Mercredi 17 janvier 2024. TG Maths expertes - PPCM - PGCD - Bézout - Gauss.

Égalité de Bézout.
PGCD(a;b) = D.
$\Leftrightarrow$
$\exists (u;v) \in \mathbb{Z}^2$ t.q $au+bv=D$

Théorème de Bézout :

PGCD(a;b) = 1.
$\Leftrightarrow$
$\exists (u;v) \in \mathbb{Z}$ t.q $au+bv=1$.

Corollaire du théorème de Bézout :
$(x;y) \in \mathbb{Z}^2$.

E : $ax+by=c$

PGCD(a;b) / c $\Leftrightarrow$ E admet des solut°.

$2x+4y=5$.

Exercice n°8
3. Montrons que 2 nombres impairs consécutifs sont premiers entre eux.
Soit $n \in \mathbb{Z}$, alors $2n+1$ est nécessairement impaire. Le nombre impaire qui le suit est :
$2n+3$.
But : montrer que PGCD(2n+1 ; 2n+3) = 1

$(n+1) \times (2n+1) + (-n) \times (2n+3)$
$= 2n^2 + n + 2n + 1 - 2n^2 - 3n$.
$= 1$.
D'après le théorème de Bézout PGCD(2n+1; 2n+3) = 1.

Soit (x;y) solut° de E :

E : $2x+4y=8$.

Méthode : On trouve un couple de solution particulier de E.
$(x_0;y_0) = (6;-1)$

$2x+4y = 8 = 2\times 6 + 4\times(-1)$.
$2x+4y = 2\times 6 + 4\times(-1)$.
$2x-2\times 6 = 4\times(-1) - 4y$.
$2(x-6) = 4(-1-y)$
$*$: $1\times(x-6) = 2(-1-y)$.

2 / $1\times(x-6)$.
D'après le théorème de Gauss, on a :

$2 / (x-6) \Leftrightarrow \exists k \in \mathbb{Z}$ t.q $x-6 = 2k$.
$\boxed{x = 2k+6}$
On injecte $x = 2k+6$ dans $*$ et on obtient :
$1\times(2k+6-6) = 2(-1-y)$.
$-1-y = k$.
$\boxed{y = -k-1}$

Les solut° de E sont sous la forme, $\forall k \in \mathbb{Z}$
$\boxed{(x;y) = (2k+6; -k-1)}$

$2x+4y = 8$.
$k=-3$ $(x;y) = (0;2)$.

$$41x - 25y = 1.$$

$41 = 25\times 1 + 16$. $\quad 1 = 7 - 2\times 3$.
$25 = 16\times 1 + 9$. $\quad 1 = 16 - 9 - 3\times(9-7)$.
$16 = 9\times 1 + 7$. $\quad 1 = (41-25) - (25-16) - 3\times(25-16-(16-9))$.
$9 = 7\times 1 + 2$. $\quad 1 = 41 - 25 - 25 + 41 - 25 - 3\times 25 + 3\times(41-25)$
$7 = 2\times 3 + \boxed{1}$
$2 = 1\times 2 + 0$.

Ex n°17 : PGCD(4;3) = 1 / 2
Donc, il existe des sol°.
(E) : $4x-3y=2$.
1) $(x_0;y_0) = (2;2)$ est une sol° de (E).
2) $4\times 2 - 3\times 2 = 8-6 = 2$.
3) $4x-3y = 4\times 2 - 3\times 2$.
$4x-4\times 2 = 3y - 3\times 2$.
$4(x-2) = 3(y-2)$.
4 / $3(y-2)$, or PGCD(4;3) = 1.
donc d'après le théorème de Gauss, on a :

$4 / (y-2) \Leftrightarrow \exists k \in \mathbb{Z}$ t.q :
$y-2 = 4k$.
$\boxed{y = 4k+2}$
D'où : $4(x-2) = 3(4k+2-2)$.
$\boxed{x = 3k+2}$.

L'ensemble des solutions est : $(x;y) = (3k+2; 4k+2)$

L'étude des nombres entiers $\mathbb{Z}$.

ARITHMETIQUE PARTIE 2

PGCD
PPCM
Théorème de Bezout.
Théorème de Gauss.
Equations diophantiennes.

Chapitre 3

PGCD, PPCM, théorème de Bézout, théorème de Gauss

Arithmétique partie 2

PGCD, PPCM, THEOREME DE BEZOUT, THEOREME DE GAUSS

I. PGCD

1. Définition

Soit a et b deux nombres entiers non nuls. Alors le plus grand diviseur commun des deux nombres a et b est noté $PGCD(a;b)$.

Exemple

$PGCD(4;16) = 4$

$PGCD(34;112) = 2$

Diviseurs de 4 : {1 ; 2 ; 4}

Diviseurs de 16 : {1 ; 2 ; 4 ; 8 ; 16}

$PGCD(a;b) = 1 \Leftrightarrow$ a et b sont premiers entre eux.

Pour trouver le $PGCD$ de deux nombres on peut dresser la liste des diviseurs des deux nombres. Alors le $PGCD$ de ces deux nombres est le plus grand diviseur commun à ces deux nombres.

Propriété (Démonstration hors programme)

Soit k un entier naturel non nul, alors on a : $PGCD(ka;kb) = k \times PGCD(a;b)$

$PGCD(2\times3;2\times4) = 2\,PGCD(3;4) = 2\times1 = 2$

2. Nombres premiers entre eux

Définition

On dit que deux nombres a et b sont premiers entre eux si et seulement si :

$$PGCD(a;b) = 1$$

Remarque

Il ne faut pas confondre nombres premiers entre eux et nombres premiers. En effet, 32 et 33 ne sont pas premiers car ils sont respectivement divisibles par 2 et 3. En revanche, 32 et 33 sont premiers entre eux car leur PGCD vaut 1.

3. Algorithme d'Euclide

L'algorithme d'Euclide permet de trouver « à la main » le PGCD de deux entiers. On souhaite déterminer le PGCD de 32 et 44. Alors on fait la division euclidienne du plus grand nombre par le plus petit :

D d q r

$$44 = 32 \times 1 + 12$$

On réalise ensuite la division euclidienne du diviseur de cette première division par son reste :

$$32 = 12 \times 2 + 8$$

On répète la dernière opération jusqu'à trouver un reste nul :

$$12 = 8 \times 1 + 4$$
$$8 = 4 \times 2 + 0$$

Dès lors le $PGCD(32;44) = 4$

II. PPCM

Définition

Soient a et b deux entiers non nuls. Alors le $PPCM$ de a et b noté $PPCM(a;b)$ est le plus petit multiple commun à a et b.

Exemple

$PPCM(18;12) = 36$
$PPCM(24;40) = 120$

Propriété (Démonstration hors programme)

$$ab = PPCM(a;b) \times PGCD(a;b)$$

Illustration

D'une part, nous avons : $PGCD(8;12) = 4$ et $PPCM(8;12) = 24$ d'où $4 \times 24 = 96$

D'autre part, nous avons $8 \times 12 = 96$.

Ainsi, nous pouvons dire que la propriété est vérifiée dans ce cas particulier. On admettra qu'elle est vraie pour tous les entiers a et b.

III. THEOREME DE BEZOUT

1. Egalité de Bézout

Soient a et b deux entiers non nuls. On pose $D = PGCD(a;b)$. Dès lors il existe un couple d'entiers $(u;v)$ tels que :

$$au + bv = D$$

Remarque IMPORTANTE

L'égalité de Bézout est une implication seulement, cela signifie que la réciproque est fausse.

Démonstration (importance : haute)

- Soient a et b deux entiers non nuls.
  On note E un ensemble constitué des nombres entiers strictement positifs sous la forme : $ma + nb$ où m et n sont des entiers relatifs quelconques.
  On peut donc dire que E est une partie de $\mathbb{N}$ qui est non vide, c'est-à-dire qu'il y a forcément au moins un élément dans E. Pour vérifier que E est non vide, on peut vérifier qu'il y existe au moins un élément.
  En effet on peut aisément vérifier que $|b| \in E$.
  Donc E admet un plus petit élément. Ce plus petit élément, on l'appelle $\boldsymbol{d = au + bv}$. En fait, d est atteint pour $m = u$ et $n = v$.
  Soit $D = PGCD(a;b)$ donc D/a et D/b donc D divise TOUTE combinaison linéaire de a et de b on a donc :
  $\boldsymbol{D/(au + bv)}$ **donc** $\boldsymbol{D/d}$ **ce qui veut dire que** $\boldsymbol{D}$ **est un diviseur de** $\boldsymbol{d}$ **donc** $\boldsymbol{D \leq d}$
- Montrons maintenant que d/a. Effectuons alors la division euclidienne de a par d, on a :
  $a = dq + r$ où $0 \leq r < d$.

Supposons que $r \neq 0$. Maintenant, on isole r et dans le même temps on remplace d par $au + bv$. On obtient donc :

$$r = a - (au + bv) \times q = a - auq - bvq = \boldsymbol{a(1 - uq) + b(-vq)}$$

En posant $1 - uq = M$ et $-vq = N$, nous venons de montrer ainsi que $r = Ma + Nb$. Donc $r \in E$. Or cela est **ABSURDE.** En effet nous savons que le plus petit élément de E est d or $r < d$. Donc on en déduit que la seule valeur possible pour r est $r = 0$. **Donc d divise a.**

En effectuant exactement la division euclidienne de b par d, on démontre exactement de la même manière que **d divise b.**

Ainsi d divise a et d divise b. Donc d est un diviseur commun de a et b. Or D est le plus grand des diviseurs communs, donc $d \leq D$.

Finalement, nous avons montré d'une part que $D \leq d$, d'autre part que $d \leq D$ donc il en résulte : $\boldsymbol{d = D}$. En d'autres termes :

$$\boldsymbol{au + bv = D}$$

2. Théorème de Bézout (équivalence)

Soient a et b deux entiers. Alors a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que :

PGCD $(a;b) = 1 \iff \exists\ au+bv = 1.$

$$\boldsymbol{au + bv = 1}$$

Remarque IMPORTANTE

Le théorème de Bézout est une équivalence, c'est-à-dire que la réciproque est vraie. Il faut donc démontrer le théorème dans les deux sens : « ⇒ » et « ⇐ »

Démonstration ROC (importance : haute)

- Dans le sens ⇒ :

Les nombres a et b sont deux entiers qui sont premiers entre eux. C'est-à-dire que $PGCD(a; b) = 1$. D'après l'égalité de Bézout il existe deux entiers u et v tels que $au + bv = 1$.

- Dans le sens ⇐ :

On suppose qu'il existe deux entiers tels que $au + bv = 1$. Notons alors D le $PGCD$ de a et de b, i.e $PCGD(a; b) = D$. Dès lors, D est le plus grand diviseur **commun** à a et à b. Donc D/a et D/b. Donc D divise **toute** combinaison linéaire de a et b. Ainsi : $D/(au + bv)$ donc $D/1$ donc $d = 1$.

$3x+4y=5$.

2x+4y=5

3. Corollaire du théorème de Bézout (équivalence)

L'équation $ax + by = c$ admet des solutions entières si et seulement si c est un multiple de $PGCD(a; b)$.

Démonstration (importance : haute)

- Dans le sens ⇒ :

L'équation $ax + by = c$ admet des solutions entières que l'on note $(x_0; y_0)$ on a donc $ax_0 + by_0 = c$.

Soit $D = PGCD(a; b)$. Ainsi D/a et D/b donc D divise toute combinaison linéaire de a et de b ainsi :

$D/(ax_0 + by_0)$. Donc D/c, en d'autres terme, c est un multiple de D.

- Dans le sens ⇐ :

D'une part, c est un multiple de $PGCD(a; b) = D$. Il existe donc il entier k tel que $c = Dk$.

D'autre part, d'après l'égalité de Bézout, il existe un couple $(u; v)$ tel que :

$$au + bv = D$$

En multipliant les deux membres de cette égalité par k, on obtient :

$$auk + bvk = Dk \Leftrightarrow a(uk) + b(vk) = c$$

On pose maintenant $x_0 = uk$ et $y_0 = vk$ on obtient finalement : $ax_0 + by_0 = c$.

IV. THEOREME DE GAUSS

Théorème (implication, réciproque fausse)

3/12x6

Soient a, b et c trois entiers non nuls. Si a divise bc et si a et b sont premiers entre eux alors a divise c.

Démonstration ROC (importance : très haute)

D'une part, a divise bc donc il existe un entier k tel que $bc = ka$.

D'autre part a et b sont premiers entre eux donc d'après le théorème de Bézout, il existe un couple $(u; v)$ tel que : $au + bv = 1$. En multipliant cette égalité par c, on a :

$auc + bvc = c$ on se souvient ici que $bc = ka$ d'où :
$a \times uc + a \times kv = c$ on factorise par a :

$$a(uc + kv) = c$$

Comme $uc + kv$ est un entier, on peut dire que a divise c.

Corollaire du théorème de Gauss

Soient a, b et c trois entiers non nuls. Si b et c divisent a, et si b et c sont premiers entre eux, alors bc divise a.

Démonstration ROC (importance : haute)

Nous savons que b et c divisent a. Ainsi, des entiers k et k' tels que $a = kb$ et $a = k'c$. Par transitivité :

$$kb = k'c$$

Donc $b/k'c$ et d'ailleurs b et c sont premiers entre eux donc d'après le théorème de Gauss, b divise k'. Il existe donc un entier k'' tel que $k' = bk''$. Cela nous permet d'écrire que :

$$\boldsymbol{a = k'c = bk''c = k''bc}$$

Donc bc divise a.

Plus grand commun diviseur (pgcd) Théorèmes de Bézout et de Gauss

PGCD

EXERCICE 1

Déterminer les entiers naturels n tels que :

1) $n \leqslant 200$ et $\text{pgcd}(n, 324) = 12$.
2) $n \leqslant 500$ et $\text{pgcd}(n, 378) = 54$.
3) $n \leqslant 400$ et $\text{pgcd}(n, 150) = 6$.

EXERCICE 2

Trouver tous les couples d'entiers naturels (a, b) avec $a < b$ tels que :

1) $\begin{cases} ab = 432 \\ \text{pgcd}(a, b) = 6 \end{cases}$
2) $\begin{cases} ab = 7\,776 \\ \text{pgcd}(a, b) = 18 \end{cases}$
3) $\begin{cases} a + b = 24 \\ \text{pgcd}(a, b) = 4 \end{cases}$

Algorithme d'Euclide

EXERCICE 3

Utiliser l'algorithme d'Euclide pour trouver le pgcd des couples suivants :

1) (144 , 840)
2) (202 , 138)
3) (441 , 777)
4) (2 004 , 9 185)

EXERCICE 4

À l'aide de l'algorithme d'Euclide, dire si les couples d'entiers suivants sont premiers entre eux.

1) (4 847 , 5 633)
2) (5 617 , 813)

EXERCICE 5

Compléter le programme en Python pour que la fonction récursive euclide(*a*,*b*) donne le pgcd(a, b).

```
def euclide(a,b):
    if b == 0:
        return ...
    return euclide(...,...)
```

Tester ce programme avec :

euclide(1 958 , 4 539) et euclide(123 456 789 , 987 654 321).

EXERCICE 6

Si on divise 4294 et 3521 par un même entier positif, on obtient respectivement 10 et 11 comme reste. Quel est cet entier ?

EXERCICE 7

Soit $n \in \mathbb{Z}$. On pose : $A = n - 1$ et $B = n^2 - 3n + 6$.

1) a) Démontrer que : $\text{pgcd}(A, B) = \text{pgcd}(A, 4)$.
   b) En déduire, selon les valeurs de n : $\text{pgcd}(A, B)$.

2) Pour quelles valeurs de $n \neq 1$, $\dfrac{n^2 - 3n + 6}{n - 1}$ est-il un entier relatif ?

Théorème de Bézout

PGCD $(a;b) = 1 \iff \exists (u;v) \in \mathbb{Z}^2$ t.q $au+bv = 1$.

EXERCICE 8

1) n est un entier naturel , $a = 7n + 4$ et $b = 5n + 3$
   Montrer, pour tout n, que a et b sont premiers entre eux.
2) Montrer que deux entiers consécutifs non nuls sont premiers entre eux.
3) Montrer que deux entiers impairs consécutifs sont premiers entre eux.

EXERCICE 9

Montrer que les fractions suivantes sont irréductibles pour tout entier naturel n :

1) $\dfrac{n}{2n+1}$ 2) $\dfrac{9n+1}{6n+1}$ 3) $\dfrac{14n+3}{5n+1}$

EXERCICE 10

Pour tout entier $n \geqslant 5$, on pose : $a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$.

1) Démontrer que a et b sont des entiers naturels divisible par $n - 4$.
2) On pose $\alpha = 2n + 1$ et $\beta = n + 3$. On note $d = \text{pgcd}(\alpha, \beta)$.
   a) Démontrer que d est un diviseur de 5.
   b) Démontrer que α et β sont multiples de 5 si et seulement si $n - 2 \equiv 0\ (5)$.
3) Démontrer que $2n + 1$ et n sont premier entre eux.
4) a) Déterminer $\text{pgcd}(a, b)$ en fonction de n.
   b) Vérifier les résultats obtenus dans les cas particuliers $n = 11$ et $n = 12$.

Couple d'entiers de Bézout

EXERCICE 11

1) Montrer que 87 et 31 sont premiers entre eux à l'aide de l'algorithme d'Euclide.
2) En remontant cet algorithme, déterminer un couple d'entiers relatifs (x, y) tel que $87x + 31y = 1$.

EXERCICE 12

1) Montrer que 38 et 45 sont premiers entre eux à l'aide de l'algorithme d'Euclide.
2) En remontant cet algorithme, déterminer un couple d'entiers relatifs (x, y) tel que $38x + 45y = 1$.

EXERCICE 13

1) Montrer que 41 et 25 sont premiers entre eux à l'aide de l'algorithme d'Euclide.
2) En remontant cet algorithme, déterminer un couple d'entiers relatifs (x, y) tel que $41x - 25y = 1$.

Théorème de Gauss

EXERCICE 14

1) Déterminer les couples d'entiers relatifs (x, y) tels que : $33x - 45y = 0$.
2) En déduire les couples d'entiers relatifs (x, y) tels que : $33x + 45y = 12$.

EXERCICE 15

1) Déterminer les couples d'entiers relatifs (x, y) tels que : $7(x - 3) = 5(y - 2)$.
2) En déduire les couples d'entiers relatifs (x, y) tels que : $7x \equiv 1\ (5)$.

EXERCICE 16

1) Montrer que si $x \equiv 0\ (3)$, $x \equiv 0\ (5)$ et $x \equiv 0\ (7)$ alors $x \equiv 0\ (105)$
2) Soit $n \in \mathbb{N}$. Montrer que $n(n+1)(n+2)$ est divisible par 6.

Équations diophantiennes

EXERCICE 17

Soit l'équation $4x - 3y = 2$.

1) Sans calcul, dire pourquoi cette équation admet des solutions entières.
2) Déterminer un couple d'entiers solution de cette équation.
3) Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 18

Soit l'équation $3x - 4y = 6$.

1) Déterminer un couple d'entiers solution de cette équation.
2) Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 19

Soit l'équation $5x + 8y = 2$.

1) Déterminer un couple d'entiers solution de cette équation.
2) Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 20

Soit l'équation $13x - 23y = 1$.

1) Déterminer un couple d'entiers solution de cette équation à l'aide de l'algorithme d'Euclide.

2) Déterminer l'ensemble des couples d'entiers solutions de cette équation.

EXERCICE 21

1) Démontrer que : $\forall n \in \mathbb{Z},\ \text{pgcd}(14n+3\,,\,5n+1) = 1$.

2) On considère l'équation : (E) $\quad 87x + 31y = 2$

   a) Vérifier, à l'aide de 1) que 87 et 31 sont premiers entre eux.

   b) En déduire un couple $(u\ ,\ v)$ d'entiers relatifs tels que $87u + 31v = 1$ puis un couple $(x_0\ ,\ y_0)$ solution de (E).

   c) Déterminer l'ensemble des solutions de (E) dans $\mathbb{Z}^2$.

3) **Application.** Trouver les points de la droite $87x - 31y - 2 = 0$ dont les coordonnées sont des entiers naturels et dont l'abscisse est comprise entre 0 et 10

EXERCICE 22

Conjonction d'astres

Un astronome a observé au jour J_0 le corps céleste A, qui apparaît périodiquement tous les 105 jours. Six jours plus tard (J_0 + 6), il observe le corps B, dont la période d'apparition est de 81 jours. On appelle J_1 le jour de la prochaine apparition simultanée des deux objets aux yeux de l'astronome.

Le but de cet exercice est de déterminer la date de ce jour J_1.

1) Soit u et v le nombre de périodes effectuées par A et B entre J_0 et J_1.
   Montrer que le couple (u, v) est solution de l'équation (E_1) : $35x - 27y = 2$.

2) a) Déterminer un couple de relatifs (x_0, y_0) solution de l'équation (E_2) :

$$35x - 27y = 1$$

   b) En déduire une solution $(u_0; v_0)$ de (E_1).

   c) Déterminer toutes les solutions de l'équation (E_1).

   d) Déterminer la solution $(u; v)$ permettant de déterminer J_1.

3) a) Combien de jours s'écouleront entre J_0 et J_1 ?

   b) J_0 était le mardi 10 décembre 2019, quelle est la date du jour J_1 ?
   On tiendra compte des années bissextiles.

   c) Si l'astronome manque ce futur rendez-vous, combien de jours devra t-il attendre jusqu'à la prochaine conjonction des deux astres ?

EXERCICE 23

En montagne, un randonneur a effectué des réservations dans deux types d'hébergement : l'hébergement A et l'hébergement B.

Une nuit en hébergement A coûte 24 € et une nuit en hébergement B coûte 45 €. Il se rappelle que le coût total de sa réservation est de 438 €.

On souhaite retrouver les nombres x et y de nuitées passées respectivement en hébergement A et en hébergement B.

1) a) Montrer que les solutions du problème sont solution de $8x + 15y = 146$.

   b) Montrer que x et y sont respectivement inférieurs ou égaux à 18 et 9.

   c) Compléter l'algorithme suivant afin qu'il affiche les couples (x,y) possibles.

```
pour x variant de 0 à ..... faire
    pour y variant de 0 à ..... faire
        si ..... alors
            Afficher x et y
        fin
    fin
fin
```

2) a) Déterminer une solution entière à l'équation : $8x + 15y = 1$.

   b) Résoudre l'équation (E) : $8x + 15y = 146$ où $x, y \in \mathbb{Z}$.

3) Le randonneur se souvient avoir passé maximum 13 nuits en hébergement A. Montrer alors qu'il peut retrouver le nombre exact de nuits passées en hébergement A et en hébergement B. Quelle est la solution du problème.

EXERCICE 24

1) On considère l'équation (E) : $8x + 5y = 1$, où $(x, y) \in \mathbb{Z}^2$.

   a) Donner une solution particulière de l'équation (E).

   b) Résoudre l'équation (E).

2) Soit $n \in \mathbb{N}$ tel qu'il existe un couple (a, b) d'entiers vérifiant : $\begin{cases} n = 8a + 1 \\ n = 5b + 2. \end{cases}$

   a) Montrer que le couple $(a\ ,-b)$ est solution de (E).

   b) Quel est le reste, dans la division de n par 40 ?

3) a) Résoudre l'équation $8x + 5y = 100$, où $(x, y) \in \mathbb{Z}^2$.

   b) Au VIII^{e} siècle, un groupe d'hommes et de femmes a dépensé 100 pièces de monnaie dans une auberge. Les hommes ont dépensé 8 pièces chacun et les femmes 5 pièces chacune. Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?

EXERCICE 25

Prendre toutes les initiatives

28 personnes participent à un repas gastronomique. Le prix normal est de 26 € sauf pour les étudiants et les enfants qui paient respectivement 17 et 13 euros. La somme totale recueillie est de 613 €.

Calculer le nombre d'étudiants et d'enfants ayant participé au repas. Proposer un algorithme puis deux méthodes pour résoudre ce problème.

Bézout et Gauss

EXERCICE 26

Théorème des restes chinois

On veut déterminer l'ensemble S des entiers $n \in \mathbb{Z}$ vérifiant : $\begin{cases} n \equiv 9\ (17) \\ n \equiv 3\ (5) \end{cases}$

1) Recherche d'un élément de S.
   On désigne par (u, v) un couple d'entiers relatifs tel que : $17u + 5v = 1$.
   a) Justifier l'existence d'un tel couple (u, v).
   b) On pose $n_0 = 3 \times 17u + 9 \times 5v$. Démontrer que n_0 appartient à S.
   c) Donner un exemple d'entier n_0 appartenant à S.
2) Caractérisation des éléments de S
   a) Soit n un entier relatif appartenant à S. Démontrer que $n - n_0 \equiv 0\ (85)$.
   b) En déduire qu'un entier relatif n appartient à S si et seulement si n peut s'écrire sous 1a forme $n = 43 + 85k$ où k est un entier relatif.
3) **Application**. Zoé sait qu'elle a entre 300 et 400 jetons. Si elle fait des tas de 17 jetons, il lui en reste 9. Si elle fait des tas de 5 jetons, il lui en reste 3.
   Combien a-t-elle de jetons ?

EXERCICE 27

Vrai-Faux

On considère le système (S) $\begin{cases} n \equiv 1\ \ (5) \\ n \equiv 3\ \ (4) \end{cases}$ d'inconnue n entier relatif.

- **Affirmation 1 :** Si n est solution de (S) alors $n - 11$ est divisible par 4 et par 5.
- **Affirmation 2 :** Pour tout $k \in \mathbb{Z}$, l'entier $11 + 20k$ est solution du système.
- **Affirmation 3 :** Si n est solution de (S) alors, il existe $k \in \mathbb{Z}$ tel que $n = 11 + 20k$.

EXERCICE 28

Vrai-Faux

- **Proposition 1 :** Pour tout $n \in \mathbb{N}^*$, $3n$ et $2n + 1$ sont premiers entre eux.
- Soit S l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ solutions de l'équation $3x - 5y = 2$.
  Proposition 2 : S est l'ensemble des couples $(5k - 1, 3k - 1)$ où $k \in \mathbb{Z}$.
- Soit $a, b \in \mathbb{N}$.
  Proposition 3 : S'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 2$ alors $\text{pgcd}(a, b) = 2$.
- **Proposition 4 :** Il existe au moins un entier naturel p inférieur à 1000, multiple de 12, et dont la division euclidienne de p par un entier naturel x, inconnu lui aussi, donne 35 pour quotient et 14 pour reste ?

EXERCICE 29

Cinq entiers naturels non nuls a, b, c, d, e sont cinq termes consécutifs d'une suite géométrique dont la raison q est une entier supérieur à 1 et premier avec a.
Déterminer ces cinq entiers tels que : $6a^2 = e - b$

EXERCICE 30

Soit (u_n) la suite définie su $\mathbb{N}$ par : $\begin{cases} u_0 = 0 \\ u_{n+1} = 4u_n + 1 \end{cases}$

1) a) Calculer u_1, u_2 et u_3.

   b) Montrer que pour $n \in \mathbb{N}$, u_{n+1} et u_n sont premiers entre eux.

2) On pose pour $n \in \mathbb{N}$: $v_n = u_n + \dfrac{1}{3}$.

   a) Montrer que (v_n) est une suite géométrique.

   b) En déduire l'expression de v_n puis celle de u_n en fonction de n.

3) Calculer $\text{pgcd}(4^{n+1} - 1\ ,\ 4^n - 1)$.

Codage

EXERCICE 31

Algorithme

Soit la définition de l'opération index sur une liste et la fonction f en Python :

list.index(x) : Renvoie la position du premier élément de la liste dont la valeur égale x (en commençant à compter les positions à partir de zéro).

```
def f(lettre):
    alphabet=["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"]
    x = alphabet.index(lettre)
    y =(11*x+8)%26
    return alphabet[y]
```

Partie A

1) Que fait la fonction « .index » sur la liste alphabet ?

2) Que fait l'opération « % » dans l'expression (11*x+8)%26 ?

3) Que renvoient le programme pour f("L") et f("W") ?

4) Expliquer le procédé de codage qu'effectue cet algorithme.

Partie B

On voudrait déterminer un algorithme permettant de déchiffrer un message codé avec la fonction f

1) Montrer que pour tous $x, z \in \mathbb{Z}$, on a : $11x \equiv z\ (26) \iff x \equiv 19z\ (26)$.

2) En déduire l'équivalence : $11x + 8 \equiv y\ (26) \iff x \equiv 19y + 4\ (26)$.

3) Écrire un programme en Python avec une fonction g qui permette de décoder un message codé avec la fonction f.

EXERCICE 32

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 définit un procédé de codage de la façon suivante.

- On choisit deux entiers naturels p et q compris entre 0 et 25.
- À la lettre à coder, on associe l'entier x correspondant dans le tableau.
- On calcule l'entier y défini par les relations : $y \equiv px + q\ (26)$ et $0 \leqslant y \leqslant 25$.
- À l'entier y, on associe la lettre correspondante dans le tableau.

1) On choisit $p = 9$ et $q = 2$.
   a) Démontrer que la lettre V est codée par la lettre J.
   b) Citer le théorème qui permet d'affirmer l'existence de deux entiers relatifs u et v tels que : $9u + 26v = 1$.
   Donner sans justifier un couple (u, v) qui convient.
   c) Démontrer que : $y \equiv 9x + 2\ (26) \quad \Leftrightarrow \quad x \equiv 3y + 20\ (26)$.
   d) Décoder la lettre R.
2) On choisit $q = 2$ et p est inconnu. On sait que J est codé par D.
   Déterminer la valeur de p (on admettra que p est unique).
3) On choisit $p = 13$ et $q = 2$.
   Coder les lettres B et D. Que peut-on dire de ce codage ?

EXERCICE 33

Une personne a mis au point le procédé de cryptage suivant :

- À chaque lettre de l'alphabet, on associe un entier n comme à l'exercice précédent :
- 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 les couples (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 : $\forall n, m \in \mathbb{N},\ m \equiv 9n+4\ (26) \Leftrightarrow n \equiv 3m+14\ (26)$
   b) Décoder le mot AQ.

EXERCICE 34

Chiffrement de Hill

Le chiffrement de Hill a été publie en 1929. C'est un chiffre non polygraphique, c'est-a-dire qu'on ne chiffre pas les lettres les unes après les autres, mais par ?« paquets ». On présente ici un exemple bigraphique, c'est a dire que les lettres sont regroupées deux a deux.

- On regroupe les lettres par paquets de 2. Chaque lettre est remplacée par un entier en utilisant le tableau .

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 obtient des couples d'entiers (x_1, x_2) où x_1 correspond à la première lettre et x_2 à la deuxième.

- Chaque couple (x_1, x_2) est transformé en (y_1, y_2) tel que :

$$(S_1) : \begin{cases} y_1 \equiv 11x_1 + 3x_2\ (26) \\ y2 \equiv 7x_1 + 4x_2\ (26) \end{cases} \quad \text{avec} \quad \begin{cases} 0 \leqslant y_1 \leqslant 25 \\ 0 \leqslant y_2 \leqslant 25 \end{cases}$$

- Chaque couple (y_1, y_2) est transformé en un couple de deux lettres en utilisant le tableau donné précédemment. On regroupe ensuite les lettres.

Exemple : TE $\rightarrow (19,4) \rightarrow \begin{cases} 11 \times 19 + 3 \times 4 \equiv 13\ (26) \\ 7 \times 19 + 4 \times 4 \equiv 19\ (26) \end{cases} \rightarrow$ NT.

1) Coder le mot ST.

2) a) Compléter l'algorithme en Python permettant de coder un groupe de deux lettres :

```
def hill(lettre1,lettre2):
    alphabet=["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"]
    x1=alphabet.index(lettre1)
    x2=alphabet.index(lettre2)
    y1= ...
    y2= ...
    return ... , ...
```

b) À l'aide de cet algorithme coder les mots PALACE et RAPACE.

c) Que constatez-vous ?

3) On veut maintenant déterminer la procédure de déchiffrement.

a) Montrer que tout couple (x_1, x_2) vérifiant $(S1)$, vérifie le système :

$$(S2) \ : \ \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \ (26) \\ 23x_2 \equiv 19y_1 + 11y_2 \ (26) \end{cases}$$

b) Montrer que pour tout $a, b \in \mathbb{Z}$: $23a \equiv b \ (26) \ \Leftrightarrow \ a \equiv 17b \ (26)$.

c) En déduire alors que tout couple (x_1, x_2) vérifiant $(S2)$, vérifie le système :

$$(S3) \ : \ \begin{cases} x_1 \equiv 16y_1 + y_2 \ (26) \\ x_2 \equiv 11y_1 + 5y_2 \ (26) \end{cases}$$

d) Écrire une fonction en Python sur le même principe que la fonction hill de chiffrage pour déchiffrer un mot.

e) Décoder le mot : PFXXKNU. Ce mot étant de 7 lettres, ajouter la lettre W à la fin du mot pour avoir des paquets de deux lettres. Le décodage terminé, supprimer la dernière lettre.

Rationalité d'un nombre

EXERCICE 35

On considère le polynôme du second degré : $P(x) = x^2 + ax + b$ où $a, b \in \mathbb{Z}$.

1) Montrer que si $P(x) = 0$ admet une solution rationnelle α, alors α est entier.

2) En déduire que $\sqrt{n}$, avec $n \in \mathbb{N}$, est soit un entier soit un irrationnel.

EXERCICE 36

On considère le polynôme : $P(x) = x^3 + ax^2 + bx + c$ où $a, b, c \in \mathbb{Z}$.

1) Montrer que si $P(x) = 0$ admet une solution rationnelle α, alors α est entier.

2) En déduire que $\sqrt[3]{n}$, avec $n \in \mathbb{Z}$, est soit un entier soit un irrationnel.

EXERCICE 37

1) Vérifier que $\dfrac{\ln 2}{\ln 3} > 0$.

2) On suppose que $\dfrac{\ln 2}{\ln 3} = \dfrac{p}{q}$ avec $\text{pgcd}(p, q) = 1$ et $p, q \in \mathbb{N}^*$
Montrer alors que $2^q = 3^p$.

3) En déduire que $\dfrac{\ln 2}{\ln 3}$ n'est pas un nombre rationnel

EXERCICE 38

On pose $\alpha = \sqrt{2} + \sqrt{3}$.

1) Calculer α^2 puis $(\alpha^2 - 5)^2$.

2) Déterminer un polynôme du 4e degré pour lequel α est une racine.
3) Prouver que α est irrationnel.

EXERCICE 39

On considère le polynôme $P(x) = x^3 + x^2 - 2x - 1$ et $p \in \mathbb{Z},\ q \in \mathbb{N}^*$.
On suppose que P admet une racine rationnelle $r = \dfrac{p}{q}$ avec $\text{pgcd}(p, q) = 1$

1) Justifier que p divise q^3 puis que p divise q. En déduire que $p = \pm 1$.
2) Par un procédé identique, montrer que $q = 1$.
3) En déduire alors que le polynôme P n'admet pas de solution rationnelle.

EXERCICE 40

Soit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux.
Soit f le polynôme : $f(x) = 2x^3 + 5x^2 + 5x + 3$.

1) Montrer que si $\dfrac{p}{q}$ est une racine de f alors p divise 3 et q divise 2.
2) Déduire que f admet une solution rationnelle.

EXERCICE 41

Soit f le polynôme : $f(x) = x^4 - 4x^3 - 8x^2 + 13x + 10$.

1) Montrer que si $f(x) = 0$ admet une solution rationnelle α alors α est un entier.
2) Montrer que si α est une solution entière de $f(x) = 0$ alors, α divise 10.
3) Trouver les racines entières éventuelle de $f(x) = 0$.

EXERCICE 42

Équation de Pell-Fermat

On étudie les équations du type $x^2 - ny^2 = 1$ où $n \in \mathbb{N}$ non carré.

Partie A : Équation E_1 : $x^2 - 2y^2 = 1$

1) Soit (a, b) une solution de E_1.
   a) Quelle est la parité de a et de b ?
   b) Déterminer $\text{pgcd}(a, b)$.
   c) On pose : $A = 3a + 4b$ et $B = 2a + 3b$.
   Montrer que (A, B) est aussi solution de E_1.
2) a) Déterminer une solution de E_1.
   b) Déduire de la question 1 c) une solution avec des entiers supérieurs à 100.
3) Déterminer, à l'aide d'une boucle conditionnelle, un algorithme, écrit en Python, qui donne un couple solution de E_1 d'entiers supérieurs à 1 000.

Partie B : Équation E_2 : $x^2 - 3y^2 = 1$

1) Déterminer la plus petite solution non triviale c'est-à-dire différente de $(1\,;0)$.
Cette solution est appelée solution fondamentale et on la note (x_0, y_0).

2) a) Vérifier l'identité de Brahmagupta pour tout entiers relatifs a_1, a_2, b_1, b_2 et n :

$$(a_1^2 - nb_1^2)(a_2^2 - nb_2^2) = (a_1a_2 + nb_1b_2)^2 - n(a_1b_2 + b_1a_2)^2$$

b) En déduire à partir de cette relation, en prenant $n = 3$, une autre solution (x_1, y_1) de E_2 connaissant (x_0, y_0).

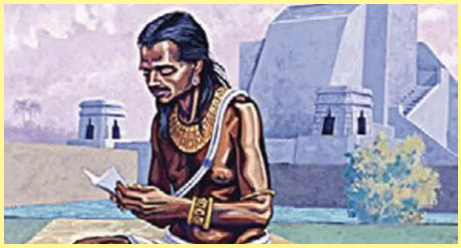
c) Soit (x_n, y_n) une solution générale de l'équation E_2, montrer la relation de récurrence donnant la solution (x_{n+1}, y_{n+1}) en fonction de (x_n, y_n) :

$$\begin{cases} x_{n+1} = 2x_n + 3y_n \\ y_{n+1} = x_n + 2y_n \end{cases}$$

d) Déterminer les 10 premières solutions de l'équation E_2, à l'aide d'un algorithme, écrit en Python .

Partie C : Équation de Brahmagupta E_3 : $x^2 - 92y^2 = 1$

1) Déterminer un algorithme en Python permettant de trouver la solution fondamentale, autre que la solution (1,0) à l'équation E_3.
2) Rentrer cet algorithme et donner cette solution.
3) Peut-on en déterminer une autre ? Si oui comment est-elle déterminée.



L'équation $x^2 - ny^2 = 1$ porte le nom du mathématicien anglais John Pell, mais c'est une erreur due à Euler qui lui attribua faussement son étude. En fait, le premier à avoir décrit l'ensemble des solutions de cette équation est le mathématicien indien Brahmagupta, qui vivait au VII^e siècle après J.-C., soit près de 1 000 ans avant Pell. Ses résultats étaient totalement inconnus des mathématiciens européens du XVII^e siècle et c'est Fermat qui remit cette équation au goût du jour, conjecturant qu'elle avait toujours une infinité de solutions.
Enfin Lagrange, un siècle plus tard, donne une preuve totalement rigoureuse de l'infinité des solutions.