

Fiche d'exercices

PGCD, THÉORÈMES DE BÉZOUT ET DE GAUSS.

Exercice 1 (Équations diophantiennes)

1. Parmi les équations suivantes où $(x ; y) \in \mathbb{Z}^2$, quelles sont celles qui admettent des solutions ? Justifier.

$$(E_1) : 28x - 33y = 1$$

$$(E_2) : 32x + 28y = 8$$

$$(E_3) : 7x - 32y = -5$$

$$(E_4) : 222x - 72y = 8$$

$$(E_5) : 99x + 58y = 1$$

$$(E_6) : 17x + 13y = 22$$

2. À l'aide de l'algorithme d'Euclide, déterminer une solution particulière de (E_1) , (E_2) et (E_3) .

3. À l'aide de la calculatrice, déterminer une solution de (E_5) et (E_6) .

4. Résoudre (E_6) .

Exercice 2 (Obtenir un couple de Bézout avec Python)

On souhaite déterminer une solution particulière de l'équation $(E) : au + bv = 1$ où a et b sont deux entiers naturels non nuls donnés.

1. À quelle condition l'équation (E) admet-elle une solution ?

2. Écrire une fonction Python `PGCD`, qui prend en argument deux entiers naturels et renvoie le PGCD de ces deux nombres.

3. Soit $(u ; v) \in \mathbb{Z}^2$ une solution de (E) . Exprimer v en fonction de a , b et u .

4. Dans cette question uniquement, on suppose que a et b sont premiers entre eux. On peut démontrer et on admettra qu'alors (E) admet au moins une solution $(u ; v)$ avec $u \in \mathbb{N}$.

Compléter l'algorithme ci-contre, écrit en langage naturel, de sorte qu'à la fin les variables U et V contiennent des entiers tels que $aU + bV = 1$.

5. Programmer en Python une fonction `bezout`, qui prend en argument deux entiers naturels, teste s'ils sont premiers entre eux à l'aide de la fonction `PGCD`, et dans ce cas renvoie un couple de Bézout, c-à-d un couple d'entiers $(u ; v)$ tel que $au + bv = 1$.

6. Utiliser le programme obtenu pour déterminer une solution particulière de l'équation $245u + 124v = 1$.

7. En adaptant la fonction `bezout` précédente, écrire une fonction `bezout2` qui prend en argument deux entiers naturels a et b et renvoie un couple de Bézout, c-à-d un couple d'entiers $(u ; v)$ tel que $au + bv = \text{PGCD}(a, b)$.

8. Vérifier avec la fonction `PGCD` que $\text{PGCD}(126, 294) = 42$ puis déterminer une solution de l'équation $126u + 294v = 42$ à l'aide de la fonction `bezout2`.

```
U ← 0
V ← .....
Tant que V n'est pas entier :
    U ← U + 1
    V ← .....
Fin Tant que
```

Exercice 3 (Inverse de a modulo n)

Soient a un entier relatif et n un entier naturel, $n \geq 2$.

On dit que l'entier a est *inversible modulo n* s'il existe un entier x tel que $ax \equiv 1 (n)$.

Dans ce cas, un tel entier x s'appelle alors *un inverse de a modulo n* .

1. a) À l'aide d'un tableau de congruences, déterminer si 4 est inversible modulo 6, puis modulo 7.

b) Donner trois inverses de 4 modulo 7.

2. Prouver que a est inversible modulo n si, et seulement si, a et n sont premiers entre eux.

3. On suppose que a est inversible modulo n .

Prouver qu'il existe un unique inverse de a modulo n , compris entre 1 et $n - 1$.

4. a) Déterminer un inverse de 17 modulo 43.

b) Résoudre alors dans $\mathbb{Z}$ les équations : $(E_1) : 17x \equiv 1 (43)$; $(E_2) : 17x \equiv 8 (43)$.

Exercice 4 (Pêle-mêle)

Les six questions suivantes sont indépendantes.

1. Calculer $\text{PGCD}(2^3 \times 5^2 \times 13^5, 2^2 \times 5^2 \times 13^4 \times 17)$.
2. Soient a et b deux entiers relatifs. Démontrer que a et b sont premiers entre eux si et seulement si a et b^2 sont premiers entre eux.
3. Soient m et n deux entiers naturels non nuls. On rappelle que $\mathbb{U}_n$ désigne l'ensemble des complexes z tels que $z^n = 1$.
 - a) Montrer que si m divise n , alors $\mathbb{U}_m \subset \mathbb{U}_n$.
 - b) On note $d = \text{PGCD}(m, n)$. Démontrer que $\mathbb{U}_d = \mathbb{U}_m \cap \mathbb{U}_n$.
4.
 - a) Quel est le reste de la division euclidienne de 6^{10} par 11 ? Justifier.
 - b) Quel est le reste de la division euclidienne de 6^4 par 5 ? Justifier.
 - c) Démontrer que $6^{40} - 1$ est divisible par 55.
5. Dans cette question x et y désignent des entiers relatifs.
 - a) Montrer que l'équation $(E) : 65x - 40y = 1$ n'a pas de solution.
 - b) Montrer que l'équation $(E') : 17x - 40y = 1$ admet au moins une solution.
 - c) Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation (E') .
 - d) Résoudre l'équation (E') . En déduire qu'il existe un unique naturel x_0 inférieur à 40 tel que $17x_0 \equiv 1 \pmod{40}$.
 - e) Pour tout entier naturel a , prouver que si $a^{17} \equiv b \pmod{55}$ et si $a^{40} \equiv 1 \pmod{55}$, alors $b^{33} \equiv a \pmod{55}$.
6. On se propose d'étudier des couples $(a ; b)$ d'entiers strictement positifs, tels que : $a^2 = b^3$.
 - a) Soit $(a ; b)$ un tel couple et $d = \text{PGCD}(a, b)$. On note u et v les entiers tels que $a = du$ et $b = dv$.
Montrer que $u^2 = dv^3$ puis que $v = 1$.
 - b) Soit $(a ; b)$ un couple d'entiers strictement positifs.
Démontrer que l'on a $a^2 = b^3$ si et seulement si a et b sont respectivement le cube et le carré d'un même entier.

Exercice 5 (PGCD d'expressions littérales)

Les sept questions suivantes sont indépendantes.

1. Soit n un entier naturel tel que $n > 1$. On pose $A = n^2 + 4n + 5$ et $B = n + 1$.
 - a) Justifier que dans la division euclidienne de A par B , le quotient est $n + 3$ et le reste est 2.
 - b) En déduire que $\text{PGCD}(A, B) = \text{PGCD}(n + 1, 2)$.
 - c) Pour quelles valeurs de n la fraction $\frac{A}{B}$ est-elle irréductible ?
2. Soient a et b deux entiers naturels non nuls premiers entre eux. Démontrer que la fraction $\frac{4a + 15b}{3a + 11b}$ est irréductible.
3. Soit n un entier naturel non nul.
 - a) Vérifier que $2n^2 + 12n + 13 = (2n + 2)(n + 5) + 3$.
 - b) On note $d = \text{PGCD}(2n^2 + 12n + 13 ; n + 5)$. Justifier que $d = \text{PGCD}(n + 5 ; 3)$.
 - c) Déterminer d selon les valeurs de n .
4. Pour tout entier naturel n non nul, on pose $a = 5n + 1$ et $b = 2n - 1$. On note $d = \text{PGCD}(a, b)$.
 - a) Prouver que les valeurs possibles de d sont 1 et 7.
 - b) Déterminer les entiers n tels que $a \equiv 0 \pmod{7}$ et $b \equiv 0 \pmod{7}$.
 - c) En déduire la valeur de d selon les valeurs de n .
5. Soit n un entier naturel non nul. On pose $A = 2n^3 + 5n^2 + 4n + 1$ et $B = 2n^2 + n$.
 - a) Prouver que $2n + 1$ divise A et B .
 - b) Démontrer que $\text{PGCD}(A, B) = 2n + 1$.
6. Soit n un entier naturel. Démontrer que les entiers $2n + 3$ et $n + 3$ sont premiers entre eux si et seulement si n n'est pas un multiple de 3.
Indication : on pourra commencer par prouver que $\text{PGCD}(2n + 3, n + 3) = \text{PGCD}(n, 3)$.
7. Soit p un entier naturel. On pose $a = 7p + 4$ et $b = 5p + 2$.
 - a) Prouver que $\text{PGCD}(a, b) = \text{PGCD}(6, p + 4)$.
 - b) Déterminer $\text{PGCD}(a, b)$ selon les valeurs de p .

Exercice 6 (Nombres de Fermat)

Pour tout entier naturel n , on note F_n le n -ième nombre de Fermat. Il est défini par $F_n = 2^{2^n} + 1$.
L'objectif est de prouver que deux nombres de Fermat distincts sont toujours premiers entre eux.

1. Démontrer que pour tout entier naturel n non nul on a $F_n = (F_{n-1} - 1)^2 + 1$.
2. Pour tout entier naturel n on note : $\prod_{i=0}^n F_i = F_0 \times F_1 \times F_2 \times \dots \times F_{n-1} \times F_n$. On a donc $\prod_{i=0}^n F_i = \left(\prod_{i=0}^{n-1} F_i \right) \times F_n$.
Montrer par récurrence et en utilisant le résultat de la question 1 que pour tout entier naturel n non nul, $\prod_{i=0}^{n-1} F_i = F_n - 2$.
3. Justifier que, pour tous entiers naturels n et m tels que $n > m$, il existe un entier naturel q tel que $F_n - qF_m = 2$.
4. En déduire que deux nombres de Fermat sont toujours premiers entre eux.

Exercice 7 (Suite et PGCD)

On considère la suite définie par son premier terme $u_0 = 3$ et, pour tout entier naturel n , par $u_{n+1} = 2u_n + 6$.

1. Démontrer que, pour tout entier naturel n , $u_n = 9 \times 2^n - 6$.
2. Démontrer que, pour tout entier $n \geq 1$, u_n est divisible par 6.
On définit la suite d'entiers (v_n) par, pour tout entier naturel $n \geq 1$, $v_n = \frac{u_n}{6}$.
3. a) Démontrer que, pour tout entier $n \geq 1$, $v_{n+1} - 2v_n = 1$.
b) En déduire que, pour tout entier $n \geq 1$, v_n et v_{n+1} sont premiers entre eux.
c) En déduire, pour tout entier $n \geq 1$, le PGCD de u_n et u_{n+1} .
4. a) Vérifier que $2^4 \equiv 1 [5]$.
b) En déduire que si n est de la forme $4k + 2$ avec k entier naturel, alors u_n est divisible par 5.
c) Le nombre u_n est-il divisible par 5 pour les autres valeurs de l'entier naturel n ? Justifier.

Exercice 8 (Recherche de points à coordonnées entières)

1. Soit p un entier relatif donné.
On s'intéresse dans cette question à l'équation $(E_p) : 3x + 4y = p$, où $(x ; y)$ est un couple d'entiers relatifs.
 - a) Vérifier que le couple $(-p ; p)$ est une solution particulière de l'équation.
 - b) Prouver que l'ensemble des solutions de (E_p) est l'ensemble des couples de la forme $(-p + 4k ; p - 3k)$ où k est un entier relatif.
2. Dans le plan rapporté à un repère orthonormé $(O ; \vec{i}, \vec{j})$, on donne les points $A(-3 ; 0)$ et $B(29 ; -24)$.
 - a) Déterminer une équation cartésienne de la droite (AB) .
 - b) Déterminer les points du segment $[AB]$ dont les coordonnées sont entières.
3. Dans cette question, l'espace est muni d'un repère orthonormé $(O ; \vec{i}, \vec{j}, \vec{k})$.
On considère le plan $\mathcal{P}$ d'équation cartésienne $6x + 8y - z = 0$.
Soit M_0 un point de coordonnées $(x_0 ; y_0 ; z_0)$ qui appartient au plan $\mathcal{P}$ et dont les trois coordonnées sont des entiers relatifs.
 - a) Démontrer que z_0 est pair.
 - b) On pose $z_0 = 2p$ où p est un entier relatif. Prouver que le couple $(x_0 ; y_0)$ est solution de l'équation (E_p) .
 - c) En utilisant la question 1, déterminer l'ensemble des points du plan $\mathcal{P}$ à coordonnées entières.

Exercice 9 (L'équation diophantienne du randonneur)

En montagne, un randonneur a effectué des réservations dans deux types d'hébergements : 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 nombres x et y sont respectivement inférieurs ou égaux à 18 et 9.
b) Compléter le script de la fonction Python `nuitées` de sorte qu'elle renvoie les couples $(x ; y)$ possibles.

```
1 def nuitées():  
2     L=[]  
3     for x in range(.....):  
4         for y in range(.....):  
5             if .....:  
6                 .....  
7     return L
```

2. a) Justifier que l'équation $8x + 15y = 1$ admet pour solution au moins un couple d'entiers relatifs.
b) Déterminer une telle solution.
c) Résoudre l'équation (E) : $8x + 15y = 146$ où x et y sont des nombres entiers relatifs.
3. Le randonneur se souvient avoir passé au maximum 13 nuits en hébergement A.
Montrer alors qu'il peut retrouver le nombre exact de nuits passées en hébergement A et celui des nuits passées en hébergement B. Calculer ces nombres.

Exercice 10 (Un chiffrement affine)

Pour coder un message, on procède de la manière suivante : à chacune des 26 lettres de l'alphabet, on commence par associer un entier n de l'ensemble $\Omega = \{0 ; 1 ; 2 ; \dots ; 24 ; 25\}$ selon 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

a et b étant deux entiers naturels donnés, on associe à tout entier n de Ω le reste de la division euclidienne de $(an + b)$ par 26 ; ce reste est alors associé à la lettre correspondante.

Exemple : pour coder la lettre P avec $a = 2$ et $b = 3$, on procède de la manière suivante :

étape 1 : on lui associe l'entier $n = 15$.

étape 2 : le reste de la division de $2 \times 15 + 3 = 33$ par 26 est 7.

étape 3 : on associe 7 à H. Donc P est codé par la lettre H.

1. Que dire alors du codage obtenu lorsque l'on prend $a = 0$?
2. Montrer que les lettres A et C sont codées par la même lettre lorsque l'on choisit $a = 13$.
3. Dans toute la suite de l'exercice, on prend $a = 5$ et $b = 2$.
 - a) On considère deux lettres de l'alphabet associées respectivement aux entiers n et p . Montrer, que si $5n + 2$ et $5p + 2$ ont le même reste dans la division par 26 alors $n - p$ est un multiple de 26. En déduire que $n = p$.
 - b) Coder le mot AMI.
4. On se propose de décoder la lettre E.
 - a) Montrer que décoder la lettre E revient à déterminer l'élément n de Ω tel que $5n - 26y = 2$, où y est un entier.
 - b) On considère l'équation $5x - 26y = 2$, avec x et y entiers relatifs.
 - i. Donner une solution particulière de l'équation $5x - 26y = 2$.
 - ii. Résoudre alors l'équation $5x - 26y = 2$.
 - iii. En déduire qu'il existe un unique couple $(x ; y)$ solution de l'équation précédente, avec $0 \leq x \leq 25$.
 - c) Décoder alors la lettre E.

Exercice 11 (Le chiffrement de Hill)

Partie A – Inverse de 23 modulo 26

On considère l'équation $(E) : 23x - 26y = 1$, où x et y désignent deux entiers relatifs.

1. Vérifier que le couple $(-9 ; -8)$ est solution de l'équation (E) .
2. Résoudre alors l'équation (E) .
3. En déduire un entier a tel que $0 \leq a \leq 25$ et $23a \equiv 1 \pmod{26}$.

Partie B – Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

Étape 1 Chaque lettre du mot est remplacée par un entier en utilisant 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

On obtient un couple d'entiers $(x_1 ; x_2)$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 $(x_1 ; x_2)$ est transformé en $(y_1 ; y_2)$ tel que :

$$(S_1) \begin{cases} y_1 & \equiv 11x_1 + 3x_2 & (\text{mod } 26) \\ y_2 & \equiv 7x_1 + 4x_2 & (\text{mod } 26) \end{cases} \quad \text{avec } 0 \leq y_1 \leq 25 \text{ et } 0 \leq y_2 \leq 25.$$

Étape 3 $(y_1 ; y_2)$ est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple : $\underbrace{\text{TE}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (19,4) \xrightarrow{\text{étape 2}} (13,19) \xrightarrow{\text{étape 3}} \underbrace{\text{NT}}_{\text{mot codé}}$

1. Coder le mot ST.
2. On veut maintenant déterminer la procédure de décodage :
 - a) Montrer que tout couple $(x_1 ; x_2)$ vérifiant les équations du système (S_1) , vérifie les équations du système :

$$(S_2) \begin{cases} 23x_1 & \equiv 4y_1 + 23y_2 & (\text{mod } 26) \\ 23x_2 & \equiv 19y_1 + 11y_2 & (\text{mod } 26) \end{cases}$$

- b) À l'aide de la **partie A**, montrer que tout couple $(x_1 ; x_2)$ vérifiant les équations du système (S_2) , vérifie les équations du système :

$$(S_3) \begin{cases} x_1 & \equiv 16y_1 + y_2 & (\text{mod } 26) \\ x_2 & \equiv 11y_1 + 5y_2 & (\text{mod } 26) \end{cases}$$

- c) Montrer que tout couple $(x_1 ; x_2)$ vérifiant les équations du système (S_3) , vérifie les équations du système (S_1) .
- d) Décoder le mot YJ.

Exercice 12 (Un système de congruences)

1. On se propose, dans cette question, de déterminer tous les entiers relatifs N tels que : $\begin{cases} N \equiv 5 & (13) \\ N \equiv 1 & (17) \end{cases}$
 - a) Soit N un entier relatif solution de ce système. Démontrer que N peut s'écrire sous la forme $N = 1 + 17x = 5 + 13y$ où x et y sont deux entiers relatifs vérifiant la relation $17x - 13y = 4$.
 - b) Résoudre l'équation $17x - 13y = 4$ où x et y sont des entiers relatifs.
 - c) En déduire qu'il existe un entier relatif k tel que $N = 18 + 221k$.
 - d) Démontrer l'équivalence entre $N \equiv 18 \pmod{221}$ et $\begin{cases} N \equiv 5 & (13) \\ N \equiv 1 & (17) \end{cases}$.
2. *Applications.*
 - a) Zoé sait qu'elle a entre 600 et 700 jetons. Si elle fait des tas de 13 jetons, il lui en reste 5. Si elle fait des tas de 17 jetons, il lui en reste 1. Combien a-t-elle de jetons ?
 - b) Existe-t-il un entier naturel n tel que $10^n \equiv 18 \pmod{221}$?

Exercice 13 (Le manège)

1. On considère l'équation $(\mathcal{E}) : 17x - 24y = 9$, où $(x ; y)$ est un couple d'entiers relatifs.

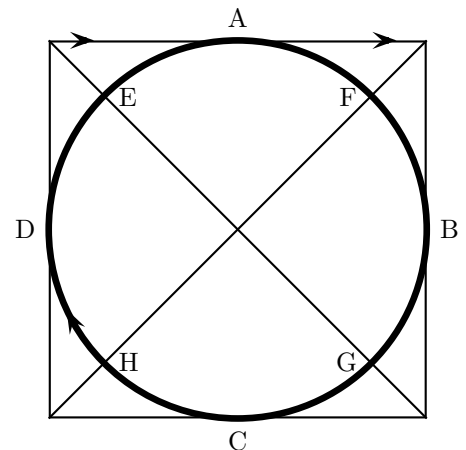
- Vérifier que le couple $(9 ; 6)$ est solution de l'équation $(\mathcal{E})$.
- Résoudre l'équation $(\mathcal{E})$.

2. Dans une fête foraine, Jean s'installe dans un manège circulaire représenté par le schéma ci-contre. Il peut s'installer sur l'un des huit points indiqués sur le cercle.

Le manège comporte un jeu qui consiste à attraper un pompon qui, se déplace sur un câble formant un carré dans lequel est inscrit le cercle. Le manège tourne dans le sens des aiguilles d'une montre, à vitesse constante. Il fait un tour à vitesse constante. Il fait un tour en 24 secondes. Le pompon se déplace dans le même sens à vitesse constante. Il fait un tour en 17 secondes.

Pour gagner, Jean doit attraper le pompon, et il ne peut le faire qu'aux points de contact qui sont notés A, B, C et D sur le dessin.

À l'instant $t = 0$, Jean part du point H en même temps que le pompon part du point A.



- On suppose qu'à un certain instant t Jean attrape le pompon en A. Jean a déjà pu passer un certain nombre de fois en A sans y trouver le pompon. À l'instant t , on note y le nombre de tours effectués depuis son premier passage en A et x le nombre de tours effectués par le pompon. Montrer que $(x ; y)$ est solution de l'équation $(\mathcal{E})$ de la question 1.
- Jean a payé pour 2 minutes ; aura-t-il le temps d'attraper le pompon ?
- Montrer que, si Jean attrape le pompon en B, alors le couple $(x ; y)$ est solution de l'équation $68x - 96y = 43$. Jean peut-il attraper le pompon en B ?
On peut montrer de même qu'il n'est possible d'attraper le pompon qu'au point A.

Exercice 14 (Suite et PGCD)

Soit (U_n) la suite numérique définie par :
$$\begin{cases} U_0 &= 0 \\ U_{n+1} &= 2U_n + 1 \end{cases} \text{ pour tout } n \in \mathbb{N}$$

1. Montrer que, pour tout entier naturel n , U_{n+1} et U_n sont premiers entre eux.

2. Montrer que pour tout entier naturel n , $U_n = 2^n - 1$.

3. Montrer que, pour tous entiers naturels n et p , $U_{n+p} = U_p(U_n + 1) + U_n$.

4. Soient n et p deux entiers naturels non nuls.

- Montrer que $\mathcal{D}(U_n, U_p) = \mathcal{D}(U_{n+p}, U_p)$ puis en déduire que $\text{PGCD}(U_n, U_p) = \text{PGCD}(U_{n+p}, U_p)$.
- Prouver que si r désigne le reste de la division euclidienne de n par p , alors $\text{PGCD}(U_n, U_p) = \text{PGCD}(U_p, U_r)$.
- En déduire que $\text{PGCD}(U_n, U_p) = U_{\text{PGCD}(n, p)}$.

5. Déterminer $\text{PGCD}(2^{1000} - 1, 2^{15} - 1)$.