la lettre Q dans le mot IYYQ.

Ex 6-38 : ***Baccalauréat S Polynésie 14 juin 2017 – ex 4***

Congruences – cryptographie

Les parties A et B sont indépendantes.

Une personne a mis au point le procédé de cryptage suivant :

— À chaque lettre de l'alphabet, on associe un entier n comme indiqué ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

— On choisit deux entiers a et b compris entre 0 et 25.

— Tout nombre entier n compris entre 0 et 25 est codé par le reste de la division euclidienne de $an+b$ par 26.

Le tableau suivant donne les fréquences f en pourcentage des lettres utilisées dans un texte écrit en français.

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Fréquence	9,42	1,02	2,64	3,38	15,87	0,94	1,04	0,77	8?41	0,89	0,00	5,33	3,23

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Fréquence	7,14	5,13	2,86	1,06	6,46	7,90	7,26	6,24	2,15	0,00	0,30	0,24	0,32

Partie A

Un texte écrit en français et suffisamment long a été codé selon ce procédé. L'analyse fréquentielle du texte codé a montré qu'il contient 15,9 % de O et 9,4 % de E.

On souhaite déterminer les nombres a et b qui ont permis le codage.

1. Quelles lettres ont été codées par les lettres O et E?
2. Montrer que les entiers a et b sont solutions du système

$$\begin{cases} 4a+b \equiv 14\ [26] \\ b \equiv 4\ [26]. \end{cases}$$

3. Déterminer tous les couples d'entiers $(a\ ,\ b)$ ayant pu permettre le codage de ce texte.

Partie B

1. On choisit $a=22$ et $b=4$.
   a. Coder les lettres K et X.
   b. Ce codage est-il envisageable?
2. On choisit $a=9$ et $b=4$.
   a. Montrer que pour tous entiers naturels n et m, on a :

$$m \equiv 9n+4\ [26] \iff n \equiv 3m+14\ [26]$$

h) Décoder le mot AQ.

PGCD – NOMBRES PREMIERS ENTRE EUX

1) PLUS GRAND COMMUN DIVISEUR : PGCD

A) DÉFINITION - PROPRIÉTÉS

Propriété – Définition :

Soit a et b deux entiers naturels non nuls.
Un entier naturel qui divise a et qui divise b est appelé **diviseur commun** à a et b.
L'ensemble des diviseurs communs à a et à b possède un plus grand élément que l'on appelle **le plus grand commun diviseur** de a et b, on le note PGCD(a ; b).

Preuve :

Soit a et b deux entiers naturels non nuls . Considérons l'ensemble D(a ; b), ensemble des diviseurs communs à a et b.
Le nombre 1 est un diviseur commun à a et b .
D(a ; b) est donc une partie non vide de $\mathbb{N}$.
De plus on sait que tout diviseur commun à a et b sera inférieur ou égal à a et à b.
Donc D(a ; b) est une partie finie de $\mathbb{N}$.
D(a ; b) a donc un plus grand élément que l'on peut obtenir en rangeant dans l'ordre croissant (ou décroissant) les éléments de D(a ; b).
C'est ce plus grand élément de D(a ; b) qui est noté PGCD(a ; b)

Exemples :

Dans $\mathbb{N}$ l'ensemble des diviseurs de 15 est et l'ensemble des diviseurs de 12 est

L'ensemble des diviseurs communs à 12 et à 15 est donc

Remarque :

a étant un entier naturel, l'ensemble des diviseurs de a est égal à l'ensemble des diviseurs de $-a$.
On pourra étendre, si besoin est, la notion de PGCD à des nombres entiers relatifs.

On dira par exemple que

Propriétés :

Soit a et b deux entiers naturels non nuls.

- PGCD(a ; b) $\leq$ a
- PGCD(a ; b) $\leq b$
- PGCD(a ; b) = PGCD(b ; a)
- Si b divise a, on a PGCD(a ; b) = b
- PGCD (a ; 1) = 1
- PGCD (a ; a) = a

Preuve :

- a étant un entier naturel, on sait que tous les diviseurs de a sont inférieurs ou égaux à a.
  PGCD(a ; b) est un diviseur de a, donc PGCD(a ; b) $\leq a$
- On montre de même que PGCD(a ; b) $\leq$ b
- Il est immédiat que les diviseurs communs à a et b, sont aussi les diviseurs communs à b et a . Donc PGCD(a ; b) = PGCD(b ; a)
- Si b divise a, alors b est un diviseur de a . Mais b est aussi un diviseur de b
  Donc b est un diviseur commun à a et b.
  PGCD(a ; b) étant le plus grand des diviseurs communs à a et b, on a donc PGCD(a ; b) $\geq b$.
  Or on a vu précédemment que PGCD(a ; b) $\leq b$
  On en déduit : PGCD(a ; b) = b
- En prenant $b = 1$, et comme 1 divise a, on a PGCD(a ; 1) = 1 (résultat qui est par ailleurs évident)
- En prenant $b = a$, et comme a divise a, on a PGCD(a ; a) = a (résultat qui est par ailleurs évident)

Exemple :

6 est un diviseur de 18 donc

B) ALGORITHME D'EUCLIDE

Propriété : Lemme d'Euclide

Soit a et b deux entiers naturels non nuls.
Soit q et r le quotient et le reste de la division euclidienne de a par b.

- Si $r = 0$, PGCD(a ; b) = b
- Si $r \neq 0$, PGCD(a ; b) = PGCD(b ; r)

Preuve :

a et b sont deux entiers naturels non nuls . q et r sont le quotient et le reste de la division euclidienne de a par b.
On a alors $a = b \times q + r$ avec $q \in \mathbb{N}$, $r \in \mathbb{N}$ et $0 \leq r < b$

- Si $r = 0$, alors $a = b \times q$ avec $q \in \mathbb{N}$, donc b divise a et par conséquent PGCD(a ; b) = b

- Si $r \neq 0$,
  - Considérons d un diviseur commun à a et b. On peut écrire $r = a - b \times q$
    Comme d divise a et b, on en déduit que d divise r.
    Donc d est un diviseur commun à b et r. On a donc $D(a ; b) \subset D(b ; r)$
  - Considérons d un diviseur commun à b et r.
    On sait que $a = b \times q + r$
    Comme d divise b et r, on en déduit que d divise a
    Donc d est un diviseur commun à a et b. On a donc $D(b ; r) \subset D(a ; b)$

  On a donc démontré que $D(a ; b) = D(b ; r)$
  Le plus grand élément de $D(a ; b)$ est donc aussi le plus grand élément de $D(b ; r)$, c'est-à-dire $PGCD(a ; b) = PGCD(b ; r)$

Exemple :

Pour trouver le PGCD de 2414 et 804, on peut écrire la division euclidienne de 2414 par 804 :

On en déduit alors PGCD(2414 ; 804) =

Il est immédiat que

Propriété : Algorithme d'Euclide

Soit a et b deux entiers naturels non nuls.
On définit la suite r_n d'entiers naturels de la façon suivante :

$r_0 = b$; r_1 est le reste de la division euclidienne de a par b

Pour $n \geq 1$:
- si $r_n = 0$ alors $r_{n+1} = 0$
- si $r_n \neq 0$ alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n

Alors il existe un entier n_0 tel que $r_{n_0} \neq 0$ et pour tout $n > n_0$, $r_n = 0$

On a $PGCD(a ; b) = r_{n_0}$

Preuve :

Soit a et b deux entiers naturels non nuls.
Supposons que pour tout entier n, on a $r_n \neq 0$
Alors pour tout entier n, r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n
D'après l'encadrement du reste dans une division euclidienne on a $r_{n+1} < r_n$
On a alors : $r_1 < r_0 \Rightarrow r_1 < b \Rightarrow r_1 \leq b - 1$ et $r_2 < r_1 \Rightarrow r_2 \leq r_1 - 1 \Rightarrow r_2 \leq b - 2$
On pourrait alors démontrer par récurrence que, pour tout n, $r_n \leq b - n$
On aurait alors $r_{b+1} \leq b - (b + 1)$ c'est-à-dire $r_{b+1} \leq -1$ ce qui est absurde puisque $r_{b+1} \in \mathbb{N}$
Il existe donc un entier n tel que $r_n = 0$
Considérons l'ensemble E des entiers n tels que $r_n = 0$
Cet ensemble est une partie non vide de $\mathbb{N}$. Elle a donc un plus petit élément n_1.
On a donc $r_{n_1} = 0$ et d'après la définition de la suite (r_n) il est immédiat que $r_n = 0$ pour tout $n \geq n_1$
Posons $n_0 = n_1 - 1$
Puisque n_1 est le plus petit élément de E, $n_0 \notin E$ donc $r_{n_0} \neq 0$
De plus si $n > n_0$ on a $n \geq n_1$ et par conséquent $r_n = 0$. On en déduit que $r_n = 0$ pour tout n tel que $n > n_0$
On a vu que lorsque r est le reste non nul de la division euclidienne de a par b, on a $PGCD(a ; b) = PGCD(b ; r)$
En utilisant cette propriété avec les éléments de la suite (r_n) pour $n \leq n_0$ on peut écrire :

$PGCD(a ; b) = PGCD(a ; r_0) = PGCD(r_0 ; r_1) = PGCD(r_1 ; r_2) = ... = PGCD(r_{n_0-1} ; r_{n_0})$

Comme de plus $r_{n_0+1} = r_{n_1} = 0$, cela signifie que r_{n_0-1} est divisible par r_{n_0} et donc $PGCD(r_{n_0-1} ; r_{n_0}) = r_{n_0}$

On a alors obtenu $PGCD(a ; b) = r_{n_0}$

Remarque :

En effectuant ainsi des divisions euclidiennes successives : de a par b, puis du diviseur par le reste, … le premier reste non nul est le PGCD de a et de b. C'est l'algorithme d'Euclide . Suivant les nombres a et b, le nombre d'itérations à effectuer peut être plus ou moins grand.
Sachant que $PGCD(a ; b) = PGCD(b ; a)$ on aura toujours intérêt à prendre $b \leq a$

Exemple :

Pour déterminer le PGCD de 410258 et de 126 écrivons les divisions euclidiennes successives :

Pour déterminer le PGCD de 15648 et de 657 écrivons les divisions euclidiennes successives :

C) CONSÉQUENCES DE L'ALGORITHME D'EUCLIDE

Propriété :

Soit a et b deux entiers naturels non nuls.
L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de leur PGCD.

Preuve :

a et b sont deux entiers naturels non nuls . On note D = PGCD(a ; b)

- Soit d un diviseur de D.
  d divise D et D divise a, donc d divise a
  d divise D et D divise b, donc d divise b.
  Donc d est un diviseur commun à a et b.
  On en déduit que tout diviseur du PGCD est un diviseur commun à a et b.

- Soit d un diviseur commun à a et b. (on peut supposer que $b \leq a$)
  - Si b divise a, alors PGCD(a ; b) = b, donc D = b, donc d divise D
  - Si b ne divise pas a.
    Écrivons la division euclidienne de a par b, $a = b \times q + r$ avec $0 < r < b$
    On a D = PGCD(a ; b) = PGCD(b ; r)
    - Si r divise b, alors D = PGCD(b ; r) = r,
      D'autre part puisque d divise a et b, alors d divise $r = a - b \times q$, donc d divise D

      - Si r ne divise pas b, on peut alors recommencer l'opération.
      Or, d'après l'algorithme d'Euclide, on obtiendra D = PGCD(r_{n-1} ; r_n)
      avec r_n le dernier reste non nul, c'est-à-dire avec r_n diviseur de r_{n-1} . Donc D = r_n
      A chaque étape on pourra écrire que d divise r_i et par conséquent d divise r_n .
      On aura donc démontré que d divise D.

  On en déduit que tout diviseur commun à a et b est un diviseur de leur PGCD.

  L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de leur PGCD.

Propriété : Homogénéité

Soit a , b et k trois entiers naturels non nuls.

$$\text{PGCD}(ka ; kb) = k\,\text{PGCD}(a ; b)$$

Preuve :

Si $a = b\,q + r$ avec $0 \leq r < b$, alors $ka = k\,b\,q + kr$ avec $0 \leq kr < kb$ (car $k \in \mathbb{N}$)
Donc kr est le reste de la division de ka par kb d'après l'unicité de l'écriture.
En utilisant les notations de l'algorithme d'Euclide et multipliant chaque membres des égalités par k, on obtient :

$$\text{PGCD}(ka ; kb) = \text{PGCD}(kb ; kr_0) = \ldots = k\,r_n = k\,\text{PGCD}(a ; b)$$

2) NOMBRES PREMIERS ENTRE EUX

Exemple :

On voudrait savoir s'il est possible de simplifier la fraction $\frac{1223}{717}$.
Pour cela on peut déterminer le PGCD de 1223 et 717. On trouve PGCD(1223 ; 717) = 1.
Par conséquent les nombres 1223 et 717 n'ont pas de diviseur commun autre que 1 (et -1).
On dit que ces deux nombres sont **premiers entre eux**.
La fraction ne peut pas être simplifiée. On dit que c'est une fraction **irréductible**.

Définition :

Soit a et b deux entiers relatifs non nuls.
On dit que a et b sont **premiers entre eux** si leur PGCD est égal à 1.

Remarques :

- Deux nombres sont donc premiers entre eux s'ils n'ont d'autres diviseurs communs que
- On dit aussi que a est premier avec b, ou que b est premier avec a.
- On dit aussi parfois que a et b sont **étrangers**.

Rappel :

On dit qu'un entier naturel non nul p est premier si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

Propriété :

Soit a un entier relatif non nul.
Si p est un nombre premier qui ne divise pas a, alors PGCD(a ; p) = 1, c'est-à-dire que a et p sont premiers entre eux.
(Si p est un nombre premier, p est premier avec tout entier qui n'est pas un de ses multiples)

Preuve :

p est un nombre premier, donc dans $\mathbb{N}$ l'ensemble des diviseurs de p est $\{1 ; p\}$.

Puisque p ne divise pas a, p n'appartient pas à l'ensemble des diviseurs de a.

Donc dans $\mathbb{N}$, le seul diviseur commun à p et a est 1 et PGCD(a ; p) = 1 .

Exemple :

Démontrons que la fraction $\frac{18866}{13}$ est irréductible.

Propriété :

Soit a et b des entiers relatifs non nuls.
Si D = PGCD(a ; b), alors $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
(il existe a' et b' deux entiers relatifs non nuls premiers entre eux tels que $a = Da'$ et $b = Db'$)

Preuve :

D = PGCD(a ; b) alors D divise a et D divise b.
On en déduit qu'il existe a' et b' deux entiers relatifs non nuls tels que $a = Da'$ et $b = Db'$.
Donc $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls.
Soit $d \in \mathbb{N}$ un diviseur commun à $\frac{a}{D}$ et $\frac{b}{D}$, alors

3) THÉORÈME DE BÉZOUT

Théorème de Bézout :

Soit a et b 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 $au + bv = 1$.

Preuve :

- Supposons qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$.

- Supposons que a et b sont premiers entre eux.
  Considérons l'ensemble E des entiers naturels non nuls de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.
  E n'est pas vide (E contient a ou $-a$, E contient b ou $-b$, E contient $2a + 3b$ ou $-2a - 3b$ ...), donc E a un plus petit élément m.
  On peut écrire $m = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.
  Écrivons la division euclidienne de a par m : $a = mq + r$ avec $r \in \mathbb{N}$ et $0 \leq r < m$.
  On a alors : $a = (au_1 + bv_1)\, q + r \Rightarrow r = a - (au_1 + bv_1)q \Rightarrow r = a\,(1 - u_1\, q) + b\,(-v_1\, q)$
  Donc r est un entier naturel de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ et d'autre part $r < m$.
  Comme m est le plus petit élément de E, on en déduit que $r = 0$, c'est-à-dire que a est divisible par m.

  De même on démontrerait que b est divisible par m.
  Donc m est un diviseur commun à a et b.
  Comme a et b sont premiers entre eux, on en déduit que $m = 1$.
  On a donc $1 = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.

Remarque : Le théorème de Bézout est particulièrement intéressant pour travailler sur des expressions littérales ou sur des grands nombres.

Exemple :

En utilisant l'algorithme d'Euclide démontrons que 383 et 127 sont premiers entre eux et déterminons des entiers relatifs u et v tels que $383u + 127v = 1$

	Pour déterminer u et v, l'idée est d'exprimer le 1 qui apparaît comme reste de la dernière division en fonction des nombres 383 et 127.
On peut écrire $383 = 127 \times 3 + 2$ (1) et $127 = 2 \times 63 + 1$ (2) Donc PGCD(383 ; 127) = 1 c'est-à-dire que 383 et 127 sont premiers entre eux.	D'après l'égalité (1), on peut écrire D'après l'égalité (2), on peut écrire En remplaçant 2 par $383 - 127 \times 3$ dans l'égalité (3), on obtient :

On peut donc prendre $u = -63$ et $v = 190$.

Le couple $(u ; v)$ d'entiers relatifs n'est pas unique, on peut vérifier que les couples (64 ; -293) et (-317 ; 956) répondent aussi à la question.

Propriété :

Soit a , b des entiers relatifs non nuls et D un entier naturel non nul . Les propositions si-dessous sont équivalentes :

- $D = PGCD(a ; b)$
- $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
- $a = Da'$ et $b = Db'$ a' et b' étant deux entiers relatifs non nuls premiers entre eux.

Preuve :

Soit a , b des entiers relatifs non nuls et D un entier naturel non nul.

- On a déjà vu que si $D = PGCD(a ; b)$, alors $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
- Supposons que $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
  Puisque $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers, D divise a et D divise b .
  Soit $g = PGCD(a ; b)$.
  D divise a et b, donc D divise g et donc $D \leq g$.
  D'autre part $\frac{a}{D}$ et $\frac{b}{D}$ sont premiers entre eux, donc il existe des entiers relatifs u et v tels que $\frac{a}{D}u + \frac{b}{D}v = 1$, c'est-à-dire $D = au + bv$.
  Mais g étant le PGCD de a et de b, g divise a et b , donc g divise $au + bv$ donc g divise D, donc $g \leq D$.
  On a donc finalement $g = D$, c'est-à-dire $D = PGCD(a ; b)$

  On a donc démontré l'équivalence des deux premières propositions.
- L'équivalence des deux dernières propositions est immédiate.

Théorème de Bézout généralisé : Caractérisation du PGCD

Soit a , b des entiers relatifs non nuls et D un entier naturel non nul .
$D = PGCD(a ; b)$ si et seulement si D divise a et b et s'il existe deux entiers relatifs u et v tels que $au + bv = D$.

Preuve : exigible

-

-

Remarque :

La condition D divise a et b est importante . Par exemple $7=4\times1+3\times1$, mais 7 n'est pas le PGCD de 4 et 3

4) THÉORÈME DE GAUSS

Théorème de Gauss :

Soit a et b deux entiers relatifs non nuls et c un entier relatif.
Si a divise bc et si a est premier avec b, alors a divise c.

Preuve : **exigible**

Soit a et b deux entiers relatifs non nuls et c un entier relatif tels que a divise bc et a est premier avec b.
a et b sont premiers entre eux, il existe donc des entiers relatifs u et v tels que $au + bv = 1$.

Propriété : (parfois appelé théorème d'Euclide)

Soit a et b deux entiers relatifs et p un nombre premier.
Si p divise le produit ab, alors p divise a ou p divise b.

Preuve :

Soit a et b deux entiers relatifs. On suppose que p est un nombre premier divisant le produit ab.

Supposons que p ne divise pas a, alors $a \neq 0$ et a et p sont premiers entre eux (puisque p est premier)

Donc p divise ab et p est premier avec a, donc p divise b. (Théorème de Gauss)

Propriété :

Soit a et b deux entiers relatifs non nuls premiers entre eux et soit n un entier naturel.
Si n est divisible par a et par b, alors n est divisible par le produit ab.

Preuve :

Soit a et b deux entiers relatifs non nuls premiers entre eux, et n un entier naturel tel que n est divisible par a et par b.

a et b sont premiers entre eux, il existe donc des entiers relatifs u et v tels que

On a alors

On sait que a divise n, donc $n = aq$ avec $q \in \mathbb{Z}$ et b divise n, donc $n = bq'$ avec $q' \in \mathbb{Z}$.

L'égalité $nau + nbv = n$ peut alors s'écrire

Alors ab divise ab divise donc ab divise c'est-à-dire ab divise

Exemple :

Si un nombre est divisible par 5 et par 6, alors

PGCD :

a étant un entier naturel, l'ensemble des diviseurs de a est égal à l'ensemble des diviseurs de $-a$.
On pourra étendre, si besoin est, la notion de PGCD à des nombres entiers relatifs. On dira par exemple :
PGCD(-15 ; 12) = PGCD(15 ; 12) = 3

Soit a et b deux entiers naturels non nuls.
Un entier naturel qui divise a et qui divise b est appelé **diviseur commun** à a et b.
L'ensemble des diviseurs communs à a et à b possède un plus grand élément que l'on appelle **le plus grand commun diviseur** de a et b,on le note **PGCD(a ; b)**.

Propriétés :

- PGCD(a ; b) $\leq a$
- PGCD(a ; b) $\leq b$
- PGCD(a ; b) = PGCD(b ; a)
- Si b divise a, on a PGCD(a ; b) = b
- PGCD (a ; 1) = 1
- PGCD (a ; a) = a

Lemme d'Euclide :

Soit a et b deux entiers naturels non nuls.
Soit q et r le quotient et le reste de la division euclidienne de a par b.

- Si $r = 0$, PGCD(a ; b) = b
- *Si $r \neq 0$,* PGCD(a ; b) = PGCD(b ; r)

Algorithme d'Euclide :

En effectuant des divisions euclidiennes successives : de a par b, puis du diviseur par le reste, … le premier reste non nul est le PGCD de a et de b.

Pour déterminer le PGCD de 410258 et de 126 écrivons les divisions euclidiennes successives :
$410258 = 126 \times 3256 + 2$
$126 = 2 \times 63 + 0$

Donc PGCD(410258 ; 126) = 2

Pour déterminer le PGCD de 15648 et de 657 écrivons les divisions euclidiennes successives :
$15648 = 657 \times 23 + 537$
$657 = 537 \times 1 + 120$
$537 = 120 \times 4 + 57$
$120 = 57 \times 2 + 6$
$57 = 6 \times 9 + 3$
$6 = 3 \times 2 + 0$

Donc PGCD(15648 ; 657) = 3

Ensemble des diviseurs :

Soit a et b deux entiers naturels non nuls.
L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de leur PGCD.

Homogénéité :

Soit a , b et k trois entiers naturels non nuls.

$$\text{PGCD}(ka ; kb) = k\,\text{PGCD}(a ; b)$$

Nombres premiers entre eux :

Soit a et b deux entiers relatifs non nuls.
On dit que a et b sont **premiers entre eux** si leur PGCD est égal à 1.
On dit aussi que a est premier avec b, ou que b est premier avec a, ou que a et b sont étrangers.

Deux nombres sont donc premiers entre eux s'ils n'ont d'autres diviseurs communs que 1 et -1.

Propriété :

Si p est un nombre premier, p est premier avec tout entier qui n'est pas un de ses multiples

Soit a un entier relatif non nul. Si p est un nombre premier qui ne divise pas a, alors PGCD(a ; p) = 1, c'est-à-dire que a et p sont premiers entre eux.

Propriété :

Si D = PGCD(a ; b), alors $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
(il existe a' et b' deux entiers relatifs non nuls premiers entre eux tels que $a = Da'$ et $b = Db'$)

Théorème de Bézout :

Soit a et b 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 $au + bv = 1$.

Comment déterminer u et v ?

En utilisant l'algorithme d'Euclide démontrons que 383 et 127 sont premiers entre eux et déterminons des entiers relatifs u et v tels que $383u + 127v = 1$

On peut donc prendre $u = -63$ et $v = 190$. Le couple (u ; v) d'entiers relatifs n'est pas unique, on peut vérifier que les couples (64 ; -293) et (-317 ; 956) répondent aussi à la question.

	Pour déterminer u et v, l'idée est d'exprimer le 1 qui apparaît comme reste de la dernière division en fonction des nombres 383 et 127.
On peut écrire $383 = 127 \times 3 + 2$ (1) et $127 = 2 \times 63 + 1$ (2) Donc PGCD(383 ; 127) = 1 c'est-à-dire que 383 et 127 sont premiers entre eux.	D'après l'égalité (1), on peut écrire $2 = 383 - 127 \times 3$ D'après l'égalité (2), on peut écrire $1 = 127 - 2 \times 63$ (3) En remplaçant 2 par 383 - 127 × 3 dans l'égalité (3), on obtient : $1 = 127 - [383 - 127 \times 3] \times 63$ $= 127 - 383 \times 63 + 127 \times 3 \times 63$ $= 127(1 + 3 \times 63) - 383 \times 63$ $= 383 \times (-63) + 127 \times (190)$

Théorème de Bézout généralisé : Caractérisation du PGCD

D = PGCD(a ; b) si et seulement si D divise a et b et s'il existe deux entiers relatifs u et v tels que $au + bv = D$.

La condition D divise a et b est importante . Par exemple $7 = 4 \times 1 + 3 \times 1$, mais 7 n'est pas le PGCD de 4 et 3

Théorème de Gauss :

Soit a et b deux entiers relatifs non nuls et c un entier relatif.
Si a divise bc et si a est premier avec b, alors a divise c.

Propriété : (Théorème d'Euclide)

Soit a et b deux entiers relatifs et p un nombre premier.
Si p divise le produit ab, alors p divise a ou p divise b.

Propriété :

Soit a et b deux entiers relatifs non nuls premiers entre eux et soit n un entier naturel.
Si n est divisible par a et par b, alors n est divisible par le produit ab.

PGCD

Ex 7-1 :

1) Déterminer l'ensemble $D(54)$ des diviseurs positifs de 54 et $D(270)$ l'ensemble des diviseurs positifs de 270.

2) En déduire l'ensemble des diviseurs communs de 54 et 270, puis le PGCD de 54 et 270

Ex 7-2 :

1) Vérifier que $5\times181-8\times113=1$

2) En déduire l'ensemble des diviseurs communs de 181et 113, puis le PGCD de 1181 et 113.

Ex 7-3 : PCDG(*a ;b*)=PGCD*(a-c ;b-c)* ?

Soit a , b et c trois entiers.
La proposition $\text{PGCD}(a;b)=\text{PGCD}(a-c;b-c)$ est-elle vraie ? Justifier.

Ex 7-4 :

Soit n un entier naturel et les entiers $a=n+2$ et $b=3n+1$.

1) Montrer que si d divise a et b , alors d divise 5.

2) En déduire les valeurs possibles du PGCD de a et b .

Ex 7-5 :

Déterminer les entiers naturels non nuls a tels que :

$\text{PGCD}(261;a)=87$ et $a<261$

Utiliser PGCD(*a*;*b*)=PGCD(*a-kb*;*b*)

Ex 7-6 :

Montrer que PGCD(1671;1669)=1.

Ex 7-7 :

Montrer que deux entiers consécutifs sont premiers entre eux.

Ex 7-8 : PGCD *de a(n) et b(n)*

Soit n un entier naturel . Déterminer suivant les valeurs de n les valeurs de :

1) $\text{PGCD}(n;3n+17)$

2) $\text{PGCD}(5n+4;3n-1)$

3) $\text{PGCD}(2n+15\,;n+3)$

Ex 7-9 : ***Montrer l'égalité de deux* PGCD**

Soit a et b deux entiers naturels non nuls.
On pose $A=5a+9b$ et $B=4a+7b$

Montrer que $\text{PGCD}(A\,;B)=\text{PGCD}(a\,;b)$

Algorithme d'Euclide et conséquences

Ex 7-10 : ***Appliquer l'algorithme***

Déterminer le PGCD de 13234 et de 4568

Vérifier avec la calculatrice.

Ex 7-11 : ***Programmation de l'algorithme d'Euclide***

En utilisant l'instruction python a%b qui donne le reste de la division euclidienne de a par b, compléter l'algorithme ci-dessous qui applique l'algorithme d'Euclide.

```
a=int(input("a="))
b=int(input("b="))
if ( ........... ):
    (a,b)=(b,a)
while (......................):
    r=...........
    a=...........
    b=...........
print(...........)
```

(a,b)=(b,a) permet d'échanger a et b

Ex 7-12 : ***Recherche des diviseurs communs***

1) Déterminer à l'aide de l'algorithme d'Euclide le PGCD de 2002 et de 4598.

2) En déduire D(2002,4598) l'ensemble des diviseurs communs positifs de 2002 et de 4598.

Ex 7-13 : ***Recherche des diviseurs communs***

Soit n un entier naturel tel que :
- dans la division euclidienne de 2791 par n, le reste est 8
- dans la division euclidienne de 2660 par n, le reste est 9.

Déterminer n.

Ex 7-14 : ***Homogénéité***

Soit m et n deux entiers naturels non nuls.

1) Déterminer $\text{PGCD}(m;4m+1)$

2) En déduire $\text{PGCD}(nm;n(4m+1))$

Ex 7-15 : ***Homogénéité***

Soit m et n deux entiers naturels non nuls.

On pose $\text{A}=n^2+7n$ et $\text{B}=n^2+9n+14$

1) Factoriser A et B.

2) Par disjonction de cas sur la parité, déterminer $\text{PGCD}(n;n+2)$

3) En déduire $\text{PGCD}(\text{A};\text{B})$ en fonction de n .

Nombres premiers entre eux

Ex 7-16 :

Soit a et b deux entiers premiers entre eux.
Montrer que $a+b$ est premier avec a et b .

Ex 7-17 :

Soit a , b et c des entiers naturels non nuls tels que a est premier avec b et c .

1) Montrer que tout diviseur commun de a et bc est un diviseur de $\text{PGCD}(ac;bc)$

2) En déduire que tout diviseur commun de a et bc est un diviseur de c .

3) En déduire que a est premier avec bc .

Ex 7-18 : ***Fractions irréductibles***

Soit n un entier naturel.

Montrer que $\dfrac{6n+7}{3n+3}$ est une fraction irréductible.

Ex 7-19 : ***Trouver deux entiers de PGCD connu***

1) Trouver tous les couples $(a;b)\in\mathbb{N}^2$ tels que $a+b=117$ et $\text{PGCD}(a;b)=13$

2) Trouver tous les couples $(a;b)\in\mathbb{N}^2$ tels que $ab=939870$ et $\text{PGCD}(a;b)=177$

Théorème de Bézout

Ex 7-20 : ***Calculer les coefficient de Bézout***

1) Montrer que 96 et 67 sont premiers entre eux et déterminer des entiers u et v tels que $96u+67v=1$

2) En déduire un couple d'entiers $(x;y)$ tels que $96x+67y=11$

3) Déterminer le PGCD de -330 et 473

Ex 7-21 : ***Recherche de u et v***

On considère deux nombres a et b premiers entre eux, avec $a>b$
Compléter l'algorithme ci-dessous permettant de trouver u et v

```
a=int(input("a="))
b=int(input("b="))
u=1
c=a
while (a%b ..........):
    u= ..........
    a=u*c
v= ..........
print ("u=",u,"v=",v)
```

Ex 7-22 : ***Utiliser le théorème de Bézout***

Dans chacun des cas, montrer que pour tout entier n, les entiers a et b sont premiers entre eux.

1) $a=5n+2$ et $b=3n+1$

2) $a=n^4+1$ et $b=n$

3) $a=n+5$ et $b=2n(n+5)+1$

Ex 7-23 : ***Utiliser le théorème de Bézout***

Soit a et b deux entiers strictement positifs tels que $(a^2+ab-b^2)^2=1$.

Montrer que a et b sont premiers entre eux.

Théorème de Gauss

Ex 7-24 : ***Résoudre une équation diophantienne de la forme*** $ax=b$

Résoudre dans $\mathbb{Z}^2$, l'équation $4(x-2)=5(y-1)$ (E)

Ex 7-25 : ***Résoudre une équation diophantienne de la forme*** $ax+by=c$

On considère l'équation $23x-11y=1(E_1)$

1) Justifier que cette équation admet au moins une solution dans $\mathbb{Z}^2$.

2) Déterminer une solution $(x_0;y_0)$ de (E1).

3) En déduire une solution particulière de $23x-11y=3(E)$

4) En déduire toutes les solutions de (E)

Ex 7-26: ***Résoudre une équation diophantienne de la forme*** $ax+by=c$

On considère les équations $45x+57y=6$ et $15x+19y=1$ (E1)

1) Justifier que l'équation (E_1) admet au moins une solution dans $\mathbb{Z}^2$.

2) Déterminer une solution $(x_0;y_0)$ de (E1).

3) Montrer que l'équation $45x+57y=6$ est équivalente à l'équation $15x+19y=2$ (E)

4) Déterminer une solution particulière de $15x+19y=2$ (E)

5) Déterminer toutes les solutions de (E)

Ex 7-27: ***Théorème d'Euclide***

Soit a et b deux entiers relatifs et p un nombre premier.

Montrer que si p divise le produit ab, alors p divise a ou p divise b.

Appliquer la dernière propriété du cours :

Si n est divisible par a et par b (premier entre eux), alors n est divisible par le produit ab.

Ex 7- 28 :

Soit un entier naturel n . On pose $a=n(n+1)(n+2)$.

Montrer que a est divisible par 2, 3 et 6.

Ex 7- 29 :

Montrer que pour tout entier naturel n , $10^n \equiv 1[9]$

En déduire que 10^n+8 est divisible par 9 et par 18.

Problèmes :

Ex 7-30 : ***Baccalauréat S Amérique du Sud 22 nov 2016 – ex 4***

Rep_units : Congruences – Divisibilié - Gauss

Les entiers naturels 1, 11, 111, 1 111, …sont des rep-units. On appelle ainsi les entiers naturels ne s'écrivant qu'avec des 1.
Pour tout entier naturel p non nul, on note N_p le rep-unit s'écrivant avec p fois le chiffre 1 :

$$N_p = \underbrace{11\ldots1}_{\substack{p \text{ répétitions} \\ \text{du chiffre 1}}} = \sum_{k=0}^{k=p-1} 10^k.$$

Dans tout l'exercice, p désigne un entier naturel non nul.
L'objet de cet exercice est d'étudier quelques propriétés des rep-units.

Partie A : divisibilité des rep-units dans quelques cas particuliers

1. Montrer que N_p n'est divisible ni par 2 ni par 5.
2. Dans cette question, on étudie la divisibilité de N_p par 3.
   a. Prouver que, pour tout entier naturel j, $10^j \equiv 1 \bmod 3$.
   b. En déduire que $N_p \equiv p \bmod 3$.
   c. Déterminer une condition nécessaire et suffisante pour que le rep-unit N_p soit divisible par 3.
3. Dans cette question, on étudie la divisibilité de N_p par 7.
   a. Recopier et compléter le tableau de congruences ci-dessous, où a est l'unique entier relatif appartenant à $\{-3\,;\,-2\,;\,-1\,;\,0\,;\,1\,;\,2\,;\,3\}$ tel que $10^m \equiv a \bmod 7$.
   On ne demande pas de justification.

m	0	1	2	3	4	5	6
a							

   b. Soit p un entier naturel non nul.
   Montrer que $10^p \equiv 1 \bmod 7$ si et seulement si p est un multiple de 6.
   On pourra utiliser la division euclidienne de p par 6.
   c. Justifier que, pour tout entier nature p non nul, $N_p = \dfrac{10^p-1}{9}$.
   d. Démontrer que « 7 divise N_p » est équivalent à « 7 divise $9N_p$ ».
   e. En déduire que N_p est divisible par 7 si et seulement si p est un multiple de 6.

Partie B : un rep-unit strictement supérieur à 1 n'est jamais un carré parfait

1. Soit n un entier naturel supérieur ou égal à 2.
   On suppose que l'écriture décimale de n^2 se termine par le chiffre 1, c'est-à-dire $n^2 \equiv 1 \bmod 10$.
   a. Recopier et compléter le tableau de congruences ci-dessous.

$n \equiv \ldots\ [10]$	0	1	2	3	4	5	6	7	8	9
$n^2 \equiv \ldots\ [10]$										

   b. En déduire qu'il existe un entier naturel m tel que : $n = 10m+1$ ou $n = 10m-1$.
   c. Conclure que $n^2 \equiv 1 \bmod 20$.
2. Soit p un entier naturel supérieur ou égal à 2.
   Quel est le reste de la division euclidienne de N_p par 20 ?
3. En déduire que, pour p entier naturel supérieur ou égal à 2, le rep-unit N_p n'est pas le carré d'un entier.

Ex 7-31 : ***Baccalauréat S Métropole 20 juin 2016 – ex 4***

Droites – Coordonnées entières : Divisibilié – PGCD - Bézout

python

Pour tout couple d'entiers relatifs non nuls (a, b), on note $\text{pgcd}(a, b)$ le plus grand diviseur commun de a et b.
Le plan est muni d'un repère $\left(O ; \vec{\imath}, \vec{\jmath}\right)$.

1. Exemple. Soit Δ_1 la droite d'équation $y = \frac{5}{4}x - \frac{2}{3}$.
   a. Montrer que si (x, y) est un couple d'entiers relatifs alors l'entier $15x - 12y$ est divisible par 3.
   b. Existe-il au moins un point de la droite Δ_1 dont les coordonnées sont deux entiers relatifs? Justifier.

Généralisation

On considère désormais une droite Δ d'équation (E) : $y = \frac{m}{n}x - \frac{p}{q}$ où m, n, p et q sont des entiers relatifs non nuls tels que $\text{pgcd}(m, n) = \text{pgcd}(p, q) = 1$.
Ainsi, les coefficients de l'équation (E) sont des fractions irréductibles et on dit que Δ est une droite rationnelle.
Le but de l'exercice est de déterminer une condition nécessaire et suffisante sur m, n, p et q pour qu'une droite rationnelle Δ comporte au moins un point dont les coordonnées sont deux entiers relatifs.

2. On suppose ici que la droite Δ comporte un point de coordonnées (x_0, y_0) où x_0 et y_0 sont des entiers relatifs.
   a. En remarquant que le nombre $ny_0 - mx_0$ est un entier relatif, démontrer que q divise le produit np.
   b. En déduire que q divise n.
3. Réciproquement, on suppose que q divise n, et on souhaite trouver un couple (x_0, y_0) d'entiers relatifs tels que $y_0 = \frac{m}{n}x_0 - \frac{p}{q}$.
   a. On pose $n = qr$, où r est un entier relatif non nul. Démontrer qu'on peut trouver deux entiers relatifs u et v tels que $qru - mv = 1$.
   b. En déduire qu'il existe un couple (x_0, y_0) d'entiers relatifs tels que $y_0 = \frac{m}{n}x_0 - \frac{p}{q}$.
4. Soit Δ la droite d'équation $y = \frac{3}{8}x - \frac{7}{4}$. Cette droite possède-t-elle un point dont les coordonnées sont des entiers relatifs? Justifier.
5. On donne l'algorithme suivant :

```
from math import floor

M=int(input("M="))
N=int(input("N="))
P=int(input("P="))
Q=int(input("Q="))

if(N%Q==0):
   X=0
   Y1=-P/Q
   Y2=-P/Q
   while ((floor(Y1)!=Y1) and (floor(Y2)!=Y2)):
      X=X+1
      Y1=M/N*X-P/Q
      Y2=-M/N*X-P/Q
   if (floor(Y1)==Y1):
      print (X,Y1)
   else:
      print (X,Y2)
else:
   print ("il n'y a pas de solutions")
```

   a. Justifier que cet algorithme se termine pour toute entrée de M, N, P, Q, entiers relatifs non nuls tels que $\text{pgcd}(M, N) = \text{pgcd}(P, Q) = 1$.
   b. Que permet-il d'obtenir?

Ex 7-32 : ***Baccalauréat S Antilles-Guyane spet 2015 – ex 4***

Cryptographie : Congruences – Équation diophantienne - Gauss – Bézout

On considère l'équation

$$51x - 26y = 1$$

où x et y sont des nombres entiers relatifs.

1. Justifier, en énonçant un théorème du cours, que cette équation admet au moins un couple solution.
2. **a.** Donner un couple solution $(x_0\,;\,y_0)$ de cette équation.
   b. Déterminer l'ensemble des couples solutions de cette équation.

Partie B

On fait correspondre à chaque lettre de l'alphabet un nombre entier comme l'indique le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Afin de coder une lettre de l'alphabet, correspondant à un entier x compris entre 0 et 25, on définit une fonction de codage f par $f(x) = y$, où y est le reste de la division euclidienne de $51x + 2$ par 26.
La lettre de l'alphabet correspondant à l'entier x est ainsi codée par la lettre correspondant à l'entier y.

1. Coder la lettre N.
2. En utilisant la partie A, déterminer l'entier a tel que $0 \leqslant a \leqslant 25$ et $51a \equiv 1\ [26]$.
3. Démontrer que si la lettre correspondant à un entier x est codée par une lettre correspondant à un entier y, alors x est le reste de la division euclidienne de $ay + 2$ par 26.
4. Déterminer alors la lettre qui est codée par la lettre N.
5. On applique 100 fois de suite la fonction de codage f à un nombre x correspondant à une certaine lettre. Quelle lettre obtient-on ?

LES NOMBRES PREMIERS

1) DÉFINITION ET PROPRIÉTÉ

Définition :

Un entier naturel est **premier** s'il n'admet que deux diviseurs positifs : 1 et lui même.

1 n'est pas un nombre premier.

Exemple :

2 , 3 , 5 , 7 sont des nombres premiers . 4, 6, 8, 9, 10 ne sont pas des nombres premiers.

Propriétés :

Soit a un entier naturel strictement supérieur à 1.

- a possède au moins un diviseur premier.
- si a n'est pas premier, alors au moins un des diviseurs premiers de a est inférieur ou égal à $\sqrt{a}$.

Preuve :

Soit a un entier naturel strictement supérieur à 1.

- Considérons D_a l'ensemble des diviseurs de a strictement supérieurs à 1.

  D_a n'est pas vide car il contient a. D_a a donc un plus petit élément n.

  Par définition, ce plus petit élément n est un diviseur de a strictement supérieur à 1.

  Supposons que n ne soit pas premier. n possède donc un diviseur p différent de 1 et de n.
  Comme on sait que 0 ne divise pas n, on a $p > 1$.
  D'autre part p étant un diviseur de n, on sait que $|p| \leq |n|$. On a donc $1 < p < n$.
  Alors on sait que p divise n et n divise a, donc p divise a . On en déduit donc que $p \in D_a$.

  Ceci est en contradiction avec le fait que n est le plus petit élément de D_a .

  On ne peut donc pas supposer que n n'est pas premier.
  On en déduit donc que n est un diviseur premier de a et que a possède donc au moins un diviseur premier.

- Soit n un diviseur premier de a. On peut écrire $a = n \times k$ avec $k \in \mathbb{N}^*$.
  a n'est pas premier et ne peut donc pas être égal à n qui est premier . On a alors $k > 1$.
  - Si $n \leq \sqrt{a}$, alors n est bien un diviseur premier de a inférieur ou égal à $\sqrt{a}$.
  - Si $n > \sqrt{a}$, alors :

    $$n \times k > k\sqrt{a} \Rightarrow a > k\sqrt{a} \Rightarrow k < \sqrt{a} .$$

    k est donc un diviseur de a inférieur à $\sqrt{a}$.
    k étant strictement supérieur à 1, il a un diviseur premier p et on sait que $p \leq k$ donc $p \leq \sqrt{a}$.
    p étant un diviseur de k et k un diviseur de a, on en déduit que p est un diviseur de a.
    p est donc un diviseur premier de a inférieur ou égal à $\sqrt{a}$.

  Dans tous les cas on a donc trouvé un diviseur premier de a inférieur ou égal à $\sqrt{a}$.

Remarques :

- Un entier naturel strictement supérieur à 1 et qui n'est pas premier est appelé **nombre composé**.
- Pour déterminer si un nombre donné N est premier, on peut chercher s'il est divisible par un nombre premier inférieur ou égal à $\sqrt{N}$.
  - Si l'un des nombres premiers inférieurs ou égaux à $\sqrt{N}$ divise N,
  - Si aucun des nombres premiers inférieurs ou égaux à $\sqrt{N}$ ne divise N,

  Cette méthode nécessite de connaître la liste des nombres premiers inférieurs ou égaux à $\sqrt{N}$.

2) CRIBLE D'ERATOSTHENE

Le crible d'Eratosthène est une méthode permettant d'obtenir tous les nombres premiers inférieurs à un nombre donné.
Pour trouver par exemple tous les nombres premiers inférieurs à 100, on écrit dans un tableau tous les nombres de 1 à 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- On raye le nombre 1 qui n'est pas premier.
Le premier nombre non rayé est 2, il est premier.
- On raye tous les multiples de 2 supérieurs à 2.
Le premier nombre non rayé est 3, il est premier.
- On raye tous les multiples de 3 supérieurs à 3.
Le premier nombre non rayé est 5, il est premier.
- On raye tous les multiples de 5 supérieurs à 5.
Le premier nombre non rayé est 7, il est premier.
- On raye tous les multiples de 7 supérieurs à 7.
Le premier nombre non rayé est 11, il est premier.

On peut s'arrêter car $11 > \sqrt{100}$.
On a obtenu alors dans les cases non rayées, les nombres premiers inférieurs à 100.

3) INFINITÉ DES NOMBRES PREMIERS

Propriété :

Il existe dans $\mathbb{N}$ une infinité de nombres premiers.

Preuve : ***exigible***

4) DÉCOMPOSITION EN PRODUIT DE FACTEURS PREMIERS

Propriété :

Soit n un entier supérieur ou égal à 2.

n peut se décomposer sous la forme : $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

où $p_1, p_2, \dots, p_k$ sont des nombres premiers tels que $p_1 < p_2 < \dots < p_k$ et $\alpha_1, \alpha_2, \dots, \alpha_k$ des entiers naturels non nuls.

Cette décomposition est appelée **décomposition de *n* en produit de facteurs premiers**.

On admet que cette décomposition est unique.

Preuve :

Soit la propriété P(n) : "tout entier q tel que $2 \leq q \leq n$ peut se décomposer en produit de facteurs premiers.", pour $n \geq 2$ (HR)

Démontrons par récurrence que cette propriété est vraie pour tout entier $n \geq 2$.

Initialisation :

2 peut se décomposer sous la forme $2 = 2^1$. La propriété P(2) est donc vraie.

Hérédité :

Supposons P(n) vraie pour un entier $n \geq 2$ fixé, c'est à dire pour tout entier q tel que $2 \leq q \leq n$, q peut se décomposer en produit de facteurs premiers.

Montrons que la propriété P(n+1) est vraie, c'est à dire pour tout entier q tel que $2 \leq q \leq n+1$, q peut se décomposer en produit de facteurs premiers.

Soit q un entier tel que $2 \leq q \leq n + 1$

- Si $2 \leq q \leq n$, q peut se décomposer en produit de facteurs premiers, d'après (HR)
- Si $q = n + 1$, alors on peut envisager deux cas :
  - Si $n + 1$ est premier, alors on peut écrire $n + 1 = (n + 1)^1$ et la décomposition est immédiate.
  - Si $n + 1$ n'est pas premier, alors $n + 1$ a un diviseur premier p tel que $1 < p < n + 1$, donc $2 \leq p \leq n$.
    On peut alors écrire $(n + 1) = p\,q$ avec q entier tel que $2 \leq q \leq n$.
    Daprès (HR), on peut décomposer q en facteurs premiers.
    On obtient alors une décomposition de $p \times q$ en facteurs premiers, c'est-à-dire une décomposition de $n + 1$ en facteurs premiers.

On a donc démontré que P(n+1) est vraie.

Conclusion :

P(n) est vraie pour tout entier $n \geq 2$ et en particulier tout entier $n \geq 2$ peut se décomposer en produit de facteurs premiers.

Exemples :

450	

On obtient :

450=

17787	

On obtient :

17787=

On cherche les diviseurs premiers dans l'ordre croissant.

Remarques :

- Du fait de l'unicité de le décomposition, si n a pour décomposition en produit de facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ alors tout diviseur premier de n est l'un des nombres $p_1, p_2, \dots, p_k$
- La plupart des calculatrices de lycée permettent d'obtenir la décomposition d'un nombre en produit de facteurs premiers :

Avec une TInspire :

factor(450) $2\cdot 3^2\cdot 5^2$

factor(17787) $3\cdot 7^2\cdot 11^2$

5) ENSEMBLE DES DIVISEURS

Exemple :

Dans $\mathbb{N}$ l'ensemble des diviseurs de 200 est {1 ; 2 ; 4 ; 5 ; 8 ; 10 ; 20 ; 25 ; 40 ; 50 ; 100 ; 200}
On peut retrouver ce résultat à partir de la décomposition de 200 en produit de facteurs premiers.

En effet cette décomposition est $200 = 2^3 \times 5^2$
On peut alors vérifier que les diviseurs de 200 sont les nombres s'écrivant sous la forme

Propriété :

Soit n un entier supérieur ou égal à 2, dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \dots p_k^{\alpha k}$
L'ensemble des diviseurs naturels de n est l'ensemble des entiers d s'écrivant sous la forme $d = p_1^{\beta 1}\, p_2^{\beta 2} \dots p_k^{\beta k}$
où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, ... , $0 \le \beta_k \le \alpha_k$.

Preuve :

n est un entier supérieur ou égal à 2, dont la décomposition en produit de facteurs premiers est : $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \dots p_k^{\alpha k}$

- Considérons un entier d s'écrivant sous la forme $d = p_1^{\beta 1}\, p_2^{\beta 2} \dots p_k^{\beta k}$

où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, ... , $0 \le \beta_k \le \alpha_k$.
On peut alors écrire $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \dots p_k^{\alpha k} = (p_1^{\beta 1}\, p_2^{\beta 2} \dots p_k^{\beta k}) \times (p_1^{\alpha 1-\beta 1}\, p_2^{\alpha 2-\beta 2} \dots p_k^{\alpha k-\beta k})$
Donc $n = d \times q$ avec $q = p_1^{\alpha 1-\beta 1}\, p_2^{\alpha 2-\beta 2} \dots p_k^{\alpha k-\beta k}$
On sait que $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, ... , $0 \le \beta_k \le \alpha_k$.
Donc $\alpha_1 - \beta_1$; $\alpha_2 - \beta_2$; ... ; $\alpha_k - \beta_k$ sont des entiers naturels.
Par conséquent q est un entier naturel et d est donc un diviseur de n.

- Considérons un entier d diviseur de n.

- Si $d = 1$, d peut s'écrire sous la forme $d = p_1^{\beta 1}\, p_2^{\beta 2} \dots p_k^{\beta k}$ avec $\beta_1 = \beta_2 = \dots = \beta_k = 0$

- Si $d > 1$, soit $d = q_1^{\gamma 1}\, q_2^{\gamma 2} \dots q_r^{\gamma r}$ la décomposition de d en produit de facteurs premiers.
  Alors $q_1, q_2, \dots, q_r$ sont des diviseurs premiers de d, donc ce sont des diviseurs premiers de n, donc ce sont certains des nombres $p_1, p_2, \dots, p_k$.
  On peut donc écrire $d = p_1^{\beta 1}\, p_2^{\beta 2} \dots p_k^{\beta k}$ où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels .
  (Si le nombre p_i n'apparaît pas dans la décomposition de d, on aura $\beta_i = 0$)

Démontrons que l'on a alors que $\beta_1 \le \alpha_1$

On sait que d divise n, et $p_1^{\beta 1}$ divise d , donc $p_1^{\beta 1}$ divise n , donc $p_1^{\beta 1}$ divise $p_1^{\alpha 1}\, p_2^{\alpha 2} \dots p_k^{\alpha k}$.
Si β_1 était strictement supérieur à α_1, alors $p_1^{\beta 1-\alpha 1}$ diviserait $p_2^{\alpha 2} \dots p_k^{\alpha k}$ donc p_1 diviserait $p_2^{\alpha 2} \dots p_k^{\alpha k}$, ce qui n'est pas possible puisque p_1 n'est pas l'un des nombres $p_2, \dots, p_k$.
On a donc $\beta_1 \le \alpha_1$. De même on peut justifier que $\beta_2 \le \alpha_2$, ... , $\beta_k \le \alpha_k$.
Donc d s'écrit sous la forme $d = p_1^{\beta 1}\, p_2^{\beta 2} \dots p_k^{\beta k}$ où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, ... , $0 \le \beta_k \le \alpha_k$

Remarque :

Si n a pour décomposition en produit de facteurs premiers $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \dots p_k^{\alpha k}$,
le nombre de diviseurs naturels de n est alors
En effet tout diviseur naturel peut s'écrire $p_1^{\beta 1}\, p_2^{\beta 2} \dots p_k^{\beta k}$ et chaque nombre β_i peut prendre les ($\alpha_i + 1$) valeurs de 0 à α_i .

La décomposition de 200 en produit de facteurs premiers est : 200 =

Ceci permet de dire que le nombre de diviseurs naturels de 200 est :

6) APPLICATION : PETIT THÉORÈME DE FERMAT

Petit théorème de Fermat :

Si p un nombre premier et a un entier naturel non divisible par p, alors $a^{p-1} - 1$ est divisible par p. ou encore

Preuve :

Soit p un nombre premier et a un entier naturel non multiple de p.
Les entiers p et a sont donc premiers entre eux.

- Considérons l'ensemble des multiples de a : A = { a , $2a$, … , $(p - 1)\,a$ }
  Ce sont p - 1 multiples non nuls de a . L'entier p ne divise aucun d'entre eux.

  En effet, si p divisait ka (avec k entier, $1 \leq k \leq p - 1$) , puisque p est premier avec a, il diviserait k d'après le théorème de Gauss, ce qui est impossible puisque $k < p$.

  Donc leurs restes dans la division euclidienne par p sont non nuls et sont donc des éléments de $\{1 , 2 ,\ldots, p - 1\}$

- Ces restes sont tous distincts : en effet si deux entiers k et k' appartenant à $\{1 , 2 ,\ldots, p - 1\}$, avec $k > k'$, étaient tels que $ka \equiv ka'$ (p) alors p diviserait $(k - k')\,a$.

  Or $1 \leq k - k' \leq p - 2$, donc $(k - k')\,a$ est élément de A et aucun élément de A n'est divisible par p.

  On a donc p - 1 multiples de a dont les restes dans la division euclidienne par p sont exactement, à l'ordre près, les entiers $1 , 2,\ldots, p - 1$.

- Considérons maintenant P le produit de ces multiples de a.

  On a donc $P \equiv 1 \times 2 \times \ldots \times (p - 1) \quad (p)$, c'est-à-dire $P \equiv (p - 1)! \quad (p)$. Ainsi p divise $(P - (p - 1)!)$.

  Or en réordonnant les facteurs de P, on obtient $P = (p - 1)! \times a^{p-1}$.

  Donc $P - (p - 1)! = (p - 1)! \times a^{p-1} - (p - 1)! = (p - 1)! \times (a^{p-1} - 1)$.

  p divise donc $(p - 1)! \times (a^{p-1} - 1)$.

  Or p est premier et ne divise aucun des facteurs de $(p - 1)!$. Il est donc premier avec $(p - 1)!$

  Donc d'après le théorème de Gauss, p divise $a^{p-1} - 1$.

Test de primalité :

Le petit théorème de Fermat donne une condition nécessaire pour que p soit premier. On dit qu'il constitue un test de primalité, ou plutôt ici de non primalité.

S'il existe un entier n compris entre 2 et $p-1$ tel que , n^{p-1} n'est pas congru à 1 modulo p , alors p n'est pas premier.

Ce test n'est pas efficace pour les grandes valeurs de p .

Propriété : ***Corollaire du petit théorème de Fermat***

Si p un nombre premier et a un entier naturel, alors $a^p - a$ est divisible par p. ou encore

Preuve :
Dans la fiche d'exercices

Définition :

Un entier naturel est **premier** s'il n'admet que deux diviseurs positifs : 1 et lui même.
Un entier naturel strictement supérieur à 1 et qui n'est pas premier est appelé **nombre composé**.

Propriété :

Soit a un entier naturel strictement supérieur à 1.

- a possède au moins un diviseur premier.
- si a n'est pas premier, alors au moins un des diviseurs premiers de a est inférieur ou égal à $\sqrt{a}$

1 n'est pas un nombre premier.

Test de primalité :

Pour déterminer si un nombre donné N est premier, on peut chercher s'il est divisible par un nombre premier inférieur ou égal à $\sqrt{N}$.

- Si l'un des nombres premiers inférieurs ou égaux à $\sqrt{N}$ divise N, alors N n'est pas premier.
- Si aucun des nombres premiers inférieurs ou égaux à $\sqrt{N}$ ne divise N, alors N est premier.

Crible d'Eratosthène :

- On raye le nombre 1 qui n'est pas premier.
Le premier nombre non rayé est 2, il est premier.
-On raye tous les multiples de 2 supérieurs à 2.
Le premier nombre non rayé est 3, il est premier.
- On raye tous les multiples de 3 supérieurs à 3.
Le premier nombre non rayé est 5, il est premier.
- On raye tous les multiples de 5 supérieurs à 5.
Le premier nombre non rayé est 7, il est premier.
- On raye tous les multiples de 7 supérieurs à 7.
Le premier nombre non rayé est 11, il est premier.

On peut s'arrêter car $11 > \sqrt{100}$

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

On a, obtenu alors dans les cases non rayées, les nombres premiers inférieurs à 100 (par exemple).

Infinité des nombres premiers :

Il existe dans $\mathbb{N}$ une infinité de nombres premiers.

Démonstration classique :

Supposons que l'ensemble des nombres premiers soit un ensemble fini $\{p_1, p_2, ..., p_k\}$.
Soit $n = p_1 \times p_2 \times ... \times p_k + 1$.
n est strictement supérieur à 1, il admet donc un diviseur premier, c'est-à-dire l'un des nombres p_i.
p_i divise n et p_i divise $p_1 \times p_2 \times ... \times p_k$, donc p_i divise leur différence, c'est-à-dire 1, ce qui est absurde.

L'ensemble des nombres premiers n'est donc pas un ensemble fini.

Décomposition en produit de facteurs premiers :

Soit n un entier supérieur ou égal à 2.
n peut se décomposer sous la forme : $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$
où $p_1, p_2, ..., p_k$ sont des nombres premiers tels que $p_1 < p_2 < \dots < p_k$ et $\alpha_1, \alpha_2, ..., \alpha_k$ des entiers naturels non nuls.
Cette décomposition est appelée **décomposition de *n* en produit de facteurs premiers**.

Tout diviseur premier de n est l'un des nombres $p_1, p_2, ..., p_k$

On admet que cette décomposition est unique.

17787	3
5929	7
847	7
121	11
11	11
1	

On obtient :

$17787 = 3 \times 7^2 \times 11^2$

Avec une Tinspire :

factor(450) $2 \cdot 3^2 \cdot 5^2$

factor(17787) $3 \cdot 7^2 \cdot 11^2$

Ensemble des diviseurs :

L'ensemble des diviseurs naturels de n est l'ensemble des entiers d s'écrivant sous la forme $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$
où $\beta_1, \beta_2, ..., \beta_k$ sont des entiers naturels tels que $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, ... , $0 \le \beta_k \le \alpha_k$.

Nombre de diviseurs :

le nombre de diviseurs naturels de n est alors $(\alpha_1 + 1) \times (\alpha_2 + 1) \times ... \times (\alpha_k + 1)$.

Petit théorème de Fermat :

Si p un nombre premier et a un entier naturel non divisible par p, alors $a^{p-1} - 1$ est divisible par p, càd $a^{p-1} \equiv 1\ [p]$

Test de primalité :

Ce test n'est pas efficace pour les grandes valeurs de p .

Le petit théorème de Fermat donne une condition nécessaire pour que p soit premier.

Si pour tout entier n inférieur à p , n^{p-1} n'est pas congru à 1 modulo p , alors p n'est pas premier.

Corollaire du petit théorème de Fermat :

Si p un nombre premier et a un entier naturel, alors $a^p - a$ est divisible par p.

Reconnaître des nombres premiers et des nombres composés

Ex 8-1 : ***Critères de divisibilité***

Les nombres suivants sont-ils premiers ?

425 , 43576 , 97 , 342153 , 909381 , 454452

Ex 8-2 : ***Décomposition en produit de facteurs premiers***

Décomposer les nombres ci-dessous en produit de facteurs premiers :

45 , 37 , 62 , 85 , 41 , 242 , 93, 500

Ex 8-3 : ***Vrai ou faux (justifier ou donner un contre-exemple)***

1) Tous les nombres premiers sont impairs.

2) Si un nombre p est premier alors $p+2$ n'est pas premier.

3) 1 est un nombre premier.

4) La somme de deux nombres premiers est un nombre premier.

5) 111 111 111 111 est premier.

Ex 8-4 : ***Puissance d'un nombre premier***

Soit p un nombre premier .

1) Le nombre p^2 est-il premier ?

2) Quels sont les diviseurs positifs de p^2 ?

3) Déterminer le nombre de diviseurs positifs de p^n où $n \in \mathbb{N}$

Ex 8-5 : ***Modulo 4***

1) Montrer que tout entier de la forme $4k$ ou $4k+2$ est composé pour $k \geqslant 1$.

2) En déduire que tout nombre premier impair est de la forme $4k+1$ ou $4k+3$.

3) La réciproque est-elle vraie ?

Ex 8-6 : ***En factorisant***

Soit n un entier naturel non nul.

1) Le nombre $\mathrm{N}=3n^2+4n$ peut-il être premier ?

2) Pour quelles valeurs de n , le nombre $\mathrm{M}=n^2-10n+16$ est-il premier ?

Ex 8-7 : ***Identité remarquable***

1) Montrer que si a^2-b^2 est premier, alors a et b sont consécutifs.

2) La réciproque est-elle vraie ?

Ex 8-8 : ***Nombre premier ou pas ?***

Compléter l'algorithme en Python ci-dessous permettant de déterminer si un entier naturel a est premier.

```
from math import *
a=int(input("a="))
m=floor(sqrt(a))
i=2
while ( ..................):
    if(..........................):
        print(a,"n'est pas un nombre premier")
        i=m+2
    else:
        i=i+1
if (i==.............):
    print(a,"est un nombre premier")
```

Utiliser les nombres premiers

Ex 8-9 : ***Fractions irréductibles***

1) Décomposer 54, 60 et 72 en produits de facteurs premiers.

2) Rendre irréductible : $\frac{72}{60}$ et $\frac{18}{54}$

Ex 8-10 :

Soit a et b deux entiers naturels avec $b \neq 0$.

Déterminer toutes les fractions $\frac{a}{b}$ égales à $\frac{168}{315}$ avec $a<168$ et $b<315$

Ex 8-11 :

1) a) Décomposer 48400 et 94864 en produit de facteurs premiers.

b) Justifier que ces deux nombres sont divisibles par 44^2 .

2) Déterminer sans calculatrice :

a) La racine carrée de 48400

b) La racine carrée de 94864

c) La fraction irréductible égale à $\frac{48400}{94864}$

Ex 8-12 : ***Avec des factorielles***

1) a) Montrer que 7 est premier avec 6 !

b) 8 est-il premier avec 7 ! ?

2) Soit p un nombre premier.

a) Montrer que p est premier avec $(p-1)!$

b) Soit un entier k , tel que $1 \leqslant k \leqslant p-1$. Que peut-on dire de p et $k!$?

Ex 8-13 : $\frac{1}{m}+\frac{1}{n}$

Soit m et n deux nombres premiers distincts.

1) mn et $m+n$ sont-ils premiers entre eux ?

2) Écrire $\frac{1}{m}+\frac{1}{n}$ sous forme d'une fraction irréductible.

Ex 8-14 :

1) Donner la décomposition en facteurs premiers de 2020.

2) Déterminer le plus petit entier naturel k tel que k^3 est un multiple de 2020.

Théorème de Gauss et nombres premiers

Ex 8-15 : $ab \equiv 0[p]$ ***avec p premier et*** $na \equiv nb[p]$ ***avec n et p premier entre eux***

1) Soit p un nombre premier .
Montrer que :

$$ab \equiv 0[p] \quad \Leftrightarrow \quad a \equiv 0[p] \text{ ou } b \equiv 0[p]$$

2) En déduire que pour tout entier n premier avec p , on a :

$$na \equiv nb[p] \quad \Leftrightarrow \quad a \equiv b[p]$$

Ex 8-16 : ***Inverse de a modulo p premier***

Soit p un nombre premier . On note $E_p = [1, 2, \ldots, p-1]$
Le but du problème est de montrer que pour tout $a \in E_p$, l'équation $ax \equiv 1[p]$ a une unique solution dans E_p .

1) Montrer qu'il existe un entier x_0 , tel que $ax_0 \equiv 1[p]$

2) On note r le reste dans la division euclidienne de x_0 par p .

a) Justifier que r est non nul.

b) Montrer que $ar \equiv 1[p]$.

c) Conclure.

3) Supposons qu'il existe $r' \in E_p$, tel que $ar' \equiv 1[p]$.
Justifier l'unicité de la solution

Ex 8-17 :

1) Pour chaque nombre a de 1 à 10, compléter le tableau ci-dessous donnant l'unique nombre b tel que $ab \equiv 1[11]$.

a	1	2	3	4	5	6	7	8	9	10
b	1		4				8	7	5	

2) En déduire que 10!+1 est divisible par 11.

Nombre de diviseurs

Ex 8-18 :

Un nombre s'écrit 4×10^n .

Existe-il une valeur de n telle que 4×10^n possède 27 diviseurs.

Ex 8-19 :

1) Soit p un nombre premier et n un entier naturel.
Déterminer le nombre de diviseurs de p^n .

2) Déterminer le produit de ces diviseurs.

Petit théorème de Fermat

Ex 8-20 : ***Démonstration du corollaire du petit théorème de Fermat***

On aimerait démontrer que si p un nombre premier et a un entier naturel, alors $a^p - a$ est divisible par p.

1) Vérifier le résultat pour $a=0$.

2) On suppose maintenant $a\neq0$.

a) Montrer que $a^{p-1} - 1$ divise $a^p - a$.

b) On suppose que a n'est pas un multiple de p . Montrer que $a^p - a$ est divisible par p.

c) Montrer le même résultat si a est un multiple non nul de p.

Ex 8-21 : $n^{11}-n$ ***divisible par*** **33**

1) Montrer que pour tout entier naturel n , le nombre $n^{11}-n$ est divisible par 11.

2) a) Montrer que pour tout entier naturel n , $n^3\equiv n[3]$.

b) En déduire que le nombre $n^{11}-n$ est divisible par 3.

3) Déduire des questions 1) et 2) que $n^{11}-n$ est divisible par 33.

Ex 8-22 : n^5-n ***divisible par*** **30**

Soit n un entier naturel non nul..
1) Justifier que n^5-n est divisible par 5.

2) Montrer que $n(n^2-1)(n^2+1)$ est divisible par 3.

3) Pourquoi n^5-n est-il divisible par 30 ?

Ex 8-23 : $3^{n+p}-3^{n+1}$ ***divisible par* 9**

Soit p un nombre premier . Montrer que pour tout entier naturel n , $3^{n+p}-3^{n+1}$ est divisible par p

Ex 8-24 : $3^{6n}-1$ ***divisible par* 7**

Montrer que pour tout entier naturel n , $3^{6n}-1$ est divisible par 7.

Ex 8-25 : $n^{13}-n$ ***divisible par* 182**

Soit n un entier naturel non nul.
1) Justifier que $n^{13}-n$ est pair.

2) Montrer que 13 et 7 divisent $n^{13}-n$

3) En déduire que $n^{13}-n$ est divisible par 182.

Problèmes :

Ex 8-26 : ***Baccalauréat S Pondichéry 17 avril 2015 – ex 4***

Nombre de Mersenne : Divisibilité - Congruences – Nombres premiers (test de primalité) - PGCD - Gauss

Les nombres de la forme 2^n-1 où n est un entier naturel non nul sont appelés **nombres de Mersenne**.

1. On désigne par a, b et c trois entiers naturels non nuls tels que PGCD$(b\,;\,c)=1$.
   Prouver, à l'aide du théorème de Gauss, que :
   si b divise a et c divise a alors le produit bc divise a.
2. On considère le nombre de Mersenne $2^{33}-1$.
   Un élève utilise sa calculatrice et obtient les résultats ci-dessous.

$(2^{33}-1)\div 3$	2863311530
$(2^{33}-1)\div 4$	2147483648
$(2^{33}-1)\div 12$	715827882,6

   Il affirme que 3 divise $(2^{33}-1)$ et 4 divise $(2^{33}-1)$ et 12 ne divise pas $(2^{33}-1)$.

   a. En quoi cette affirmation contredit-elle le résultat démontré à la question **1.**?
   b. Justifier que, en réalité, 4 ne divise pas $(2^{33}-1)$.
   c. En remarquant que $2\equiv -1\quad[3]$, montrer que, en réalité, 3 ne divise pas $2^{33}-1$.
   d. Calculer la somme $S=1+2^3+(2^3)^2+(2^3)^3+\cdots+(2^3)^{10}$.
   e. En déduire que 7 divise $2^{33}-1$.
3. On considère le nombre de Mersenne 2^7-1. Est-il premier ? Justifier.
4. On donne l'algorithme suivant où MOD$(N,\ k)$ représente le reste de la division euclidienne de N par k.

```
from math import *
n=int(input("n="))
k=2
while (((2**n-1)%k!=0) and (k<=sqrt(2**n-1))):
    k=k+1
print(k)
if k>sqrt(2**n-1):
    print("cas1")
else:
    print("cas2")
```

a. Qu'affiche cet algorithme si on saisit $n = 33$? Et si on saisit $n = 7$?

b. Que représente le CAS 2 pour le nombre de Mersenne étudié? Que représente alors le nombre k affiché pour le nombre de Mersenne étudié?

c. Que représente le CAS 1 pour le nombre de Mersenne étudié?*

Ex 8-27 : ***Baccalauréat S Centres étrangers juin 2015 – ex 4***

Triplets pythagoriciens

Dans cet exercice, on s'intéresse aux triplets d'entiers naturels non nuls $(x,\ y,\ z)$ tels que

$$x^2 + y^2 = z^2.$$

Ces triplets seront nommés « triplets pythagoriciens » en référence aux triangles rectangles dont ils mesurent les côtés, et notés en abrégé « TP ».
Ainsi $(3, 4, 5)$ est un TP car $3^2 + 4^2 = 9 + 16 = 25 = 5^2$.

Partie A : généralités

1. Démontrer que, si $(x,\ y,\ z)$ est un TP, et p un entier naturel non nul, alors le triplet $(px,\ py,\ pz)$ est lui aussi un TP.
2. Démontrer que, si $(x,\ y,\ z)$ est un TP, alors les entiers naturels x, y et z ne peuvent pas être tous les trois impairs.
3. Pour cette question, on admet que tout entier naturel non nul n peut s'écrire d'une façon unique sous la forme du produit d'une puissance de 2 par un entier impair :
   $n = 2^{\alpha} \times k$ où α est un entier naturel (éventuellement nul) et k un entier naturel impair.
   L'écriture $n = 2^{\alpha} \times k$ est nommée *décomposition* de n.
   Voici par exemple les *décompositions* des entiers 9 et 120 : $9 = 2^0 \times 9$,
   $120 = 2^3 \times 15$.
   a) Donner la décomposition de l'entier 192.
   b) Soient x et z deux entiers naturels non nuls, dont les décompositions sont $x = 2^{\alpha} \times k$ et $z = 2^{\beta} \times m$.
   Écrire la *décomposition* des entiers naturels $2x^2$ et z^2.
   c) En examinant l'exposant de 2 dans la *décomposition* de $2x^2$ et dans celle de z^2 , montrer qu'il n'existe pas de couple d'entiers naturels non nuls $(x,\ z)$ tels que $2x^2 = z^2$.

   On admet que la question **A - 3.** permet d'établir que les trois entiers naturels x, y et z sont deux à deux distincts. Comme de plus les entiers naturels x, y jouent un rôle symétrique, dans la suite, pour tout TP $(x,\ y,\ z)$, les trois entiers naturels x, y et z seront rangés dans l'ordre suivant :

$$x < y < z.$$

Partie B : recherche de triplets pythagoriciens contenant l'entier 2015

1. Décomposer en produit de facteurs premiers l'entier 2 015 puis, en utilisant le TP donné dans le préambule, déterminer un TP de la forme $(x,\ y,\ 2015)$.
2. On admet que, pour tout entier naturel n,
   $(2n+1)^2 + \left(2n^2+2n\right)^2 = \left(2n^2+2n+1\right)^2$.
   Déterminer un TP de la forme $(2015,\ y,\ z)$.
3. **a)** En remarquant que $403^2 = 169 \times 961$, déterminer un couple d'entiers naturels non nuls $(x,\ z)$ tels que : $z^2 - x^2 = 403^2$, avec $x < 403$.
   b) En déduire un TP de la forme $(x,\ 2015,\ z)$.

Ex 8-28 : ***Baccalauréat S Centres étrangers juin 2015 – ex 4***

Divisibilité – Gauss – Décomposition en produits de facteurs premiers

Pour tout entier naturel n non nul, on appelle $S(n)$ le nombre égal à la somme des diviseurs positifs de n.

1. Vérifier que $S(6) = 12$ et calculer $S(7)$.
2. **a.** Démontrer que, pour tout entier naturel n supérieur ou égal à 2, $S(n) \geqslant 1 + n$.
   b. Quels sont les entiers naturels n tels que $S(n) = 1 + n$?
3. On suppose dans cette question que n s'écrit $p \times q$ où p et q sont des nombres premiers distincts.
   a. Démontrer que $S(n) = (1 + p)(1 + q)$.
   b. On considère la proposition suivante :
   « Pour tous entiers naturels n et m non nuls distincts,
   $S(n \times m) = S(n) \times S(m)$ ».
   Cette proposition est-elle vraie ou fausse? Justifier.
4. On suppose dans cette question que l'entier n s'écrit p^k, où p est un nombre premier et k un nombre entier naturel non nul.
   a. Quels sont les diviseurs de n?

   b. En déduire que $S(n) = \dfrac{1 - p^{k+1}}{1 - p}$.
5. On suppose dans cette question que n s'écrit $p^{13} \times q^7$, où p et q sont des nombres premiers distincts.
   a. Soit m un entier naturel.
   Démontrer que m divise n si, et seulement si, il existe deux nombres entiers s et t avec $0 \leqslant s \leqslant 13$ et $0 \leqslant t \leqslant 7$ tels que $m = p^s \times q^t$.
   b. Démontrer que $S(n) = \dfrac{1 - p^{14}}{1 - p} \times \dfrac{1 - q^8}{1 - q}$.*

MATRICES - OPÉRATIONS ÉLÉMENTAIRES

1) DÉFINITIONS

Définition :

Soit m et n deux entiers naturels non nuls. Une matrice de **dimension** $m \times n$ est un tableau rectangulaire formé de m lignes et n colonnes de nombres réels

On dit aussi la taille ou le format d'une matrice.

Remarque :

Quand on parle de dimension $m \times n$, on ne calcule pas le produit !

Par exemple : $\begin{pmatrix} 1 & -2 & 3 \\ 1 & 5 & 0 \end{pmatrix}$ est

Définitions :

- **Une matrice ligne** est une matrice formée d'une seule ligne.
- **Une matrice colonne** est une matrice formée d'une seule colonne.
- **Une matrice carrée** d'ordre n est une matrice $n \times n$.

Exemple :

Écriture générale d'une matrice :

Une matrice A de dimension $m \times n$ (où $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$) peut s'écrire sous cette forme :

$$A = \underbrace{\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{m-1,n} \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}}_{taille\ m \times n}$$

Les nombres a_{ij} (notés parfois $a_{i,j}$ pour éviter les confusions) (où $1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant n$) s'appellent **les coefficients** de la matrice A .

On peut aussi noter $\mathrm{A} = (a_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$.

Définition :

Deux matrices sont **égales** si et seulement si elles ont la même dimension et ont les mêmes coefficients aux mêmes places.

2) MATRICES PARTICULIÈRES

Définition :

La matrice nulle d'ordre n , notée O_n , est la matrice carrée d'ordre n dont tous les coefficients sont nuls.

Définition :

Dans une matrice carrée d'ordre n , les coefficients a_{11} , a_{22} , …, a_{nn} forment l**a diagonale principale** de la matrice.

Une matrice carrée est **diagonale** si et seulement si ses coefficients qui ne sont pas sur la diagonale principale sont tous nuls.

Exemple :

Définition :

La matrice unité d'ordre n (ou matrice identité d'ordre n), notée I_n , est la matrice carrée d'ordre n contenant uniquement des 1 sur sa diagonale principale et des 0 ailleurs.

Exemple :

3) OPÉRATIONS SUR LES MATRICES

A) ADDITION ET MULTIPLICATION PAR UN RÉEL

Définition :

Soit $\mathrm{A}=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$ et $\mathrm{B}=(b_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$ deux matrices de même taille $m\times n$.

La somme A+B est la matrice définie par $\mathrm{A}+\mathrm{B}=(a_{ij}+b_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$.

On ne peut ajouter que des matrices de même taille, et pour cela on ajoute les coefficients situés à la même place.

Exemple : $\begin{pmatrix}-1 & 1 & 4\\ 0 & 0 & 1\\ 2 & 3 & 5\end{pmatrix}+\begin{pmatrix}1 & 0 & 2\\ 0 & -1 & 1\\ -2 & 3 & 4\end{pmatrix}=$

Remarques :

- On a de façon évidente .
- Pour toute matrice carrée A d'ordre n , on a

Définition :

Soit $\mathrm{A}=(a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$ une matrice et $\lambda\in\mathbb{R}$.

La matrice $\lambda\,\mathrm{A}$ est la matrice définie par $\lambda\,\mathrm{A}=(\lambda\,a_{ij})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$.

- Multiplier une matrice par un réel revient à multiplier tous les coefficients par ce réel.
- Par convention, on écrit le réel λ à gauche de la matrice A.

Exemple : $3\begin{pmatrix}-1 & 1 & 4\\ 0 & 0 & 1\\ 2 & 3 & 5\end{pmatrix}=$

Remarques :

- Les règles de priorité sont les mêmes qu'avec les réels : 5 A+2 B désigne la matrice (5 A)+(2B)
- On note $-\mathrm{A}$ la matrice $(-1)\times\mathrm{A}$. $-\mathrm{A}$ est **la matrice opposée** de A.
- On peut maintenant définir la différence de deux matrices A et B de même taille : A−B=A+(−1) B .

B) MULTIPLICATION D'UNE MATRICE LIGNE PAR UNE MATRICE COLONNE

Définition :

Soit n un entier naturel non nul.
Soit $A=(a_{1j})$ une matrice ligne de dimension $1\times n$ et $B=(b_{i1})$ une matrice colonne de dimension $n\times 1$

La matrice $A\times B$ est la matrice définie par :

$$A\times B=\begin{pmatrix} a_{11} & a_{12} & ,\dots, & a_{1n}\end{pmatrix}\times\begin{pmatrix} b_{11}\\ b_{21}\\ \dots\\ b_{n1}\end{pmatrix}=a_{11}b_{11}+a_{12}b_{21}+\dots+a_{1n}b_{n1}=\sum_{k=1}^{n} a_{1k}b_{k1}$$

le nombre de colonnes de A est donc égal au nombre de lignes de B .

Exemple : $\begin{pmatrix}1 & 0 & 5\end{pmatrix}\times\begin{pmatrix}0\\2\\2\end{pmatrix}=$

C) MULTIPLICATION DE DEUX MATRICES

Définition :

Soit A une matrice de dimension $m\times n$ et B une matrice de taille $n\times p$.

Le produit A×B ou A B est la matrice de dimension $m\times p$ dont le coefficient situé à la ligne i et la colonne j est le coefficient du produit de la ligne i de A par la colonne j de B pour $1\leqslant i\leqslant m$ et $1\leqslant j\leqslant p$.

Le produit AB de deux matrices A et B existe si et seulement si le nombre de colonnes de A est égal au nombre de lignes de B .

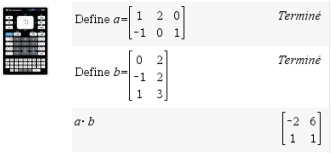
Exemple :

Le produit d'une matrice 2×3 par une matrice 3×2 est une matrice 2×2 .

$$\begin{pmatrix}1 & 2 & 0\\ -1 & 0 & 1\end{pmatrix}\times\begin{pmatrix}0 & 2\\ -1 & 2\\ 1 & 3\end{pmatrix}=$$

Au brouillon, il est beaucoup plus simple de présenter les calculs de la façon suivante : $\begin{array}{cc} & \begin{pmatrix}0 & 2\\ -1 & 2\\ 1 & 3\end{pmatrix}\\ \begin{pmatrix}1 & 2 & 0\\ -1 & 0 & 1\end{pmatrix} & \begin{pmatrix}-2 & 6\\ 1 & 1\end{pmatrix}\end{array}$ (sans détailler les calculs)

La plupart des calculatrices de lycée permettent d'obtenir le produit de deux matrices . **Avec une TInspire :**



Propriété :

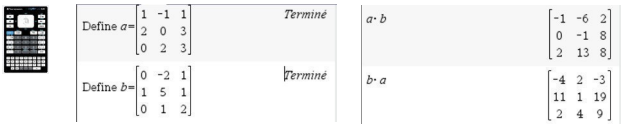
Soit A , B , C des matrices carrées d'ordre $n\in\mathbb{N}^*$.

- **Associativité** : $(A\times B)\times C=A\times(B\times C)=A\times B\times C=ABC$
- **Distributivité** : $A\times(B+C)=AB+AC$ et $(A+B)\times C=AC+BC$
- Produit par un réel λ : $(\lambda A)\times B=\lambda AB$ et $A\times(\lambda B)=\lambda AB$
- Soit I_n la matrice unité d'ordre n alors $I_n\times A=A$ et $A\times I_n=A$.

Attention :

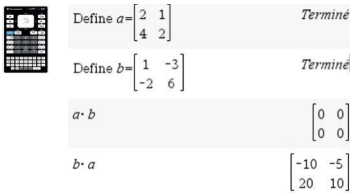
- La multiplication de matrices n'est pas commutative :

  en général, $A\times B\neq B\times A$



- Soit A, B et C des matrices carrées d'ordre $n \in \mathbb{N}^*$.

- Soit A et B et C des matrices d'ordre $n \in \mathbb{N}^*$.



D) PUISSANCES ENTIÈRES D'UNE MATRICE

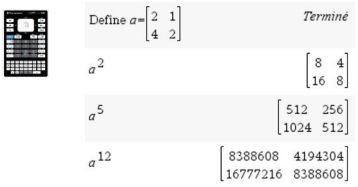
Définition :

Soit A une matrice carrée d'ordre $n \in \mathbb{N}^*$.

On note $A^2 = A \times A$, $A^3 = A \times A \times A$, etc.

Plus généralement, pour $k \in \mathbb{N}^*$, A^k est le produit de k matrices toutes égales à A .

Par convention, on posera $A^0 = I_n$.



3) MATRICES INVERSIBLES ET APPLICATION AUX SYSTÈMES

A) MATRICE INVERSIBLES

Définition et propriété :

Soit A une matrice carrée d'ordre $n \in \mathbb{N}^*$.

On dit que A est **inversible** si et seulement si il existe une matrice carrée d'ordre n , notée A^{-1} telle que $A \times A^{-1} = A^{-1} \times A = I_n$.

La matrice A^{-1} est unique, elle et appelée **matrice inverse** de A .

On admet que :
$A\,A^{-1} = I_n \Leftrightarrow A^{-1}A = I_n$

Dans les exercices il suffira de faire un seul des deux produits.

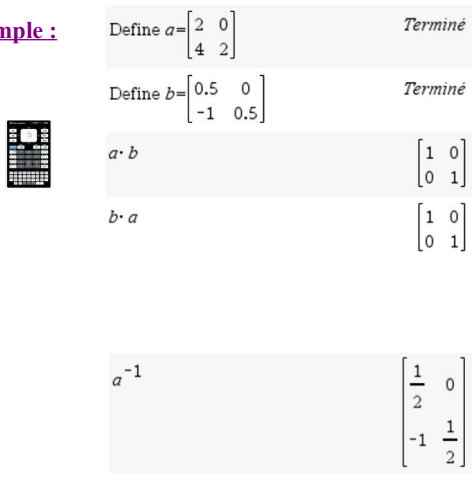
Preuve : (de l'unicité)

Supposons que A possède deux inverses, notés B et B' . On a donc $AB = I_n$, $AB' = I_n$, $BA = I_n$, $B'A = I_n$.

On peut donc écrire :

Remarque : Un matrice $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$,de dimension 2, est inversible si et seulement si $ad - bc \neq 0$ (preuve dans la feuille d'exercices)

Exemple :



La matrice $\begin{pmatrix} 2 & 0 \\ 4 & 2 \end{pmatrix}$ est inversible de matrice inverse $\begin{pmatrix} 0{,}5 & 0 \\ -1 & 0{,}5 \end{pmatrix}$

Avec la TInspire, on peut obtenir directement (si elle existe) la matrice inverse.

B) APPLICATION AUX SYSTÈMES LINÉAIRES

Propriété :

Un système linéaire à n inconnues x_1 , x_2 , …, x_n

$$\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1,n}x_n=y_1 \\ a_{21}x_1+a_{22}x_2+\ldots+a_{2,n}x_n=y_2 \\ \ldots \\ a_{n,1}x_1+a_{n,2}x_2+\ldots+a_{n,n}x_n=y_n \end{cases}$$

peut s'écrire sous la forme A X=Y , où $\mathrm{A}=(a_{ij})_{1\leqslant i\leqslant n,1\leqslant j\leqslant n}$ est une matrice carrée d'ordre n , $\mathrm{X}=\begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}$ et $\mathrm{Y}=\begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_n \end{pmatrix}$

sont des matrices colonnes de dimension $n\times 1$.

Si A est inversible, le système a alors une solution unique : $\mathrm{X}=\mathrm{A}^{-1}\mathrm{Y}$.

Preuve :

Si A est inversible, on peut écrire :

A X =Y $\Rightarrow$

Réciproquement,

$\mathrm{X}=\mathrm{A}^{-1}\mathrm{Y}$ $\Rightarrow$

$\mathrm{A}^{-1}\mathrm{Y}$ est donc l'unique solution du système écrite sous forme matricielle.

Exemple : Résoudre $\begin{cases} x+y-z=3 \\ 2x+y-z=0 \\ -x+2y+z=3 \end{cases}$

On pose

On a donc $\begin{cases} x+y-z=3 \\ 2x+y-z=0 \\ -x+y-z=3 \end{cases}$ $\Leftrightarrow$

Avec la calculatrice on voit que A est inversible
et on détermine A^{-1} .

Define $a=\begin{bmatrix} 1 & 1 & -1 \\ 2 & 1 & -1 \\ -1 & 2 & 1 \end{bmatrix}$ *Terminé*

a^{-1} $\begin{bmatrix} -1 & 1 & 0 \\ \frac{1}{3} & 0 & \frac{1}{3} \\ \frac{-5}{3} & 1 & \frac{1}{3} \end{bmatrix}$

Ainsi : $\mathrm{AX}=\mathrm{Y}$ $\Leftrightarrow$

Define $y=\begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix}$ *Terminé*

$a^{-1}\cdot y$ $\begin{bmatrix} -3 \\ 2 \\ -4 \end{bmatrix}$

Définitions :

$\begin{pmatrix} -1 & \frac{2}{3} & \frac{1}{2} \end{pmatrix}$

$\begin{pmatrix} 1 \\ 4 \\ 1 \end{pmatrix}$

$\begin{pmatrix} -1 & 1 & 4 \\ 0 & 0 & 1 \\ 2 & 3 & 5 \end{pmatrix}$

Soit m et n deux entiers naturels non nuls. Une matrice de **dimension (ou taille ou format)** $m \times n$ est un tableau rectangulaire formé de m lignes et n colonnes de nombres réels

- **Une matrice ligne** est une matrice formée d'une seule ligne.
- **Une matrice colonne** est une matrice formée d'une seule colonne.
- **Une matrice carrée** d'ordre n est une matrice $n \times n$.

Le coefficient $a_{i,j}$ est le nombre placé à la i-ième ligne et la j-ième colonne.

Une matrice A de dimension $m \times n$ (où $m \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$) peut s'écrire sous cette forme :

$$A = \underbrace{\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n} \\ a_{21} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{m-1,n} \\ a_{m,1} & \cdots & a_{m,2} & a_{m,n} \end{pmatrix}}_{\text{taille } n \times n}$$

Les nombres a_{ij} (notés parfois $a_{i,j}$ pour éviter les confusions) (où $1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant n$) s'appellent **les coefficients** de la matrice A .

On peut aussi noter $A = (a_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$.

Deux matrices sont **égales** si et seulement si elles ont la même dimension et ont les mêmes coefficients aux mêmes places.

Matrices particulières :

Matrice nulle

La matrice nulle d'ordre n , notée O_n , est la matrice carrée d'ordre n dont tous les coefficients sont nuls.

$$O_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Matrice diagonale

Dans une matrice carrée d'ordre n , les coefficients a_{11} , a_{22} , …, a_{nn} forment **la diagonale principale** de la matrice. **Une matrice carrée est diagonale** si et seulement si ses coefficients qui ne sont pas sur la diagonale principale sont tous nuls.

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Matrice unité

La matrice unité d'ordre n (ou matrice identité d'ordre n), notée I_n , est la matrice carrée d'ordre n contenant uniquement des 1 sur sa diagonale principale et des 0 ailleurs.

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Opérations :

Si A est d'ordre n , $A + O_n = A$

$(-1) \times A = -A$ est **la matrice opposée** de A.

Différence : $A - B = A + (-1)\,B$

Somme

A+B=B+A (commutativité)

$$\begin{pmatrix} -1 & 1 & 4 \\ 0 & 0 & 1 \\ 2 & 3 & 5 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ -2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 6 \\ 0 & -1 & 2 \\ 0 & 6 & 9 \end{pmatrix}$$

On ne peut ajouter que des matrices de même taille, et pour cela on ajoute les coefficients situés à la même place.

Multiplication par un réel

$$3 \begin{pmatrix} -1 & 1 & 4 \\ 0 & 0 & 1 \\ 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} -3 & 3 & 12 \\ 0 & 0 & 3 \\ 6 & 9 & 15 \end{pmatrix}$$

Multiplier une matrice par un réel revient à multiplier tous les coefficients par ce réel.

Multiplication d'une matrice ligne par une matrice colonne

$$\begin{pmatrix} 1 & 0 & 5 \end{pmatrix} \times \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix} = 1 \times 0 + 0 \times 2 + 5 \times 2 = 10$$

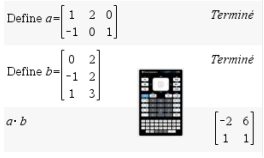
Le nombre de colonnes de A est égal au nombre de lignes de B .

Multiplication de deux matrices

$$\begin{pmatrix} 1 & 2 & 0 \\ -1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 2 \\ -1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 0 \times 1 + 2 \times (-1) + 0 \times 1 & 1 \times 2 + 2 \times 2 + 0 \times 3 \\ -1 \times 0 + 0 \times (-1) + 1 \times 1 & -1 \times 2 + 0 \times 2 + 1\,3 \end{pmatrix}$$

$$= \begin{pmatrix} -2 & 6 \\ 1 & 11 \end{pmatrix}$$

Avec une Ti-nspire



Représentation pratique

$$\begin{pmatrix} 0 & 2 \\ -1 & 2 \\ 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 0 \\ -1 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} -2 & 6 \\ 1 & 11 \end{pmatrix}$$

En général, la multiplication de matrices n'est pas commutative :

$\mathbf{A \times B \neq B \times A}$

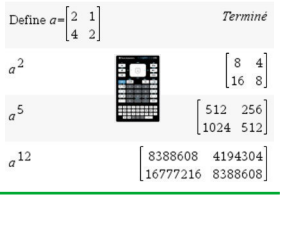
Le produit AB de deux matrices A et B existe si et seulement si le nombre de colonnes de A estt égal au nombre de lignes de B .

Propriétés :

Soit A , B , C des matrices carrées d'ordre $n \in \mathbb{N}^*$.

- **Associativité** : $(A \times B) \times C = A \times (B \times C) = A \times B \times C = ABC$
- **Distributivité** : $A \times (B + C) = AB + AC$ et $(A + B) \times C = AC + BC$
- Produit par un réel λ : $(\lambda A) \times B = \lambda AB$ et $A \times (\lambda B) = \lambda AB$
- Soit I_n la matrice unité d'ordre n alors $I_n \times A = A$ et $A \times I_n = A$.

Attention : AB=AC n'implique pas que B=C (On ne peut pas simplifier par A)
$AB = O_n$ n'implique pas que $A = O_n$ ou $B = O_n$



Puissances :

Soit A une matrice carrée d'ordre $n \in \mathbb{N}^*$.

On note $A^2 = A \times A$, $A^3 = A \times A \times A$, etc ...
Plus généralement, pour $k \in \mathbb{N}^*$, A^k est le produit de k matrices toutes égales à A .
Par convention, on posera $A^0 = I_n$.

Matrices inversibles :

Soit A une matrice carrée d'ordre $n \in \mathbb{N}^*$.

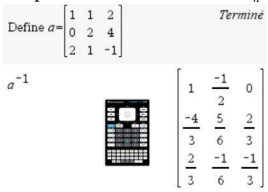
Attention :

A^{-1} n'existe pas toujours

On dit que A est **inversible** si et seulement si il existe une matrice carrée d'ordre n , notée A^{-1} telle que $A \times A^{-1} = A^{-1} \times A = I_n$
La matrice A^{-1} est unique, elle et appelée **matrice inverse** de A .

On admet que : $A\,A^{-1} = I_n \Leftrightarrow A^{-1} A = I_n$.
Dans les exercices il suffira de faire un seul des deux produits.

Un matrice $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$,de dimension 2, est inversible si et seulement si $ad - bc \neq 0$



Application aux systèmes linéaires :

Exemple :

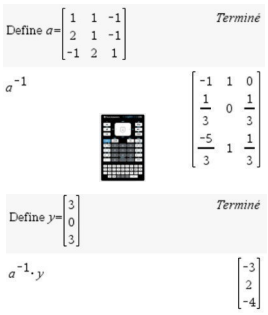
Résoudre $\begin{cases} x + y - z = 3 \\ 2x + y - z = 0 \\ -x + 2y + z = 3 \end{cases}$

On pose $A = \begin{pmatrix} 1 & 1 & -1 \\ 2 & 1 & -1 \\ -1 & 2 & 1 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $Y = \begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix}$

On a donc $\begin{cases} x + y - z = 3 \\ 2x + y - z = 0 \\ -x + y - z = 3 \end{cases} \Leftrightarrow AX = Y$

Avec la calculatrice on voit que A est inversible et on détermine A^{-1} .

Ainsi : $AX = Y \Leftrightarrow X = A^{-1} Y \Leftrightarrow \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 \\ \frac{1}{3} & 0 & \frac{1}{3} \\ -\frac{5}{3} & 1 & \frac{1}{3} \end{pmatrix} \begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} -3 \\ 2 \\ -4 \end{pmatrix}$



Notion de matrice :appendre le cours

Ex 9-1 : ***Vrai ou faux***

1) Une matrice de taille $n \times p$ possède p lignes et n colonnes.

2) Le coefficient d'une matrice A noté a_{ij} se situe à la i -ème ligne et à la- j -ième colonne.

3) Une matrice nulle est nécessairement carrée.

4) Une matrice unité est nécessairement carrée.

5) Une matrice ligne est aussi appelée vecteur ligne.

6) La taille d'une matrice ligne est notée $1 \times p$ où $p \in \mathbb{Z}$.

7) On peut additionner deux matrices de tailles différentes.

8) On peut multiplier deux matrices de tailles différentes.

9) On peut multiplier deux matrices de n'importe quelles tailles.

10) Pour que le produit AB soit une matrice carrée, il faut que A et B soient des matrices carrées de même taille.

11) Pour que le produit AB soit une matrice carrée, il suffit que A et B soient des matrices carrées de même taille.

12) AB=AC implique B=C

13) $AB = O_n$ implique $A = O_n$ ou $B = O_n$

Calculs élémentaires

Ex 9-2 : ***Somme, produit, commutativité***

Dans chacun des cas, effectuer la somme A+B et les produits des matrices A B et BA lorsque cela est possible.

1) $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 3 & -3 \\ 5 & 8 \end{pmatrix}$

2) $A = \begin{pmatrix} 1 & -2 \\ 3 & 1 \\ 0 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 0 \\ 7 & -1 \\ 1 & 5 \end{pmatrix}$

3) $A = \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix}$ $B = \begin{pmatrix} 3 & 4 & 7 \end{pmatrix}$

4) La multiplication des matrices est-elle commutative ?

Ex 9-3 : ***Combinaisons linéaires***

On considère les matrices $A=\begin{pmatrix}3 & 4\\ 1 & -1\end{pmatrix}$ et $B=\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix}$

1) Calculer $2A-3B$

2) Déterminer les réels x et y tels que $xA+yB=\begin{pmatrix}7 & 7\\ 2 & 0\end{pmatrix}$

Ex 9-4 : ***Carré***

On considère la matrice $A=\begin{pmatrix}3 & 4\\ -5 & x\end{pmatrix}$

Déterminer la valeur de x telle que $A^2=\begin{pmatrix}-11 & 12\\ -15 & 20\end{pmatrix}$

Ex 9-5 : ***Identités remarquables***

1) On considère les matrices $A=\begin{pmatrix}1 & 2\\ 3 & -1\end{pmatrix}$ et $B=\begin{pmatrix}3 & 4\\ 6 & 8\end{pmatrix}$

a) Calculer et comparer $(A+B)^2$ et $A^2+2AB+B^2$

b) Développer $(A+B)^2$

c) En déduire une condition nécessaire et suffisante pour que l'identité remarquable soit vérifiée.

2) On considère maintenant les matrices $A=\begin{pmatrix}-1 & 2\\ 3 & -1\end{pmatrix}$ et $B=\begin{pmatrix}1 & 2\\ 3 & -1\end{pmatrix}$

Vérifier que les matrices A et B vérifient la condition trouvée précédemment et comparer à nouveau les égalités $(A+B)^2$ et $A^2+2AB+B^2$

Ex 9-6 : ***Puissances de matrices et récurrence***

On considère les matrices $A=\begin{pmatrix}0,8 & 0,8\\ 0,2 & 0,2\end{pmatrix}$, $B=\begin{pmatrix}0,2 & -0,8\\ -0,2 & 0,8\end{pmatrix}$ et $M=\begin{pmatrix}0,9 & 0,4\\ 0,1 & 0,6\end{pmatrix}$

1) Montrer que $M=A+0,5B$

2) Vérifier que $A^2=A$ et que $AB=BA=O_2$

3) Montrer (par récurrence) que pour tout entier naturel n strictement positif : $A^n=A$.

On admet que $B^n=B$.

4) On considère la relation $M^n=A+0,5^n B$.

a) Montrer que cette relation est vraie pour $n=0$.

b) Montrer que cette relation est vraie pour tout entier naturel n strictement positif.

Inverses de matrices :

Ex 9-7 : ***Développement et inverses***

Dans chacun des cas ci-dessous, A est une matrice de dimension $n\times p$ (on peut avoir $n=p$) et I est une matrice identité.
Préciser les tailles possibles des matrices B et I, puis développer les expressions données :

1) A(B+I)

2) $(B+A)A^{-1}$

3) $AB(B^{-1}A^{-1}-AB)$

4) B(I-A)

Ex 9-8 : ***Factorisation et inverses***

Factoriser les expressions suivantes :

1) $(A+I)^{-1}A+(A+I)^{-1}$

2) $(A+I)^{-1}+A(A+I)^{-1}$

3) $(A+I)^{-1}+A(I+A^{-1})$

Ex 9-9 : ***Avec la calculatrice***

Avec la calculatrice déterminer s'ils existent les inverses des matrices ci-dessous :

$A=\begin{pmatrix}1 & 2\\ 3 & -1\end{pmatrix}$, $B=\begin{pmatrix}3 & 4\\ 6 & 8\end{pmatrix}$, $C=\begin{pmatrix}-1 & 0 & 1\\ 0 & 2 & 0\\ 3 & 0 & 1\end{pmatrix}$

Ex 9-10 : ***Vérifier que deux matrices sont inverses l'une de l'autre***

Les matrices suivantes sont-elles inverses l'une de l'autre ?

1) $A=\begin{pmatrix}-1 & 2\\ 3 & -1\end{pmatrix}$ et $B=\frac{1}{5}\begin{pmatrix}1 & 2\\ 3 & 1\end{pmatrix}$

2) $A=\begin{pmatrix}0 & 0 & -1\\ 0 & -1 & 0\\ -1 & 0 & 0\end{pmatrix}$ et elle même

Ex 9-11 : ***Inverse d'un produit***

Soit A et B deux matrices inversibles.
Démontrer que $(AB)^{-1}=B^{-1}A^{-1}$

Ex 9-12 : ***Inverse d'une matrice*** 2×2 ***(condition d'existence à connaître)***

Soit $A=\begin{pmatrix}a & c\\ b & d\end{pmatrix}$.

1) Démontrer que $(a+d)A-A^2=(ad-bc)I_2$.

2) Factoriser le membre de gauche par A.

3) En déduire une condition pour que le matrice A admette un inverse.

4) Déterminer cet inverse.

Ex 9-13 : ***Inverse à partir d'une relation polynomiale***

On considère la matrice $A=\begin{pmatrix}1 & -a & 0 & 0\\ 0 & 1 & -a & 0\\ 0 & 0 & 1 & -a\\ 0 & 0 & 0 & 1\end{pmatrix}$

1) Déterminer la matrice J telle que $A=I_4-aJ$

2) Calculer J^2 , J^3 et J^4 et en déduire que $I_4=I_4-a^4J^4$.

3) Développer $(I_4-aJ)(I_4+aJ+a^2J^2+a^3J^3)$
En déduire l'expression de A^{-1} en fonction de J, puis en fonction de a .

4) Vérifier avec la calculatrice ou un logiciel.

Ex 9-14 : ***Inverse à partir d'une relation polynomiale***

On considère la matrice $A=\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & 1 & -1\\ 1 & -1 & -1 & -1\end{pmatrix}$

1) Calculer A^2 et A^3 .

2) Déterminer les réels a et b tels que $A^3=aA+bI_4$

3) En déduire l'inverse de A.

Ex 9-15 : ***Système linéaire de deux équations à deux inconnues***

On considère le système linéaire : $\begin{cases}4x-3y=-2\\ x-y=-5\end{cases}$ (S)

1) Écrire le système sous la forme AX=Y.

2) Résoudre le système (S) en utilisant l'inverse de la matrice A.

Ex 9-16 : ***Système linéaire de trois équations à trois inconnues***

On considère le système linéaire : $\begin{cases} 4x-2y+z=7 \\ -x+y-z=-9 \\ x-5y-2z=10 \end{cases}$ (S)

1) Écrire le système sous la forme AX=Y.

2) Résoudre le système (S) en utilisant l'inverse de la matrice A.

Ex 9-17 : ***Matrice diagonalisable et puissances***

On considère les matrices $A=\begin{pmatrix} 4 & 3 \\ -2 & -1 \end{pmatrix}$, $P=\begin{pmatrix} 3 & 1 \\ -2 & -1 \end{pmatrix}$ et $D=\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$

1) Montrer que P est inversible et calculer P^{-1} .

2) Montrer que $A=PDP^{-1}$.

3) Montrer que $A^n=PD^nP^{-1}$, pour tout $n\in\mathbb{N}^*$

4) Avec la calculatrice, conjecturer une expression de D^n pour tout $n\in\mathbb{N}^*$, puis démontrer cette conjecture.

5) En déduire A^n pour tout $n \in \mathbb{N}^*$.

Problèmes :

Ex 9-18 : ***Baccalauréat S Amérique du nord juin 2015 – ex 4***

Parabole passant par trois points : Congruences - Matrices

On donne les matrices $M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 4 & 2 & 1 \end{pmatrix}$ et $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Partie A

1. Déterminer la matrice M^2. On donne $M^3 = \begin{pmatrix} 20 & 10 & 11 \\ 12 & 2 & 9 \\ 42 & 20 & 21 \end{pmatrix}$.
2. Vérifier que $M^3 = M^2 + 8M + 6I$.
3. En déduire que M est inversible et que $M^{-1} = \frac{1}{6}\left(M^2 - M - 8I\right)$.

Partie B Étude d'un cas particulier

On cherche à déterminer trois nombres entiers a, b et c tels que la parabole d'équation $y = ax^2 + bx + c$ passe par les points A(1 ; 1), B(−1 ; −1) et C(2 ; 5).

1. Démontrer que le problème revient à chercher trois entiers a, b et c tels que
$$M\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}.$$
2. Calculer les nombres a, b et c et vérifier que ces nombres sont des entiers.

Partie C Retour au cas général

Les nombres a, b, c, p, q, r sont des entiers.
Dans un repère $\left(O, \vec{\imath}, \vec{\jmath}\right)$, on considère les points A(1 ; p), B(−1 ; q) et C(2 ; r).
On cherche des valeurs de p, q et r pour qu'il existe une parabole d'équation $y = ax^2 + bx + c$ passant par A, B et C.

1. Démontrer que si $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = M^{-1}\begin{pmatrix} p \\ q \\ r \end{pmatrix}$ avec a, b et c entiers, alors
$$\begin{cases} -3p + q + 2r & \equiv & 0\,[6] \\ 3p - 3q & \equiv & 0\,[6] \\ 6p + 2q - 2r & \equiv & 0\,[6] \end{cases}$$
2. En déduire que $\begin{cases} q - r & \equiv & 0\,[3] \\ p - q & \equiv & 0\,[2] \end{cases}$.
3. Réciproquement, on admet que si $\begin{cases} q - r & \equiv & 0\,[3] \\ p - q & \equiv & 0\,[2] \\ \text{A, B, C ne sont pas alignés} \end{cases}$
alors il existe trois entiers a, b et c tels que la parabole d'équation $y = ax^2 + bx + c$ passe par les points A, B et C.
   a. Montrer que les points A, B et C sont alignés si et seulement si $2r + q - 3p = 0$.
   b. On choisit $p = 7$. Déterminer des entiers q, r, a, b et c tels que la parabole d'équation $y = ax^2 + bx + c$ passe par les points A, B et C.

Ex 9-19 : ***Baccalauréat S Centres étrangers 8 juin 2016 – ex 4***

Chiffrement de Hill : Congruences – Bézout - Matrices

Le but de cet exercice est d'étudier, sur un exemple, une méthode de chiffrement publiée en 1929 par le mathématicien et cryptologue Lester Hill. Ce chiffrement repose sur la donnée d'une matrice A, connue uniquement de l'émetteur et du destinataire.

Dans tout l'exercice, on note A la matrice définie par : $A = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$.

Partie A – Chiffrement de Hill

Voici les différentes étapes de chiffrement pour un mot comportant un nombre pair de lettres :

Étape 1	On divise le mot en blocs de deux lettres consécutives puis, pour chaque bloc, on effectue chacune des étapes suivantes.
Étape 2	On associe aux deux lettres du bloc les deux entiers x_1 et x_2 tous deux compris entre 0 et 25, qui correspondent aux deux lettres dans le même ordre, dans le tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Étape 3	On transforme la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ vérifiant $Y = AX$.
Étape 4	On transforme la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, où r_1 est le reste de la division euclidienne de y_1 par 26 et r_2 celui de la division euclidienne de y_2 par 26.
Étape 5	On associe aux entiers r_1 et r_2 les deux lettres correspondantes du tableau de l'étape 2. Le bloc chiffré est le bloc obtenu en juxtaposant ces deux lettres.

Question : utiliser la méthode de chiffrement exposée pour chiffrer le mot « HILL ».

Partie B - Quelques outils mathématiques nécessaires au déchiffrement

1. Soit a un entier relatif premier avec 26.
   Démontrer qu'il existe un entier relatif u tel que $u \times a \equiv 1$ modulo 26.
2. On considère l'algorithme suivant :

```
from math import *
a=int(input("a="))
u=0
r=0
while (r!=1):
    u=u+1
    r=(u*a)%26
print(u)
```

Partie C - Déchiffrement

On veut déchiffrer le mot VLUP.

On note $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ la matrice associée, selon le tableau de correspondance, à un bloc de deux lettres avant chiffrement, et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ la matrice définie par l'égalité : $Y = AX = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} X$.

Si r_1 et r_2 sont les restes respectifs de y_1 et y_2 dans la division euclidienne par 26, le bloc de deux lettres après chiffrement est associé à la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$.

1. Démontrer que : $\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$
2. En utilisant la question B .2., établir que : $\begin{cases} x_1 \equiv 9r_1 + 16r_2 \text{ modulo } 26 \\ x_2 \equiv 17r_1 + 25r_2 \text{ modulo } 26 \end{cases}$
3. Déchiffrer le mot VLUP, associé aux matrices $\begin{pmatrix} 21 \\ 11 \end{pmatrix}$ et $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

Ex 9-20 : ***Baccalauréat S Métropole sept 2017 – ex 4***

Points de coordonnées entières dans l'espace : Équations diophantiennes - Matrices

Dans l'espace rapporté à un repère orthonormé $\left(O, \vec{\imath}, \vec{\jmath}, \vec{k}\right)$, on considère les points A(1 ; 5 ; −2), B(7 ; −1 ; 3) et C(−2 ; 7 ; −2) et on note $\mathscr{P}$ le plan (ABC).
On cherche une équation cartésienne du plan $\mathscr{P}$ sous la forme : $ax + by + cz = 73$, où a, b et c sont des nombres réels.

On note X et Y les matrices colonnes : $X = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ et $Y = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

1. Montrer que X vérifie la relation : $MX = 73Y$, où M est la matrice
$M = \begin{pmatrix} 1 & 5 & -2 \\ 7 & -1 & 3 \\ -2 & 7 & -2 \end{pmatrix}$.

2. Soit N la matrice : $N = \begin{pmatrix} 19 & 4 & -13 \\ -8 & 6 & 17 \\ -47 & 17 & 36 \end{pmatrix}$.
À l'aide d'une calculatrice, on a calculé les produits $M \times N$ et $N \times M$, et on a obtenu les copies d'écran suivantes :

Pour $M \times N$:

Ans	1	2	3
1	73	0	0
2	0	73	0
3	0	0	73

Pour $N \times M$:

Ans	1	2	3
1	73	0	0
2	0	73	0
3	0	0	73

À l'aide de ces informations, justifier que la matrice M est inversible et exprimer sa matrice inverse M^{-1} en fonction de la matrice N.

3. Montrer alors que : $X = NY$.
En déduire que le plan $\mathscr{P}$ admet pour équation cartésienne :
$10x + 15y + 6z = 73$.

Partie B

L'objectif de cette partie est l'étude des points à coordonnées entières du plan $\mathscr{P}$ ayant pour équation cartésienne : $10x + 15y + 6z = 73$.

1. Soit $M(x\,;\,y\,;\,z)$ un point appartenant au plan $\mathscr{P}$ et au plan d'équation $z = 3$. On suppose que les coordonnées x, y et z appartiennent à l'ensemble $\mathbb{Z}$ des entiers relatifs.
   a. Montrer que les entiers x et y sont solutions de l'équation
   $(E) : 2x + 3y = 11$.
   b. Justifier que le couple $(7\,;\,-1)$ est une solution particulière de (E) puis résoudre l'équation (E) pour x et y appartenant à $\mathbb{Z}$.
   c. Montrer qu'il existe exactement deux points appartenant au plan $\mathscr{P}$ et au plan d'équation $z = 3$ et dont les coordonnées appartiennent à l'ensemble $\mathbb{N}$ des entiers naturels. Déterminer les coordonnées de ces deux points.

2. Dans cette question, on se propose de déterminer tous les points $M(x\,;\,y\,;\,z)$ du plan $\mathscr{P}$ dont les coordonnées sont des entiers naturels.
   Soient x, y et z des entiers naturels tels que $10x + 15y + 6z = 73$.
   a. Montrer que y est impair.
   b. Montrer que : $x \equiv 1 \quad [3]$. On admet que : $z \equiv 3 \quad [5]$.
   c. On pose alors : $x = 1 + 3p$, $y = 1 + 2q$ et $z = 3 + 5r$, où p, q et r sont des entiers naturels.
   Montrer que le point $M(x\,;\,y\,;\,z)$ appartient au plan $\mathscr{P}$ si et seulement si $p + q + r = 1$.
   d. En déduire qu'il existe exactement trois points du plan $\mathscr{P}$ dont les coordonnées sont des entiers naturels. Déterminer les coordonnées de ces points.

Ex 9-21 : ***Baccalauréat S Pondichéry avril 2016 – ex 3***

Cryptographie : Congruences – Gauss - Matrices

Partie A

On considère les matrices M de la forme $M = \begin{pmatrix} a & b \\ 5 & 3 \end{pmatrix}$ où a et b sont des nombres entiers.

Le nombre $3a - 5b$ est appelé le déterminant de M. On le note $\det(M)$.
Ainsi $\det(M) = 3a - 5b$.

1. Dans cette question on suppose que $\det(M) \neq 0$ et on pose $N = \dfrac{1}{\det(M)} \begin{pmatrix} 3 & -b \\ -5 & a \end{pmatrix}$.
   Justifier que N est l'inverse de M.
2. On considère l'équation (E) : $\det(M) = 3$.
   On souhaite déterminer tous les couples d'entiers $(a\,;\,b)$ solutions de l'équation (E).
   a. Vérifier que le couple $(6\,;\,3)$ est une solution de (E).
   b. Montrer que le couple d'entiers $(a\,;\,b)$ est solution de (E) si et seulement si $3(a-6) = 5(b-3)$.
   En déduire l'ensemble des solutions de l'équation (E).

Partie B

1. On pose $Q = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$.
   En utilisant la partie A, déterminer la matrice inverse de Q.
2. *Codage avec la matrice Q*
   Pour coder un mot de deux lettres à l'aide de la matrice $Q = \begin{pmatrix} 6 & 3 \\ 5 & 3 \end{pmatrix}$ on utilise la procédure ci-après :
   Étape 1 : On associe au mot la matrice $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ où x_1 est l'entier correspondant à la première lettre du mot et x_2 l'entier correspondant à la deuxième lettre du mot selon le tableau de correspondance ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

   Étape 2 : La matrice X est transformée en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ telle que $Y = QX$.
   Étape 3 : La matrice Y est transformée en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ telle que r_1 est le reste de la division euclidienne de y_1 par 26 et r_2 est le reste de la division euclidienne de y_2 par 26.
   Étape 4 : À la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ on associe un mot de deux lettres selon le tableau de correspondance de l'étape 1.

$$\text{Exemple : JE} \rightarrow X = \begin{pmatrix} 9 \\ 4 \end{pmatrix} \rightarrow Y = \begin{pmatrix} 66 \\ 57 \end{pmatrix} \rightarrow R = \begin{pmatrix} 14 \\ 5 \end{pmatrix} \rightarrow \text{OF.}$$

   Le mot JE est codé en le mot OF.
   Coder le mot DO.
3. *Procédure de décodage*
   On conserve les mêmes notations que pour le codage.
   Lors du codage, la matrice X a été transformée en la matrice Y telle que $Y = QX$.
   a. Démontrer que $3X = 3Q^{-1}Y$ puis que $\begin{cases} 3x_1 \equiv 3r_1 - 3r_2 & [26] \\ 3x_2 \equiv -5r_1 + 6r_2 & [26] \end{cases}$
   b. En remarquant que $9 \times 3 \equiv 1 \quad [26]$, montrer que $\begin{cases} x_1 \equiv r_1 - r_2 & [26] \\ x_2 \equiv 7r_1 + 2r_2 & [26] \end{cases}$
   c. Décoder le mot SG.

GRAPHES

1) GRAPHES NON-ORIENTÉS

A ; B ; C ; D ; E et F sont 6 poissons.

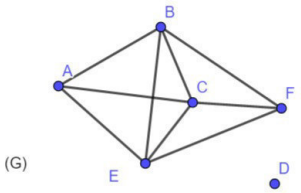
Dans le tableau ci-dessous, une croix indique que
les poissons ne peuvent pas cohabiter dans le même aquarium.

	A	B	C	D	E	F
A		×	×		×	
B	×		×		×	×
C	×	×			×	×
D						
E	×	×	×			×
F		×	×		×	

On peut représenter la situation de la façon suivante :

- Chaque poisson est représenté par un point.

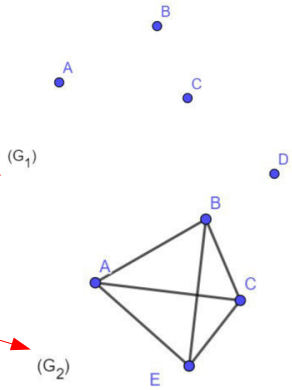
- 2 poissons qui ne peuvent pas cohabiter sont reliés



Définitions :

- Un **graphe non-orienté** G est un ensemble de sommets reliés par des arrêtes.
- Les points A ; B ; C ; D ; E et F sont **les sommets** du graphe.
- **L'ordre** d'un graphe est le nombre total de sommets.
- Les segments reliant deux sommets sont **des arêtes**.
- Deux sommets sont **adjacents** lorsqu'ils sont reliés par une arête.
- Une arête reliant deux sommets est dite **incidente** à ces deux sommets.
- Une arête est une **boucle** si elle relie un sommet à lui-même.

- **Le degré d'un sommet** est le nombre d'arêtes dont ce sommet est une extrémité. (Une boucle compte double)
- Un sommet est **isolé** lorsqu'il n'est relié à aucun autre sommet.
- Un graphe est **simple** si au plus une arête relie deux sommets et s'il n'y a pas de boucle sur un sommet.
- **Un sous graphe** (G') de (G) est un graphe composé de certains sommets et de toutes les arêtes qui relient ces sommets.
- Un graphe (G) ou un sous graphe (G_1) de (G) est **stable** lorsqu'il ne contient aucune arête.
- Un graphe (G) ou un sous graphe (G_2) de (G) est **complet** lorsque ses sommets sont deux à deux adjacents.



Exemple :

Propriété :

- La somme S des degrés des sommets d'un graphe est égale à deux fois le nombre d'arêtes a du graphe. $S=2\times a$
- Dans un graphe simple non-orienté le nombre de sommets de degré impair est pair.

Exemple :

Sommet	A	B	C	D	E	F
Degré						

2) PARCOURIR UN GRAPHE NON-ORIENTÉS

A) CHAÎNE

Définitions :

- **Une chaîne** d'un graphe est une liste ordonnée de sommets telle que chaque sommet soit adjacent au suivant.
- **La longueur** d'une chaîne est égale au nombre d'arêtes qui la composent.
- **Une chaîne est fermée** lorsque son origine et son extrémité sont confondues.
- **Un cycle** est une chaîne fermée dont les arêtes sont distinctes.
- Un graphe est **connexe** si deux sommets distincts quelconques peuvent être reliés par une chaîne.
- **La distance** entre deux sommets d'un graphe est la plus petite longueur des chaînes qui les relient.
- **Le diamètre d'un graphe** est la plus grande distance (par le plus court chemin) entre deux sommets.

Exemple :

- La chaîne C-D-E-F-G est une chaîne de longueur

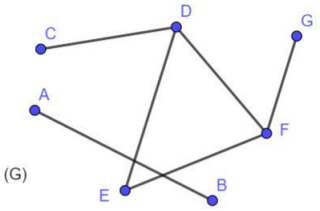
- E-D-G

- La chaîne C-D-E-F-D-C

- Le graphe (G) est d'ordre

- La chaîne E-D-F-E est un cycle de longueur

- La distance entre les sommets C et E vaut Le diamètre du graphe (G) vaut

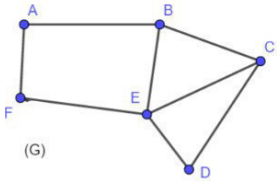


B) CHAÎNE EULÉRIENNE

Définitions :

- Une chaîne est **eulérienne** lorsqu'elle contient une et une seule fois chaque arête du graphe.
- **Un cycle eulérien** est une chaîne eulérienne fermée.

Exemple :



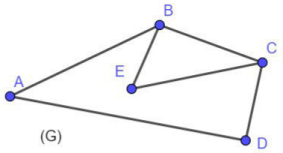
Théorème d'Euler : (admis)

Dans la cas d'un graphe non-orienté, un graphe connexe admet une chaîne eulérienne si et seulement si le nombre de sommets de degré impair vaut 0 ou 2.

Conséquences :

- Pour qu'un graphe connexe (G) admette un cycle eulérien, il faut et il suffit que tous les sommets de (G) soient de degré pair.
- Si le graphe connexe a deux sommets de degré impair, alors ce sont les extrémités de la chaîne eulérienne.
- Un graphe ayant plus de deux sommets de degré impair ne possède pas de chaîne eulérienne.

Exemple :



3) GRAPHES ORIENTÉS

Définitions :

- **Un graphe orienté** est un graphe dont les arêtes sont orientées.
- Le sommet A et le sommet B d'une arête orientée reliant A à B s'appellent respectivement **l'origine** et **l'extrémité** de l'arête orientée A – B.
- On parle de **degré entrant** pour indiquer le nombre d'arcs se dirigeant vers le sommet et de **degré sortant** pour indiquer le nombre d'arcs partant du sommet.
- **Une chaîne orientée** d'un graphe orienté est une liste ordonnée de sommets telle que chaque sommet soit relié au suivant par l'arête orientée dont il est l'origine.

Dans la cas d'un graphe orienté, les arêtes sont aussi appelées **arcs** .

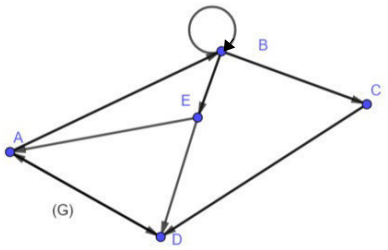
Exemple :

- (G) est un graphe orienté d'ordre

- L'arête orienté C-D a pour

- L'arête orienté

- Il y a reliant les sommets A et D.



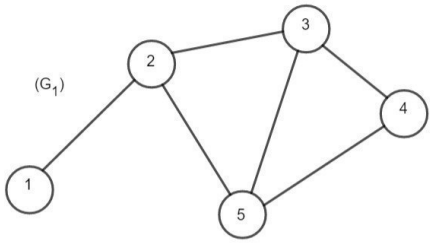
Remarque :

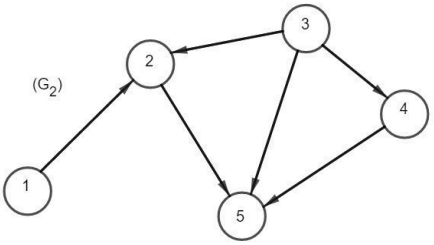
Hormis la notion de graphe complet et le théoème d'Euler, les définitions et les propriétés précédentes sont identiques pour les graphes orientés.

Définition :

On numérote les sommets d'un graphe orienté (G) d'ordre n .
La matrice carrée associée au graphe (G) (orienté ou non) est la matrice à n lignes et à n colonnes où le terme a_{ij} situé à l'intersection de la ligne i et de la colonne j est égal au nombre d'arêtes reliant le sommet i à j .
Cette matrice est appelée **matrice d'adjacence** du graphe.

Exemple :





La matrice d'adjacence de (G_1) est

La matrice d'adjacence de (G_2) est

Remarque :

La matrice d'adjacence d'un graphe non-orienté est le nombre d'arêtes reliant la sommet i au sommet j est bien sûr égal au nombre d'arêtes reliant le sommet j au sommet i .

Propriété :

Soit M la matrice d'ordre n associée à un graphe (G) et un entier naturel non nul k .
Le terme de la matrice M^k situé à l'intersection de la ligne i et de la colonne j est égal au nombre de chaînes de longueur k reliant le sommet i au sommet j .

Preuve : ***exigible***

Soit la propriété P(k) : "Le terme de la matrice M^k situé à l'intersection de la ligne i et de la colonne j est égal au nombre de chaînes de longueur k reliant le sommet i au sommet j ", pour $k \geq 1$ (HR)
Démontrons par récurrence que cette propriété est vraie pour tout entier $k \geq 1$.

Initialisation :
Par définition, le terme a_{ij} de la matrice M situé à l'intersection de la ligne i et de la colonne j est égal au nombre d'arêtes reliant i à j. Il est bien égal au nombre de chaînes de longueur 1 reliant i à j.
P(1) est donc vraie.

Hérédité :
Supposons P(k) vraie pour un entier $k \geq 1$ fixé, c'est à dire, le terme (que nous notons ici b_{ij}) de la matrice M^k situé à l'intersection de la ligne i et de la colonne j est égal au nombre de chaînes de longueur k reliant le sommet i au sommet j

Montrons que la propriété P(k+1) est vraie, c'est à dire , Le terme (que nous notons ici c_{ij}) de la matrice M^{k+1} situé à l'intersection de la ligne i et de la colonne j est égal au nombre de chaînes de longueur $k+1$ reliant le sommet i au sommet j

Puisque $M^{k+1}=M\times M^k$, alors $c_{ij}=a_{i1}\times b_{1j}+\ldots+a_{iq}\times b_{qj}+\ldots+a_{in}\times b_{nj}$.
- Si $a_{iq}\times b_{qj}\neq 0$, alors $a_{iq}=1$ et $b_{qj}=s$ où s est le nombre non nul de chaînes de longueur k reliant q à j .
Il existe alors s chaînes de longueur $k+1$ reliant i à j et dont le deuxième sommet est q .

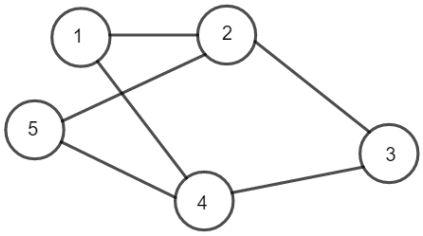
- Si $a_{iq}\times b_{qj}=0$, alors $a_{iq}=0$ ou $b_{qj}=0$. Il n'existe pas de chaîne de longueur $k+1$ reliant i à j et dont le deuxième sommet est q .
En considérant un à un les nombres q , c_{ij} est le nombre de chaînes de longueur $k+1$ reliant i à j .
P$(k+1)$ est donc vraie.

Conclusion :

Pour tout $k \geqslant 1$, le terme de la matrice M^k situé à l'intersection de la ligne i et de la colonne j est égal au nombre de chaînes de longueur k reliant le sommet i au sommet j

Exemple :

(G)



La matrice d'adjacence de (G) est M=

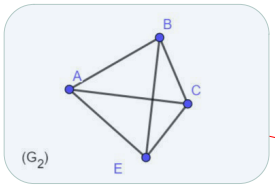
On a $M^2=$ $M^3=$

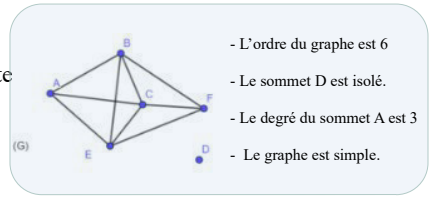
-

-

-

Graphes non-orientés :





- L'ordre du graphe est 6
- Le sommet D est isolé.
- Le degré du sommet A est 3
- Le graphe est simple.

- Un **graphe non-orienté** G est un ensemble de sommets reliés par des arrêtes
- Les points A ; B ; C ; D ; E et F sont **les sommets** du graphe.
- **L'ordre** d'un graphe est le nombre total de sommets.
- Les segments reliant deux sommets sont **des arêtes**.
- Deux sommets sont **adjacents** lorsqu'ils sont reliés par une arête.
- Une arête reliant deux sommets est dite **incidente** à ces deux sommets.

- Une arête est une **boucle** si elle relie un sommet à lui-même.
- **Le degré d'un sommet** est le nombre d'arêtes dont ce sommet est une extrémité. (Une boucle compte double)
- Un sommet est **isolé** lorsqu'il n'est relié à aucun autre sommet.
- Un graphe est **simple** si au plus une arête relie deux sommets et s'il n'y a pas de boucle sur un sommet.
- **Un sous graphe** (G') de (G) est un graphe composé de certains sommets et de toutes les arêtes qui relient ces sommets.
- Un graphe (G) ou un sous graphe (G_1) de (G) est **stable** lorsqu'il ne contient aucune arête.
- Un graphe (G) ou un sous graphe (G_2) de (G) est **complet** lorsque ses sommets sont deux à deux adjacents.

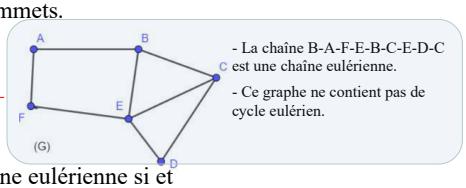
Propriété :

- **La somme S des degrés** des sommets d'un graphe est égale à deux fois le nombre d'arêtes a du graphe
- Dans un graphe simple non-orienté l**e nombre de sommets de degré impair** est pair.

Parcourir un graphe non-orienté :

- **Une chaîne** d'un graphe est une liste ordonnée de sommets telle que chaque sommet soit adjacent au suivant.
- **La longueur** d'une chaîne est égale au nombre d'arêtes qui la composent.
- **Une chaîne est fermée** lorsque son origine et son extrémité sont confondues.
- **Un cycle** est une chaîne fermée dont les arêtes sont distinctes.
- Un graphe est **connexe** si deux sommets distincts quelconques peuvent être reliés par une chaîne.
- **La distance** entre deux sommets d'un graphe est la plus petite longueur des chaînes qui les relient.
- **Le diamètre d'un graphe** est la plus grande distance entre deux sommets.

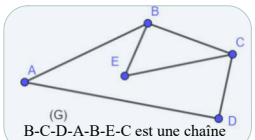
Chaîne eulérienne :



- La chaîne B-A-F-E-B-C-E-D-C est une chaîne eulérienne.
- Ce graphe ne contient pas de cycle eulérien.

- Une chaîne est **eulérienne** lorsqu'elle contient une et une seule fois chaque arête du graphe.
- **Un cycle eulérien** est une chaîne eulérienne fermée.

Théorème d'Euler :

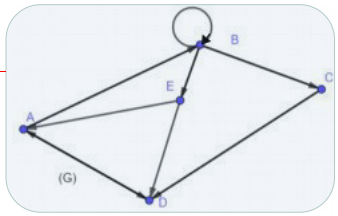


B-C-D-A-B-E-C est une chaîne eulérienne.

Dans la cas d'un graphe non-orienté, un graphe connexe admet une chaîne eulérienne si et seulement si **le nombre de sommets de degré impair vaut 0 ou 2**.

- Pour qu'un graphe connexe (G) admette **un cycle eulérien**, il faut et il suffit que tous les sommets de (G) soient de **degré pair**.
- Si le graphe connexe a deux sommets de degré impair, alors ce sont **les extrémités de la chaîne eulérienne**.
- Un graphe ayant plus de deux sommets de degré impair ne possède pas de chaîne eulérienne.

Graphes orientés :



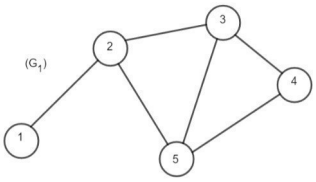
- **Un graphe orienté** est un graphe dont les arêtes (ou **arcs**) sont orientées.
- Le sommet A et le sommet B d'une arête orientée reliant A à B s'appellent respectivement **l'origine** et **l'extrémité** de l'arête orientée A – B.
- On parle de **degré entrant** pour indiquer le nombre d'arcs se dirigeant vers le sommet et de **degré sortant** pour indiquer le nombre d'arcs partant du somme
- **Une chaîne orientée** d'un graphe orienté est une liste ordonnée de sommets telle que chaque sommet soit relié au suivant par l'arête orientée dont il est l'origine.

Matrice d'adjacence :

On numérote les sommets d'un graphe orienté (G) d'ordre n .
La matrice carrée associée au graphe (G) (orienté ou non) est la matrice à n lignes et à n colonnes où le terme a_{ij} situé à l'intersection de la ligne i et de la colonne j est égal au nombre d'arêtes reliant le sommet i à j .
Cette matrice est appelée **matrice d'adjacence** du graphe.

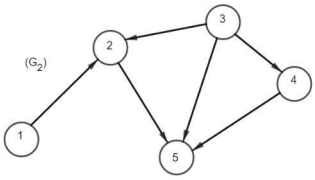
Exemple :

La matrice d'adjacence d'un graphe non-orienté est symétrique



La matrice d'adjacence de (G_1) est $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

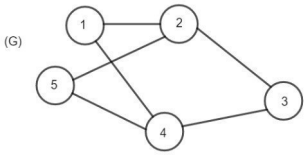
La matrice d'adjacence de (G_2) est $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$



Nombre de chaînes de longueur k :

Soit M la matrice d'ordre n associée à un graphe (G) et un entier naturel non nul k .
Le terme de la matrice M^k situé à l'intersection de la ligne i et de la colonne j est égal au nombre de chaînes de longueur k reliant le sommet i au sommet j .

Exemple :



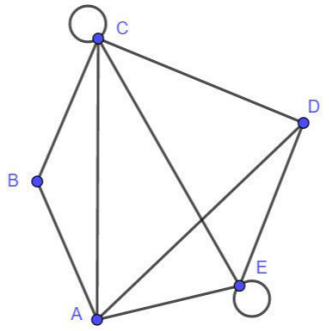
$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$ $M^2 = \begin{pmatrix} 2 & 0 & 2 & 0 & 2 \\ 0 & 3 & 0 & 3 & 0 \\ 2 & 0 & 2 & 0 & 2 \\ 0 & 3 & 0 & 3 & 0 \\ 2 & 0 & 2 & 0 & 2 \end{pmatrix}$ $M^3 = \begin{pmatrix} 0 & 6 & 0 & 6 & 0 \\ 6 & 0 & 6 & 0 & 6 \\ 0 & 6 & 0 & 6 & 0 \\ 6 & 0 & 6 & 0 & 6 \\ 0 & 6 & 0 & 6 & 0 \end{pmatrix}$

Il existe 6 chaînes de longueur 3 reliant le sommet 2 au sommet 3.

Graphes non-orientés

Ex 10-1 :

On considère le graphe ci-contre :



1) Quel est l'ordre du graphe ?

2) Ce graphe est-il simple ?

3) compléter le tableau ci-dessous :

Sommet	A	B	C	D	E
Degré					

4) Combien vaut la somme des degrés des sommets de ce graphe ?

En déduire le nombre d'arêtes du graphe.

5) Les sommets B et D sont-ils adjacents ?

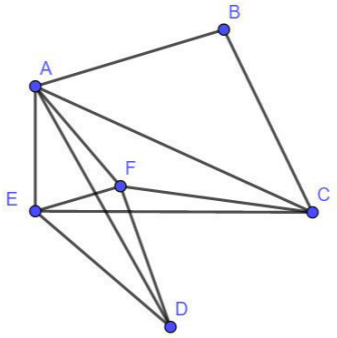
6) Dessiner le sous-graphe ADC.

Quel est son ordre ?

Combien possèdes-t-il d'arêtes ?

Ex 10-2 :

On considère le graphe ci-contre



1) Quel est l'ordre du graphe ?

2) Ce graphe est-il simple ?

3) Ce graphe est-il complet ?

4) Déterminer un sous-graphe complet d'ordre 4.

5) Déterminer un sous-graphe complet d'ordre 3 . Quel est le degré de chacun de ses sommets ?

Ex 10-3 : ***Fête d'anniversaire***

Alexandre aimerait inviter 5 amis (notés A,B,C,D et E) pour son anniversaire, mais certains ne s'entendent pas.

amis	A	B	C	D	E
Ne s'entendent pas	D	C D E	B	A B E	B D

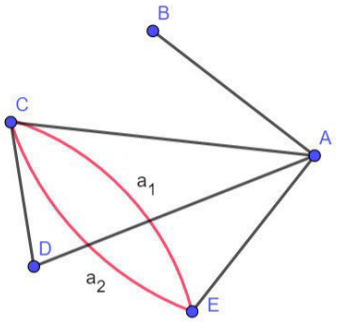
Combien Alexandre peut-il inviter d'amis à son anniversaire pour que la fête soit réussie ?

Ex 10-4 : ***Rencontres sportives***

Lors de rencontres sportives, il y a 7 équipes de basketball représentant 7 établissement différents.
Les professeurs d'EPS aimeraient organiser des rencontres de telle sorte que chaque équipe en rencontre trois autres.
Est-ce possible ?

Ex 10-5 : ***Graphe connexe ?***

On considère le graphe ci-contre



1) Quel est l'ordre du graphe ?

2) Ce graphe est-il simple ?

3) Ce graphe est-il connexe ?

4) Quelle est la distance entre B et C.

5) Quel est le diamètre du graphe ?

6) On considère la chaîne $B-A-C-a_1-E-A-B$

a) Déterminer sa longueur.

b) Est-ce une chaîne fermée ?

c) Est-ce un cycle ?

Ex 10-6 : ***Sommets de même degré***

1) a) Essayer de construire un graphe simple (non orienté) ayant au moins deux sommets et tel que tous les sommets ont des degrés distincts ?

b) Que peut-on conjecturer ?

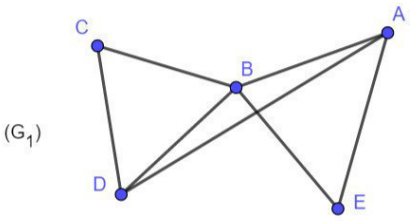
c) En faisant un raisonnement par l'absurde, démontrer la conjecture précédente.

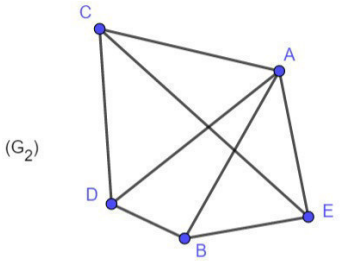
2) Montrer que dans un groupe de personnes, il y a toujours deux personnes ayant le même nombre d'amis présents.

Parcourir un graphe non-orienté

Ex 10-7 :

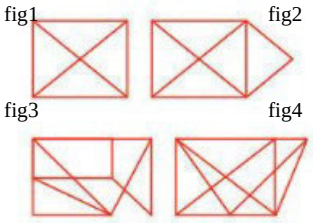
Peut-on dessiner en ne passant qu'une seule fois par chaque arête les graphes ci-dessous ?





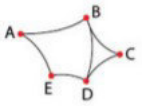
Ex 10-8 : ***Tracer une figure sans lever le crayon***

Est-il possible de tracer les graphes suivant sans lever le crayon et sans passer deux fois sur le même trait ?



Ex 10-9 : ***Extrémités d'une chaîne eulérienne***

Dans un parc, il y a cinq bancs reliés entre eux par des allées.
On modélise les bancs par les sommets A, B, C, D E et les allées par les arêtes du graphe ci-dessous.

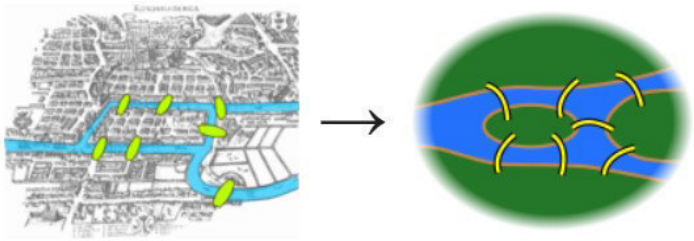


1) Est-il possible de parcourir toutes les allées de ce parc sans passer deux fois par la même allée ?

2) Amine est assis sur le banc A . Peut-il parcourir toutes les allées de ce parc sans passer deux fois par la même allée ?

Ex 10-10 : ***Problème des sept ponts de Königsberg***
https://fr.wikipedia.org/wiki/Probl%C3%A8me_des_sept_ponts_de_K%C3%B6nigsberg

La ville de Königsberg (aujourd'hui Kaliningrad) est construite autour de deux îles situées sur le Pregel et reliées entre elles par un pont. Six autres ponts relient les rives de la rivière à l'une ou l'autre des deux îles, comme représentés sur le plan ci-dessus. Le problème consiste à déterminer s'il existe ou non une promenade dans les rues de Königsberg permettant, à partir d'un point de départ au choix, de passer une et une seule fois par chaque pont, et de revenir à son point de départ, étant entendu qu'on ne peut traverser le Pregel qu'en passant sur les ponts.



1) Dessiner un graphe représentant la situation.

2) Est-il possible de se promener dans les rues de Königsberg en passant une et une seule fois par chaque pont ?

Ex 10-11 : ***Traverser une seule fois la frontière***

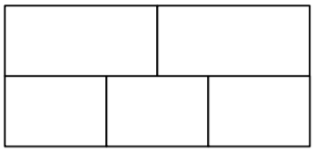
Un voyageur visite ces six pays d'Asie.
Il aimerait traverser une fois et une seule chaque frontières.

1) Dessiner un graphe représentant la situation.

2) Est-il possible de traverser une fois et une seule chaque frontière ?

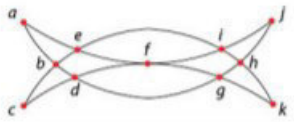
Ex 10-12 : ***Couper 16 segments***

Est-il possible de tracer une courbe, sans lever le crayon, qui coupe chacun des 16 segments de la figure suivante ?



Ex 10-13 : ***Signature de Mahomet et cycle eulérien***

La signature de Mahomet est formée de deux croissants opposés comme sur le dessin ci-dessous.



On raconte qu'il la traçait sans lever la pointe de son cimeterre.
Est-ce possible ? Si oui, proposer une manière de faire.

Ex 10-14 : ***Ajouter un sommet et des arêtes pour trouver un cycle eulérien***

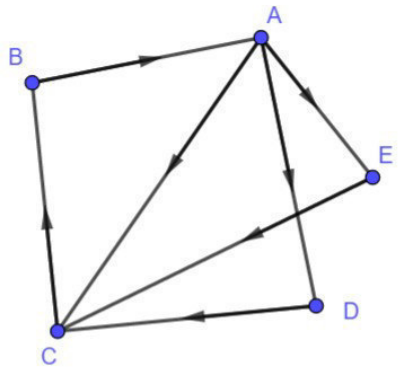
Soit G un graphe connexe ne possédant pas de cycle eulérien.

Est-il toujours possible, en rajoutant un sommet et quelques arêtes, de transformer G en un graphe possédant un cycle eulérien?

Graphe orienté

Ex 10-15 :

On considère le graphe orienté ci-dessous :



1) Quel est l'ordre du graphe ?

2) Quel est le degré entrant du sommet C et le degré sortant du sommet A ?

3) Déterminer une chaîne de longueur 3 reliant les sommets A et B.

Ex 10-16 : ***Relation « être diviseur de »***

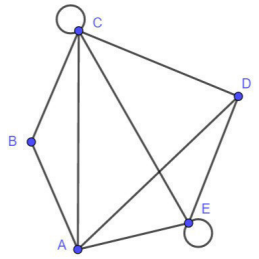
Construire un graphe orienté dont les sommets sont les entiers compris entre 1 et 12 et dont les arcs représentent la relation « être diviseur de ».

Matrice d'adjacence

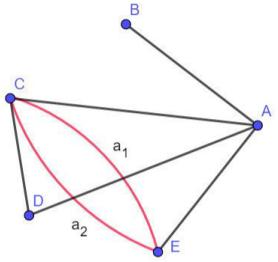
Ex 10-17 :

Dans chacun des cas déterminer la matrice d'adjacence associée aux graphes donnés (en considérant les sommets dans l'ordre alphabétique)

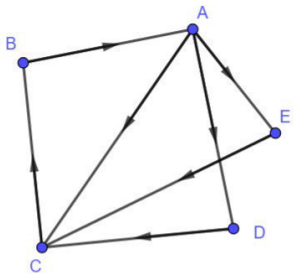
1)



2)



3)



Ex 10-18 :

On considère la matrice d'adjacence d'un graphe (G) :

$$M=\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

1) Déterminer l'ordre du graphe.

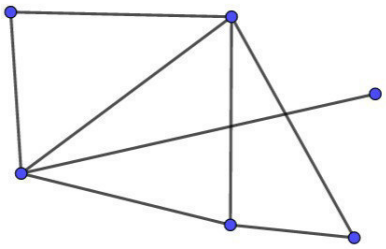
2) Le graphe (G) est-il orienté ?

3) Dessiner un graphe possible.

Ex 10-19 :

1) Déterminer les sommets A,B,C,D,E et F du graphe ci dessous, sachant que la matrice d'adjacence associée, en prenant les sommets par ordre alphabétique est :

$$M=\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$



2) Déterminer à l'aide de la calculatrice les matrices M^3 et M^5 .

3) En déduire le nombre de chaînes de longueur 3 reliant A à C et le nombre de chaînes de longueur 5 reliant C à E.

Ex 10-20 : ***Nombres élégants***

Un nombre est dit élégant si la différence entre deux chiffres consécutifs est d'au plus 1.
Le but du problème est de déterminer le nombre de nombres élégants à 8 chiffres, dont les chiffres sont tous compris entre 0 et 4 (inclus) ?

1) On construit un nombre élégant en concaténant les chiffres un à un. Compléter les pointillés ci-dessous :

- 0 est suivi de ...
- 1 est suivi de ...
- 2 est suivi de ...
- 3 est suivi de …
- 4 est suivi de …

2) Construire le graphe dont les sommets sont les chiffres de 0 à 4, et tel qu'il y ait une arête entre deux sommets si la différence entre les sommets vaut au plus 1.

3) Déterminer la matrice d'adjacence du graphe.

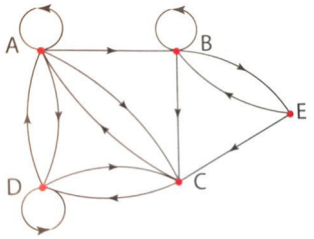
4) Un nombre élégant à 8 chiffres correspond à une suite de 8 sommets reliés par des arêtes, soit 8 sommets qui forment une chaîne. Mais, comme il y a 8 sommets, il n'y a besoin que de 7 arêtes pour parcourir la chaîne.

a) Déterminer le nombre de nombres élégants commençant par 2 et finissant par 4.

b) Comment obtenir le nombre de nombres élégants à 8 chiffres, dont les chiffres sont tous compris entre 0 et 4 (inclus) ?

Ex 10-21 : ***Niveaux d'un jeu vidéo***

Un jeu vidéo est composé de cinq niveaux A,B,C,D et E.
Le graphe ci-dessous représente les différentes possibilités pour passer d'un niveau à l'autre (éventuellement le même).



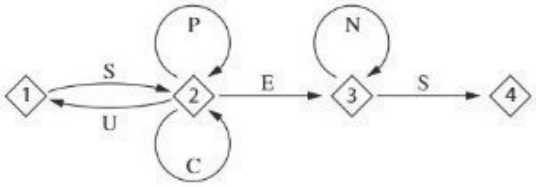
1) En considérant les sommets dans l'ordre alphabétique, déterminer la matrice d'adjacence du graphe.

2) Combien existe-t-il de chaînes de longueur 4 allant de C à E ? Déterminer ces chaînes.

3) Un joueur passe quatre niveaux et se retrouve … sur le même niveau ! De combien de façons différentes cette situation peut-elle arriver ?

Ex 10-22 : ***Code de messagerie***

Pour accéder à sa messagerie, Camille a choisi un code qui doit être reconnu par le graphe étiqueté ci-dessous de sommets 1,2,3 et 4.



Une succession de lettres constitue un code possible si les lettres se succèdent sur un chemin du graphe orienté en partant du sommet 1 et en sortant au sommet 4
Le code SENS et un code possible, alors que SUN n'est pas possible.

1) Parmi les trois codes ci-dessous, lequel est reconnu par le graphe.

SCENES - SUCCES - SUSPENS

2) Déterminer la matrice d'adjacence associée au graphe.

3) Déterminer le nombre de codes de 4 lettres reconnus par le graphe. Quels sont ces codes ?

MATRICES - QUELQUES UTILISATIONS

1) SUITES DE MATRICES

Définitions :

Soit un entier naturel n .

- On appelle **suite de matrices colonnes** (U_n) , des matrices colonnes dont tous les éléments sont des termes de suites numériques.
- On dit que (U_n) **converge** si et seulement si tous ses éléments convergent. La limite de (U_n) est alors la matrice ayant pour coefficients les limites de chaque terme de (U_n) .

On définit de la même manière **une suite de matrices lignes**.

Dans les autres cas, on dit que la suite est divergente.

Exemple :

- La suite (U_n) définie par $\mathrm{U}_n=\begin{pmatrix} n^3 \\ 2-n \end{pmatrix}$ est une suite de matrices dont les coefficients sont les suites numériques (a_n) et (b_n) définies par $a_n=n^3$ et $b_n=2-n$.

- La suite (V_n) définie par $\mathrm{V}_n=\begin{pmatrix} \dfrac{1}{n+1} \\ 2+e^{-n} \end{pmatrix}$

Propriété :

Si A est une matrice carrée d'ordre $p\in\mathbb{N}$ et (U_n) une suite de matrices colonnes à p lignes telles que pour tout entier naturel n , $\mathrm{U}_{n+1}=\mathrm{A}\,\mathrm{U}_n$, alors :

$$\forall n\in\mathbb{N}\ ,\ \mathrm{U}_n=\mathrm{A}^n\mathrm{U}_0$$

Preuve :

Soit la propriété $\mathrm{P}(n)$: " $\mathrm{U}_n=\mathrm{A}^n\mathrm{U}_0$ ", pour $n\in\mathbb{N}$

Démontrons par récurrence que cette propriété est vraie pour tout $n\in\mathbb{N}$.

Initialisation :

Hérédité :

Supposons $\mathrm{P}(n)$ vraie pour un entier $n\in\mathbb{N}$ fixé, c'est à dire $\mathrm{U}_n=\mathrm{A}^n\mathrm{U}_0$ (HR)

Montrons que la propriété $\mathrm{P}(n+1)$ est vraie, c'est à dire

On a

Ainsi

On a donc démontré que $\mathrm{P}(n+1)$ est vraie.

Conclusion :

$\mathrm{P}(n)$ est vraie pour tout entier $n\in\mathbb{N}$, c'est à dire : $\forall n\in\mathbb{N}$, $\mathrm{U}_n=\mathrm{A}^n\mathrm{U}_0$

Exemple :

Soit (a_n) et (b_n) deux suites définies par $a_0=1$, $b_0=2$ et $\begin{cases} a_{n+1}=a_n+b_n \\ b_{n+1}=a_n-2\,b_n \end{cases}$, pour tout entier naturel n .

On considère la matrice $\mathrm{A}=\begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}$ et pour tout entier naturel n , on pose $\mathrm{U}_n=\begin{pmatrix} a_n \\ b_n \end{pmatrix}$.

Define $a=\begin{bmatrix} 1 & 1 \\ 1 & -2 \end{bmatrix}$ *Terminé*

Define $u0=\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ *Terminé*

$a^7\cdot u0$ $\begin{bmatrix} 171 \\ -531 \end{bmatrix}$

Propriété et définition : ***admise***

Soit A une matrice carrée d'ordre $p \in \mathbb{N}$, B une matrice colonne à p lignes et (U_n) une suite de matrices colonnes à p lignes, telles que pour tout entier naturel n , $U_{n+1} = A\,U_n + B$.

Si la suite (U_n) converge alors sa limite U est une matrice colonne vérifiant $U = AU + B$.

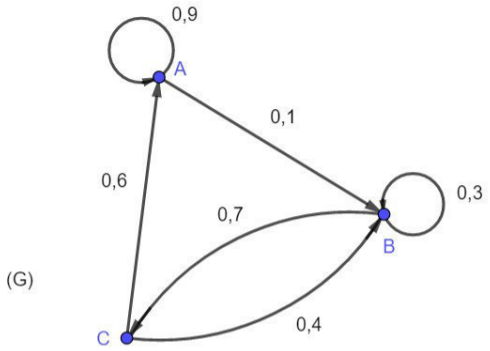
On dit que la matrice U est **l'état stable** de la suite (U_n)

2) CHAÎNES DE MARKOV

Définition :

- **Un graphe pondéré** est un graphe dont les arêtes sont affectées de coefficients positifs.
- **Le poids** d'une chaîne est la somme des coefficients affectés aux arêtes qui composent la chaîne.
- **Un graphe probabiliste** est un graphe orienté pondéré où tous les poids sont compris entre 0 et 1et tel que la somme des poids des arêtes issues d'un même sommet est égale à 1.

Exemple :



Définition :

La matrice associée à un graphe probabiliste comportant p sommets s'appelle **une matrice de transition.**

C'est une matrice carrée d'ordre p telle que le terme de la i -ème ligne et j -ième colonne est égal au poids de l'arête allant du sommet i au sommet j si elle existe , 0 sinon.

Si les sommets sont des lettres, on numérote les sommets en respectant l'ordre alphabétique.

Exemple : La matrice de transition du graphe (G) de l'exemple précédent est

Remarque :

Définition :

Soit une suite de variables aléatoires (X_n) permettant de modéliser l'évolution par étapes successives d'un système aléatoire comportant différents états.

La loi de probabilité de X_0 (étape 0) s'appelle **la distribution initiale du système.**

La loi de probabilité de X_n (étape n) s'appelle **la distribution après *n* transitions**.

Si, à chaque étape, la probabilité de transition d'un état à un autre ne dépend pas de n , on dit que la suite (X_n) est une **chaîne de Markov**.

On associe à une chaîne de Markov un graphe probabiliste tel que les sommets sont les états du système aléatoire et le poids de chaque arête est égal à la probabilité de transition d'un état à un autre.

3) CHAÎNES DE MARKOV : REPRÉSENTATION À L'AIDE D'UNE SUITE DE MATRICES

Propriété :

Soit une chaîne de Markov à 2 (respectivement 3) états et P la matrice de transition associée.

Soit trois entiers naturels n , i et j tels que $n \geqslant 1$, $1 \leqslant i \leqslant 2$ et $1 \leqslant j \leqslant 2$ (respectivement $1 \leqslant i \leqslant 3$ et $1 \leqslant j \leqslant 3$).

La probabilité de passer de l'état i à l'état j en n étapes est égale au terme de la i -ème et j -ième colonne de la matrice P^n .

Preuve : Démonstration pour une chaîne de Markov à 2 états.

Soit la propriété $Q(n)$: " $P^n = \begin{pmatrix} P_{X_0=1}(X_n=1) & P_{X_0=1}(X_n=2) \\ P_{X_0=2}(X_n=1) & P_{X_0=2}(X_n=2) \end{pmatrix}$ ", pour $n \in \mathbb{N}^*$

Démontrons par récurrence que cette propriété est vraie pour tout $n \in \mathbb{N}^*$.

Initialisation :

Pour $n=1$, on a par définition de la matrice de transition

Q(1) est donc vraie.

Hérédité :

Supposons $Q(n)$ vraie pour un entier $n \in \mathbb{N}$ fixé, c'est à dire $P^n = \begin{pmatrix} P_{X_0=1}(X_n=1) & P_{X_0=1}(X_n=2) \\ P_{X_0=2}(X_n=1) & P_{X_0=2}(X_n=2) \end{pmatrix}$ (HR)

Montrons que la propriété Q(n+1) est vraie, c'est à dire $P^{n+1} = \begin{pmatrix} & P_{X_0=1}(X_{n+1}=2) \\ P_{X_0=2}(X_{n+1}=1) & P_{X_0=2}(X_{n+1}=2) \end{pmatrix}$

Soit deux entiers naturels i et j tels que $1 \leqslant i \leqslant 2$ et $1 \leqslant j \leqslant 2$.

Dans un premier temps, on calcule la probabilité de passer de l'état à i à l'état j en $n+1$ transitions.

(Pour cette démonstration, on utilise le fait que $P_{X_0=i}$ est une probabilité)

Or $P^{n+1} = P^n P = \begin{pmatrix} {}_{=1}(X_n=2) \\ P_{X_0=2}(X_n=1) \quad P_{X_0=2}(X_n=2) \end{pmatrix} \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix}$ d'après (HR)

$$= \begin{pmatrix} P_{X_0=1}(X_n=1)\, p_{12} + P_{X_0=1}(X_n=2)\, p_{22} \\ P_{X_0=2}(X_n=1)\, p_{11} + P_{X_0=2}(X_n=2)\, p_{21} \quad P_{X_0=2}(X_n=1)\, p_{12} + P_{X_0=2}(X_n=2)\, p_{22} \end{pmatrix}$$

$$= \begin{pmatrix} P_{X_0=1}(X_{n+1}=2) \\ P_{X_0=2}(X_{n+1}=1) \quad P_{X_0=2}(X_{n+1}=2) \end{pmatrix}$$

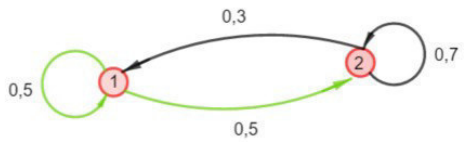
On a donc démontré que P(n+1) est vraie

Conclusion :

P(n) est vraie pour tout entier $n \in \mathbb{N}^*$, c'est à dire : $\forall n \in \mathbb{N}^*$, $P^n = \begin{pmatrix} P_{X_0=1}(X_n=1) & P_{X_0=1}(X_n=2) \\ P_{X_0=2}(X_n=1) & P_{X_0=2}(X_n=2) \end{pmatrix}$

Exemple :

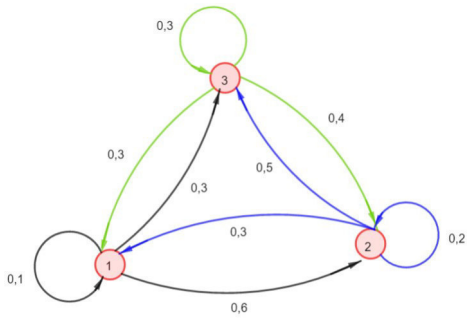
- On considère une marche aléatoire à deux états modélisée par le graphe probabiliste ci-dessous et P la matrice de transition associée.



Define $p = \begin{bmatrix} 0.5 & 0.5 \\ 0.3 & 0.7 \end{bmatrix}$ *Terminé*

p^4 $\begin{bmatrix} 0.376 & 0.624 \\ 0.3744 & 0.6256 \end{bmatrix}$

- On considère une marche aléatoire à trois états modélisée par le graphe probabiliste ci-dessous et P la matrice de transition associée.



Define $p=\begin{bmatrix}0.1 & 0.6 & 0.3\\ 0.3 & 0.2 & 0.5\\ 0.3 & 0.4 & 0.3\end{bmatrix}$ *Terminé*

p^3 $\begin{bmatrix}0.244 & 0.396 & 0.36\\ 0.252 & 0.364 & 0.384\\ 0.252 & 0.372 & 0.376\end{bmatrix}$

4) CHAÎNES DE MARKOV : ÉTUDE ASYMPTOTIQUE

Définition :

Soit une chaîne de Markov à 2 (respectivement 3) états et P la matrice de transition associée.

On note π_n la matrice ligne à 2 (respectivement 3) colonnes dont le terme de la j -ième colonne est la probabilité qu'à l'étape n la variable aléatoire X_n soit égalé à j , c'est à dire :

$$\pi_n=(P(X_n=1)\quad P(X_n=2))\quad (\text{ respectivement } \pi_n=(P(X_n=1)\quad P(X_n=2)\quad P(X_n=3))\ )$$

Remarque : π_0 représente la distribution initiale et π_n la distribution après n transitions.

Propriété :

Pour tout entier naturel $n\geqslant 1$, $\pi_{n+1}=\pi_n P$ et $\pi_n=\pi_0 P^n$.

P^n ne contient pas de 0 signifie qu'en n étapes on peut passer de n'importe quel état à n'importe quel autre état.

Preuve : ***Démonstration pour une chaîne de Markov à 2 états.*** *exigible*

Par définition de la matrice de transition $P=\begin{pmatrix}p_{11} & p_{12}\\ p_{21} & p_{22}\end{pmatrix}$ où $p_{ij}=P_{x_0=i}(X_1=j)$ (avec $i\in\{1;2\}$ et $j\in\{1;2\}$)

Soit un entier naturel n . On a :

On démontre de même que $P(X_{n+1}=2)=p_{12}P(X_n=1)+p_{22}P(X_n=2)$. On a donc bien $\pi_{n+1}=\pi_n P$

On suppose maintenant $n\geqslant 1$. On a déjà vu que $P^n=\begin{pmatrix}P_{X_0=1}(X_n=1) & P_{X_0=1}(X_n=2)\\ P_{X_0=2}(X_n=1) & P_{X_0=2}(X_n=2)\end{pmatrix}$.

On a alors $\pi_0 P^n=(P(X_0=1)\quad P(X_0=2))\begin{pmatrix}P_{X_0=1}(X_n=1) & P_{X_0=1}(X_n=2)\\ P_{X_0=2}(X_n=1) & P_{X_0=2}(X_n=2)\end{pmatrix}$

Propriété : ***admise***

S'il existe un entier naturel n tel que P^n ne contient pas de 0 alors la suite (π_n) converge vers la matrice π vérifiant $\pi=\pi P$ et cette limite ne dépend pas de π_0 .

La matrice π représente **la distribution invariante du système**.

Remarque : Si la matrice P ne contient pas de 0, alors la suite (π_n) converge.

Suites de Matrices :

On définit de la même manière **une suite de matrices lignes**.

- On appelle **suite de matrices colonnes** (U_n), des matrices colonnes dont tous les éléments sont des termes de suites numériques.
- On dit que (U_n) **converge** si et seulement si tous ses éléments convergent. La limite de (U_n) est alors la matrice ayant pour coefficients les limites de chaque terme de (U_n).

Propriété :

Si A est une matrice carrée d'ordre $p \in \mathbb{N}$ et (U_n) une suite de matrices colonnes à p lignes telles que pour tout entier naturel n, $U_{n+1} = A\,U_n$, alors :

$$\forall n \in \mathbb{N}, \quad U_n = A^n U_0$$

Propriété et définition :

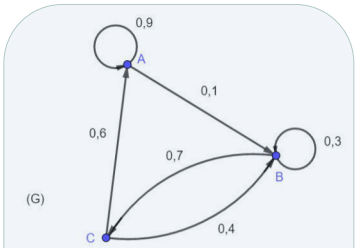
Soit A une matrice carrée d'ordre $p \in \mathbb{N}$, B une matrice colonne à p lignes et (U_n) une suite de matrices colonnes à p lignes, telles que pour tout entier naturel n, $U_{n+1} = A\,U_n + B$.

Si la suite (U_n) converge alors sa limite U est une matrice colonne vérifiant $U = AU + B$.

On dit que la matrice U est **l'état stable** de la suite (U_n)

Graphe probabiliste :

- **Un graphe pondéré** est un graphe dont les arêtes sont affectées de coefficients positifs.
- **Le poids** d'une chaîne est la somme des coefficients affectés aux arêtes qui composent la chaîne.
- **Un graphe probabiliste** est un **graphe orienté pondéré** où tous les poids sont compris entre 0 et 1et tel que la somme des poids des arêtes issues d'un même sommet est égale à 1.



(G) est un graphe prababiliste à trois états.

La matrice de transition du graphe (G) est

$$\begin{pmatrix} 0{,}9 & 0{,}1 & 0 \\ 0 & 0{,}3 & 0{,}7 \\ 0{,}6 & 0{,}4 & 0 \end{pmatrix}$$

La somme des termes de chaque ligne est égale à 1.

Matrice de transition :

Si les sommets sont des lettres, on numérote les sommets en respectant l'ordre alphabétique.

La matrice associée à un graphe probabiliste comportant p sommets s'appelle **une matrice de transition**.
C'est une matrice carrée d'ordre p telle que le terme de la i-ème ligne et j-ième colonne est égal au poids de l'arête allant du sommet i au sommet j si elle existe, 0 sinon.

Chaîne de Markov :

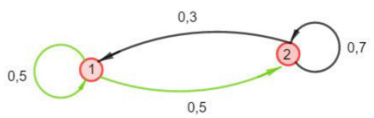
Soit une suite de variables aléatoires (X_n) permettant de modéliser l'évolution par étapes successives d'un système aléatoire comportant différents états.
La loi de probabilité de X_0 (étape 0) s'appelle **la distribution initiale du système**.
La loi de probabilité de X_n (étape n) s'appelle **la distribution après *n* transitions**.
Si, à chaque étape, la probabilité de transition d'un état à un autre ne dépend pas de n, on dit que la suite (X_n) est une **chaîne de Markov**.
On associe à une chaîne de Markov un graphe probabiliste tel que les sommets sont les états du système aléatoire et le poids de chaque arête est égal à la probabilité de transition d'un état à un autre.

Représentation à l'aide d'une suite de matrices :

Soit une chaîne de Markov à 2 (respectivement 3) états et P la matrice de transition associée.
Soit trois entiers naturels n, i et j tels que $n \geqslant 1$, $1 \leqslant i \leqslant 2$ et $1 \leqslant j \leqslant 2$ (respectivement $1 \leqslant i \leqslant 3$ et $1 \leqslant j \leqslant 3$).
La probabilité de passer de l'état i à l'état j en n étapes est égale au terme de la i-ème et j-ième colonne de la matrice P^n.

Exemple :

On considère une marche aléatoire à deux états modélisée par le graphe probabiliste ci-dessous et P la matrice de transition associée.



$$P = \begin{pmatrix} 0{,}5 & 0{,}5 \\ 0{,}3 & 0{,}7 \end{pmatrix}$$

Define $p = \begin{bmatrix} 0.5 & 0.5 \\ 0.3 & 0.7 \end{bmatrix}$ *Terminé*

p^4 $\begin{bmatrix} 0.376 & 0.624 \\ 0.3744 & 0.6256 \end{bmatrix}$

La probabilité de passer de l'état 1 à l'état 2 en 4 étapes 0,624

Chaîne de Markov : étude asymptotique :

π_0 représente la distribution initiale et π_n la distribution après n transitions.

Soit une chaîne de Markov à 2 (respectivement 3) états et P la matrice de transition associée.
On note π_n la matrice ligne à 2 (respectivement 3) colonnes dont le terme de la j-ième colonne est la probabilité qu'à l'étape n la variable aléatoire X_n soit égalé à j, c'est à dire :
$\pi_n = (P(X_n = 1) \quad P(X_n = 2))$ (respectivement $\pi_n = (P(X_n = 1) \quad P(X_n = 2) \quad P(X_n = 3))$)

Propriété :

Pour tout entier naturel $n \geqslant 1$, $\pi_{n+1} = \pi_n P$ et $\pi_n = \pi_0 P^n$.

Propriété : distribution invariante du système

P^n ne contient pas de 0 signifie qu'en n étapes on peut passer de n'importe quel état à n'importe quel autre état.

S'il existe un entier naturel n tel que P^n ne contient pas de 0 alors la suite (π_n) converge vers la matrice π vérifiant $\pi = \pi P$ et cette limite ne dépend pas de π_0.

La matrice π représente **la distribution invariante du système**.

Suites de matrices

Ex 11-1 :

On considère la suite de matrices définie par $U_0=\begin{pmatrix}-1\\2\end{pmatrix}$ et pour tout entier naturel n, $U_{n+1}=A\,U_n$ où $A=\begin{pmatrix}1&2\\-1&1\end{pmatrix}$.

1) Calculer U_1 et U_2

2) Exprimer $U_n=\begin{pmatrix}x_n\\y_n\end{pmatrix}$ en fonction de n et A, puis déterminer la matrice U_{10} avec la calculatrice.

Ex 11-2 : ***Calculer les termes d'une suite en utilisant l'écriture matricielle de la relation de récurrence***

On considère les suites (a_n) et (b_n) définies pour tout entier naturel n par :

$a_{n+1}=2a_n-b_n$ et $a_2=3$

$b_{n+1}=-a_n+2b_n$ et $b_2=5$

On définit pour tout entier naturel n, la matrice $U_n=\begin{pmatrix}a_n\\b_n\end{pmatrix}$

1) Déterminer la matrice A, telle que $U_{n+1}=A\,U_n$

2) Calculer a_0 et b_0

3) Calculer a_6 et b_6

Ex 11-3 : ***Calculer les termes d'une suite en utilisant l'écriture matricielle de la relation de récurrence***

On considère la suite de nombres réels (a_n) telle que pour tout entier naturel n non nul : $a_{n+1}=2a_n-a_{n-1}$

1) Traduite la relation de récurrence par une égalité matricielle du type $U_{n+1}=A\,U_n$

2) On donne $a_0=2$ et $a_1=5$. Calculer a_4 et a_5 .

Ex 11-4 : ***Vrai ou faux***

1) La suite de matrices colonnes (U_n) définie par $U_n=\begin{pmatrix}e^{-n}\\\frac{1}{2^n}\end{pmatrix}$ est convergente.

2) La suite de matrices colonnes (V_n) définie par $V_n=\begin{pmatrix}0,2^n-1\\3^n\end{pmatrix}$ est convergente.

3) La matrice $U=\begin{pmatrix}1\\0\\-1\end{pmatrix}$ est un état stable de la suite de matrices colonnes $U_{n+1}=AU_n$ où $A=\begin{pmatrix}2&1&1\\1&3&1\\4&5&2\end{pmatrix}$

Ex 11-5 : ***Mettre sous la forme*** $U_{n+1}=AU_n+B$

Traduire les relations de récurrence des suites ci-dessous par une égalité matricielle du type $U_{n+1}=AU_n+B$

1) $a_0=1$, $b_0=2$ et pour tout entier naturel n :

$$\begin{cases}a_{n+1}=3a_n-2b_n+2\\b_{n+1}=-a_n+2b_n-7\end{cases}$$

2) $a_0=-1$, $a_1=1$ et pour tout entier naturel $n\geqslant 0$:

$$a_{n+2}=-a_n+5a_{n+1}-2$$

Ex 11-6 : $U_{n+1}=AU_n$ ***et état stable***

On considère la suite de matrices (U_n) définie par $U_0=\begin{pmatrix}2\\3\end{pmatrix}$ et pour tout entier naturel n , $U_{n+1}=AU_n$ où $A=\begin{pmatrix}3&0\\0&2\end{pmatrix}$.

1) Montrer que la suite diverge.

2) La suite (U_n) a-t-elle un état stable ?

Ex 11-7 :

Soit la suite de matrices (U_n) , définie pour tout entier naturel n par $U_{n+1}=AU_n+B$ où $U_0=\begin{pmatrix}1\\2\end{pmatrix}$, $A=\begin{pmatrix}\frac{1}{2}&0\\-\frac{1}{2}&\frac{1}{2}\end{pmatrix}$ et $B=\begin{pmatrix}-2\\1\end{pmatrix}$

1) Déterminer une matrice U telle que $U=AU+B$.

2) On pose $V_n=U_n-U$. Montrer que pour tout entier naturel n , $V_{n+1}=AV_n$.
En déduire l'expression de V_n en fonction de n .

3) Avec la calculatrice, déterminer A^2 , A^3 , A^4 et A^5 .
Conjecturer une expression de A^n

4) Démontrer la conjecture précédente pour tout entier naturel n non nul.

5) En déduire l'expression de U_n en fonction de n .

6) On admet que $\lim_{n \to +\infty} n\,0{,}5^n = 0$. Étudier la convergence de la suite (U_n) .

Ex 11-8 : ***Avec la calculatrice***

On donne $A = \begin{pmatrix} 0{,}3 & 0{,}5 \\ 0{,}4 & 0{,}1 \end{pmatrix}$ et $B = \begin{pmatrix} 0{,}2 \\ 0{,}3 \end{pmatrix}$

1) On considère la suite de matrices colonne (U_n) telles que pour tout entier naturel n , $U_{n+1} = A\,U_n + B$.

Déterminer la matrice U telle que $U = AU + B$

2) Conjecturer le comportement asymptotique de A^n

3) Quelle conjecture peut-on alors faire sur le comportement asymptotique de la suite (U_n) ?

Ex 11-9 :

Soit les matrices $A = \begin{pmatrix} \frac{13}{30} & -\frac{2}{15} \\ -\frac{1}{15} & \frac{11}{30} \end{pmatrix}$ et $B = \begin{pmatrix} 6 \\ 0 \end{pmatrix}$

On considère la suite de matrices colonne (U_n) telles que pour tout entier naturel n , $U_{n+1} = A\,U_n + B$.

1) Déterminer la matrice U telle que $U = AU + B$

2) Soit $P=\begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix}$ et $D=\begin{pmatrix} 0{,}3 & 0 \\ 0 & 0{,}5 \end{pmatrix}$.
Vérifier que $A=P^{-1}DP$

3) a) Montrer que $A^n=PD^nP^{-1}$.

b) En déduire les coefficients de A^n .

4) On pose $V_n=U_n-U$. Montrer que pour tout entier naturel n , $V_{n+1}=AV_n$.
En déduire l'expression de V_n en fonction de n , puis l'expression de U_n en fonction de n .

5) Étudier la convergence de la suite (U_n) .

Ex 11-10 : ***Baccalauréat S – Liban 31 mai 2019 – ex 4***

$U_{n+1} = A\,U_n + B$ - matrices diagonales - récurrence

Dans un jardin public, un artiste doit installer une œuvre aquatique commandée par la mairie. Cette œuvre sera constituée de deux bassins A et B ainsi que d'une réserve filtrante R.
Au départ, les deux bassins contiennent chacun 100 litres d'eau.
Un système de canalisations devra alors permettre de réaliser, toutes les heures et dans cet ordre, les transferts d'eau suivants :

— dans un premier temps, la moitié du bassin A se vide dans la réserve R ;
— ensuite, les trois quarts du bassin B se vident dans le bassin A ;
— enfin, on rajoute 200 litres d'eau dans le bassin A et 300 litres d'eau dans le bassin B.

Une étude de faisabilité du projet amène à étudier la contenance des deux bassins A et B qui est à prévoir pour éviter tout débordement.

On modélise les quantités d'eau des deux bassins A et B à l'aide de deux suites (a_n) et (b_n) : plus précisément pour tout entier naturel n, on note a_n et b_n les quantités d'eau en centaines de litres qui seront respectivement contenues dans les bassins A et B au bout de n heures. On suppose pour cette étude mathématique que les bassins sont a priori suffisamment grands pour qu'il n'y ait pas de débordement.

Pour tout entier naturel n, on note U_n la matrice colonne $U_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$. Ainsi $U_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

1. Justifier que, pour tout entier naturel n, $U_{n+1} = MU_n + C$ où $M = \begin{pmatrix} 0{,}5 & 0{,}75 \\ 0 & 0{,}25 \end{pmatrix}$ et $C = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.

2. On considère la matrice $P = \begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}$.

a. Calculer P^2. En déduire que la matrice P est inversible et préciser sa matrice inverse.

b. Montrer que PMP est une matrice diagonale D que l'on précisera.

c. Calculer PDP.

d. Démontrer par récurrence que, pour tout entier naturel n, $M^n = PD^nP$.

On admet par la suite que pour tout entier naturel n, $M^n = \begin{pmatrix} 0{,}5^n & 3 \times 0{,}5^n - 3 \times 0{,}25^n \\ 0 & 0{,}25^n \end{pmatrix}$.

3. Montrer que la matrice $X = \begin{pmatrix} 10 \\ 4 \end{pmatrix}$ vérifie $X = MX + C$.

4. Pour tout entier naturel n, on définit la matrice V_n par $V_n = U_n - X$.

a. Montrer que tout entier naturel n, $V_{n+1} = MV_n$.

b. On admet que, pour tout entier naturel non nul n, $V_n = M^nV_0$.

Montrer que pour tout entier naturel non nul n, $U_n = \begin{pmatrix} -18 \times 0{,}5^n + 9 \times 0{,}25^n + 10 \\ -3 \times 0{,}25^n + 4 \end{pmatrix}$.

5. **a.** Montrer que la suite (b_n) est croissante et majorée. Déterminer sa limite.

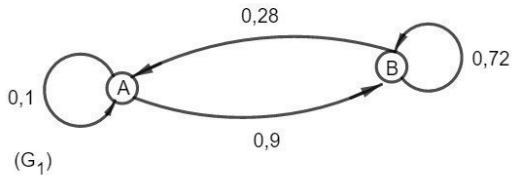
b. Déterminer la limite de la suite (a_n).

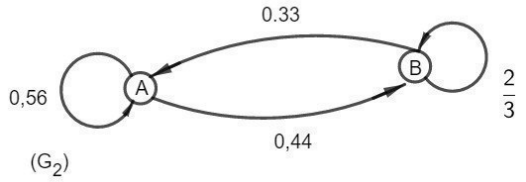
c. On admet que la suite (a_n) est croissante. En déduire la contenance des deux bassins A et B qui est à prévoir pour la faisabilité du projet, c'est-à-dire pour éviter tout débordement.

Graphes probabilistes

Ex 11-11 : ***Graphes probabilistes ?***

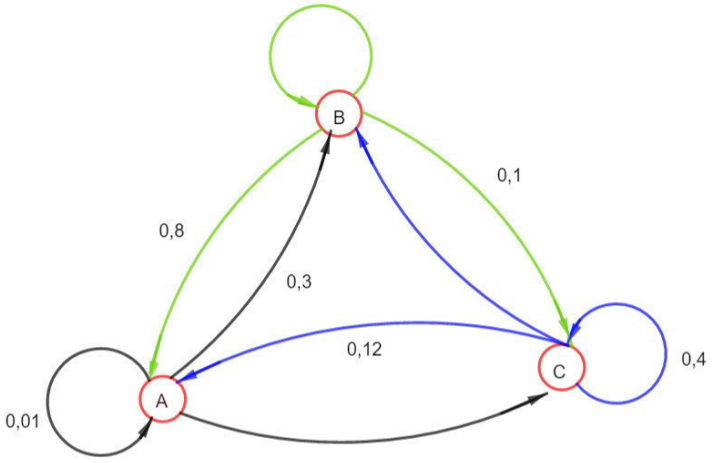
Les graphes ci-dessous sont-ils des graphes probabilistes ?
Si oui, donner la matrice de transition associée.





Ex 11-12 : ***Compléter un graphe probabiliste***

Compléter le graphe probabiliste ci-dessous et donné la matrice de transition associée .



Ex 11-13 :

Une grenouille saute aléatoirement plusieurs fois par heure sur trois rochers . A chaque étape :

- Si elle est sur le rocher A, elle choisit de manière équiprobable, soit de rester en A, soit de sauter vers le rocher B ou vers le rocher C.

- Si elle est sur le rocher B, elle choisit de manière équiprobable de sauter sur le rocher A ou sur le rocher C.

- Si elle est sur le rocher C, elle saute sur le rocher A.

On note X_n la variable aléatoire donnant la position de la grenouille à l'étape n .
Au début, pour $n=0$, la grenouille est sur le rocher A.

1) Donner la distribution initiale du système.

2) En utilisant un arbre pondéré, donner la distribution du système après deux étapes.

3) Expliquer pourquoi la suite (X_n) est une chaîne de Markov et donner le graphe probabiliste et la matrice associée.

4) Quelle est la probabilité que la grenouille se retrouve à nouveau sur le rocher A au bout de 5 étapes ?

5) La grenouille (de compétition) , saute sans jamais s'arrêter . Conjecturer grâce à la calculatrice, la probabilité qu'elle soit sur le rocher A au bout d'une semaine ?

Ex 11-14 :

Un chimpanzé navigue sur un site internet comptant trois pages.
Sur chacune des pages, il y a des bananes représentant des liens ramenant sur les autres pages.
- Sur la page 1, il y a deux bananes, l'une menant à la page 2 et l'autre à la page 3.
- Sur la page 2, il y a quatre bananes, trois menant à la page 3 et une à la page 1.
- Sur la page 3, il y a une banane menant à la page 2.

1) Représenter la situation à l'aide d'un graphe probabiliste et donner la matrice de transition P associée.

2) Le chimpanzé est sur la page 2 et clique 15 fois . Sur quelle page a-t-il le plus de chance de se retrouver ?

Déterminer une distribution invariante

Ex 11-15 :

La matrice $P=\begin{pmatrix} \frac{1}{4} & \frac{3}{4} \\ \frac{2}{3} & \frac{1}{3} \end{pmatrix}$ est la matrice de transition associée à une chaîne de Markov.

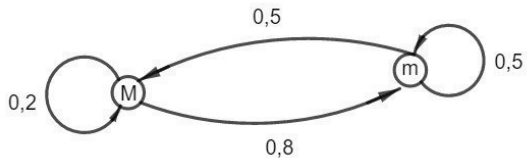
1) Représenter le graphe associé.

2) Déterminer la distribution invariante de cette chaîne.

3) Déterminer le comportement asymptotique de cette chaîne.

Ex 11-16 :

Un ordinateur est programmé pour afficher successivement des lettres qui sont soit des lettres majuscules (M) soit des lettres minuscules (m) selon le graphe probabiliste ci-dessous :



1) On suppose que la première lettre est une majuscule . Calculer la probabilité que la 10-ième lettre soit aussi une majuscule.

2) Déterminer la distribution invariante de ce système, puis interpréter le résultat.

Ex 11-17 :

La matrice $P=\begin{pmatrix} 0,5 & 0,5 & 0 \\ 0 & 0,5 & 0,5 \\ 1 & 0 & 0 \end{pmatrix}$ est la matrice de transition associée à une chaîne de Markov de distribution initiale $\pi_0=\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$

1) Représenter cette chaîne par un graphe pondéré.

2) Calculer la distribution après 5 transitions.

3) Avec la calculatrice, conjecturer le comportement asymptotique de cette chaîne de Markov.

4) Conjecturer que la suite des distributions (π_n) converge et donner sa limite.

Ex 11-18 :

Un chat, au cours de la journée se déplace pour dormir entre le lit (A), le canapé (B) et le tapis (C).
On note a_n , b_n et c_n les probabilités respectives que le chat soit en A, en B et en C après n déplacements.

À l'étape $n=0$, il dort tranquillement sur le lit.

Une étude sur le comportement de ce chat a permis d'établir que :

$$\begin{cases} a_{n+1}=0,3a_n+0,3b_n+0,3c_n \\ b_{n+1}=0,2a_n+0,5b_n+0,3c_n \\ c_{n+1}=0,5a_n+0,2b_n+0,4c_n \end{cases}$$

On note $\pi_n=(a_n\, b_n\, c_n)$

1) Écrire la matrice P, telle que, pour tout entier naturel n , $\pi_{n+1}=\mathrm{P}\pi_n$

2) Calculer la probabilité pour que le chat dorme sur le tapis après 4 étapes.

3) Justifier que la suite de matrices (π_n) converge vers une matrice $\pi=(a \quad b \quad c)$

4) Démontrer que les nombres a , b et c vérifient le système suivant :

$$(\mathrm{S}):\begin{cases} a+b+c=1 \\ -0,7a+0,3b+0,3c=0 \\ 0,5a+0,2b-0,6c=0 \end{cases}$$

5) Résoudre ce système à l'aide d'un calcul matriciel.

6) En déduire l'endroit où le chat a le plus de chance de dormir à long terme.

L’alphabet grec en sciences

majuscules	minuscules	
	α	alpha
	β	beta
Γ	γ	gamma
Δ	δ	delta
	ε	epsilon
	ζ	zêta
	η	êta
Θ	θ	thêta
	ι	iota
	κ	kappa
Λ	λ	lambda
	μ	mu
	ν	nu
X	χ	xi ou ksi
	ο	omicron
Π	π	pi
	ρ	rhô
Σ	σ	sigma
	τ	tau
	υ	upsilon
Φ	ϕ	phi
	ξ	chi ou khi
	ψ	psi
Ω	ω	omega

Ne sont indiquées que les capitales utilisées en sciences . Les autres, identiques à des lettres de l’alphabet latin, ne sont pas utilisées.

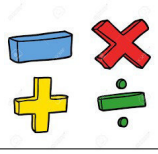
La lettre omicron, identique à notre lettre o, n’est pas utilisée en sciences.

PYTHON - les instructions de base utilisées au lycée

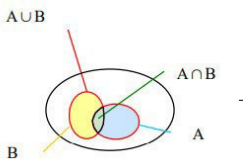
http://pierrelux.net

Créer un programme	- On va à la ligne après chaque instruction. - On peut séparer plusieurs instructions sur la même ligne en les séparant par « **;** »
Saisir une variable Il existe aussi d'autres types numériques : **type long** : Entier compris entre – inf et 2 147 483 647 ou entre 2 147 483 648 et + inf **type complex** : Nombre complexe Pour connaître tous les types … https://fr.wikiversity.org/wiki/Python/Les_types_de_base	- **A=input("A=")** si A est une chaîne de caractère (c'est le type par défaut) **type str** : *Chaîne de caractères* - **A=float(input("A="))** si A est un flottant **type float** : *Valeur spécifiée avec un point dans le programme (exemple : a=2.0) permettant une approximation de nombre réel* - **A=int(input("A="))** si A est un entier **type int** : *Entier compris entre -2 147 483 648 et 2 147 483 647 (codage sur 32 bits soit 4 octets)*
Afficher	- **print(A)** affiche la valeur de la variable A - **print("Vive les maths")** affiche le texte Vive les maths - On peut aussi mélanger texte et variable : **print("la valeur de A est ",A)**
Affecter	**B=A** affecte la valeur A ou le contenu de la variable A à la variable B
Écrire un commentaire	Les commentaires s'écrivent après le signe **#**
Opérations élémentaires	addition **+** soustraction **-** multiplication ***** puissance ****** division **/** reste de division entière **%** (9%2 donne 1) quotient de division entière **//** (9//2 donne 4)
Tester ...	**A==B** (égal) **A!=B** (différent) **A>B** (supérieur) **A<B** (inférieur) **A>=B** (supérieur ou égal) **A<=B** (inférieur ou égal)
Et / Ou	A **and** B / A **or** B
Si … Sinon Si … Sinon	**if** *condition C1* **:** *instruction A1* **elif** *condition C2* **:** *instruction A2* **else :** *instruction A3* C'est **le décalage** vers la droite qui indique les instructions faisant partie de la structure conditionnelle. Il n'y a pas d'instruction de fin. Il en est de même pour **for** , **while** et **def**.
Boucle Pour	**for i in range(1,n+1) :** *instruction A* la variable i parcourt tous les entiers de 1 à n - **for i in range(n):** la variable i parcourt tous les entiers de 0 à n-1 - **for i in range(m,n):** la variable i parcourt tous les entiers de m à n-1 - **for i in range(m,n,p):** la variable i parcourt tous les entiers de m à n-1 avec un **pas** de p.
Boucle Tant que	**while** *condition* **:** *instruction A*
Fonctions	**Def exemple(a,b …):** *instruction … y=…* **return(y)** a,b,… sont **les arguments** de la fonction exemple On peut aussi retourner plusieurs valeurs : return(x,y,z,...)
Insérer un **module**	Un module est une bibliothèque comportant un ensemble de fonctions. Je présente ci-dessous les modules utilisés au lycée.
Opérations mathématiques : math **Toutes les fonctions du module math** **https://www.afpy.org/doc/python/3.5/library/math.html**	**from math import *** On peut aussi importer uniquement la fonction souhaitée : **from math import sqrt** Le module math, contient les définitions de nombreuses fonctions mathématiques telles que **sin**, **cos** , **tan** ,**sqrt** , **pi** …
Nombres aléatoires : random **Toutes les fonctions du module random** **https://docs.python.org/fr/3.5/library/random.html**	**from random import *** Le module random contient les définitions de nombreuses fonctions faisant référence au hasard telles que : - **uniform(a,b)** qui retourne un nombre aléatoire compris entre a et b - **randint(a,b)** qui retourne un entier aléatoire compris entre a et b
Graphiques : pylab Bases du module **pylab** **http://matplotlib.free.fr/bases.html**	**from pylab import *** Le module pylab contient de nombreuses fonctions graphiques, ce qui en fait un outil très puissant pour créer des graphiques scientifiques. Ce module possède aussi les fonctions usuelles du module math , il n'est donc pas utile d'importer aussi celle-ci lorsqu'on utilise pylab. On peut aussi utiliser une version plus légère : **matplotlib.pyplot**. Mais celui-ci ne possède pas les fonctions du module math.
Listes et chaînes de caractères	**A=[]** permet de définir la liste vide A **A.append(x)** ajoute la valeur x à la liste (Si la liste était définie jusqu'au 10 ème terme, x sera le 11ème terme)
Longueur	**len(A)** renvoie la longueur de la liste ou de la chaîne de caractères A
Extraire	**A[k]** renvoie le k+1 ème élément de la liste ou de la chaîne de caractères A. Attention A[0] est le premier terme de la liste.
Concaténer	"mathé "**+**"matiques" donne la chaîne de caractères "mathématiques" [1,2,3,4]**+**[5,6,7,8] donne la liste [1,2,3,4,5,6,7,8]

Quelques symboles mathématiques à connaître



http://pierrelux.net

				Exemples
Symbole d'implication	$A \Rightarrow B$	A **implique** B **Si** A **alors** B B est **nécessaire** à A A est **suffisant** pour B	Ce symbole est censé exprimer l'idée que A est vraie entraîne que B aussi.	$x=2 \Rightarrow x^2=4$
Symbole d'équivalence	$A \Leftrightarrow B$ A ssi B	A **équivaut à** B A **si et seulement si** B	Il s'agit d'une implication dans les deux sens : A implique B et B implique A	$x=2$ ou $x=-2$ $\Leftrightarrow x^2=4$
Quantificateur universel	$\forall x \ , \ P(x)$	**Quel que soit** x ; **pour tout** x	La propriété $P(x)$ est vérifiée pour tout x	$\forall x \in \mathbb{R}^+ \ , \ x^2+\frac{1}{x+1}>0$
Quantificateur existentiel	$\exists x \ , \ P(x)$	**Il existe** x tel que...	La propriété $P(x)$ est vérifiée pour au moins un x .	$\exists x \in \mathbb{R} \ , \ (x-2)(x-3)>0$
Symbole d'appartenance	$x \in E$	x **appartient à** E x **est élément de** E E **contient** x	Pour un ensemble E donné, ce symbole signifie qu'il contient l'élément x .	$A \in d$ $2 \in]-3;5[$
Symbole de non-appartenance	$x \notin E$	x **n'appartient pas à** E	Négation de l'appartenance de x à E .	$-5 \notin \mathbb{N}$
Symbole d'inclusion	$A \subset B$	A est **inclus** dans B A est **un sous-ensemble** de B A est **une partie** de B B **contient** A	Pour deux ensembles A et B donnés, ce symbole signifie que tous les éléments de A sont éléments de B .	$]-2;5[\subset]-3;8[$
Symbole de non-inclusion	$A \not\subset B$	A n'est **pas inclus** dans B	Négation de l'inclusion de A dans B , c'est-à-dire qu'il existe au moins un élément de A qui n'appartient pas à B .	$\mathbb{Q} \not\subset \mathbb{Z}$
Ensemble vide	$\emptyset$	**Ensemble vide**	Ensemble qui ne comporte aucun élément	$]3,1;5[\cap [5,2;+\infty[= \emptyset$
Singleton, paire, ensembles finis Accolades { … }	$\{x\}$ $\{x,y\}$ $\{x_1,x_2 \ldots x_n\}$	**Singleton** x **Paire** $x \quad y$ **Ensemble** $x_1 \ , \ x_2 \ \ldots \ x_n$	Ensemble dont l'unique élément est x Ensemble dont les seuls éléments sont x et y Ensemble dont les n éléments sont $x_1 \ , \ x_2 \ \ldots \ x_n$.	L'ensemble des solutions de l'équation $x^2=4$ est $S=\{-2;2\}$ L'ordre n'est pas important. On aurait pu écrire $\{2;-2\}$
Couple, Triplet, n-uplet Parenthèses (...)	(x,y) (x,y,z) $(x_1,x_2 \ldots x_n)$	**Couple** $x \quad y$ **Triplet** $x \quad y \quad z$ **n-uplet** $x_1 \ , \ x_2 \ \ldots \ x_n$	Représentation d'une collection d'objets occupant chacun **une place précise**, au sens où contrairement à un ensemble finis, l'ordre et la répétition des objets n'est pas anodine.	Le point de coordonnées $(5;7)$ n'est pas le point de coordonnées $(7;5)$.
Réunion $A \cup B$		A **union** B **Réunion** de A et B	Ensemble contenant les éléments de A **ou** B et seulement ceux-là. Les éléments en commun à A et B sont dans la réunion. On dit que le ou mathématique est **inclusif**.	$]-7;8] \cup [-3;10[=]-7;10[$
Intersection $A \cap B$		A **inter** B **Intersection** de A et B	Ensemble contenant les éléments en communs de A et B et seulement ceux-là.	$]-7;8] \cap [-3;10[= [-3;8]$
Somme	$\sum_{i=1}^{n}$	**Somme** de $i=1$ à $i=n$	On avance de 1 en 1, c'est à dire : 1,2,3,4,5 $\ldots, n$	$\sum_{i=3}^{7} i^2 = 3^2+4^2+5^2+6^2+7^2$
Association	$f : x \longmapsto f(x)$	fonction f **qui à** x associe le nombre $f(x)$	Attention, il ne faut pas utiliser la flèche $\rightarrow$	$f : x \longmapsto x^2$

$\mathbb{N}$ est l'ensemble des **nombres entiers naturels**. $\mathbb{N}=\{0;1;2;3;\ldots\}$

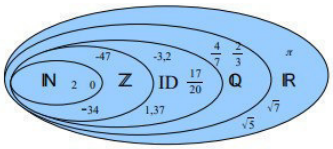
$\mathbb{Z}$ est l'ensemble des **nombres entiers relatifs** (ou ***nombres entiers***) $\mathbb{Z}=\{\ldots;-3;-2;-1;0;1;2;3;\ldots\}$

$\mathbf{D}$ est l'ensemble des **nombres décimaux**. (nombres s'écrivant $n \times 10^p$ avec n et p dans $\mathbb{Z}$)

$\mathbb{Q}$ est l'ensemble des **nombres rationnels**. (nombres que l'on peut écrire sous la forme $\frac{p}{q}$, p étant un nombre entier et q un entier non nul)

On appelle **nombre irrationnel** tout nombre que l'on ne peut pas écrire sous la forme $\frac{p}{q}$, p étant un nombre entier et q un entier non nul.

$\mathbb{R}$ est l'ensemble des **nombres réels**, c'est à dire qui sont soit rationnels, soit irrationnels.



$$\mathbb{N} \subset \mathbb{Z} \subset \mathbf{D} \subset \mathbb{Q} \subset \mathbb{R}$$

$\mathbb{N}^*$ est l'ensemble des entiers naturels privé de 0.
$\mathbb{R}^*$ est l'ensemble des réels privé de 0. $\mathbb{R}^+$ est l'ensemble des réels positifs. $\mathbb{R}^-$ est l'ensemble des réels négatifs.
$\mathbb{R}^{+*}$ est l'ensemble des réels strictement positifs. $\mathbb{R}^{-*}$ est l'ensemble des réels strictement négatifs.

$\mathbb{R}-\{2\}$ ou $\mathbb{R} \setminus \{2\}$ est l'ensemble des réels privé de 2

$\mathbb{R}-\{2;5,2\}$ ou $\mathbb{R} \setminus \{2;5,2\}$ est l'ensemble des réels privé de 2 et 5,2