T^ale spé Maths expertes
J. Bérard

Lycée Saint-Augustin

2025–2026

TD 22 **PGCD de deux entiers**

Exercice 1 (★☆☆☆) Calcul d'un pgcd

1. Existe-t-il des entiers relatifs n tels que 3 divise n^2+1 ?
2. En déduire, quel que soit $n \in \mathbb{Z}$, le pgcd $\left(7n^2+4, n^2+1\right)$.

Exercice 2 (★★☆☆) Une fraction réductible

1. Trouver les 5 premiers entiers naturels n impairs tels que la fraction

$$\frac{n^3-n}{n+2} \text{ soit réductible.}$$

   Qu'observez-vous ?
2. Quel que soit $n \in \mathbb{N}$, justifier que

$$\text{pgcd}\left(n^3-n, n+2\right) = \text{pgcd}(n+2, 6).$$

   En déduire la preuve de la conjecture émise à la question 1.

Exercice 3 (★★☆☆) pgcd par soustraction

Soient a et b deux entiers naturels non nuls tels que $a > b$.

1. Prouver l'égalité

$$\text{Div}(a,b) = \text{Div}(b, a-b).$$

   En déduire que $\text{pgcd}(a,b) = \text{pgcd}(b, a-b)$.
2. Que restitue le script Python qui suit ?

```
def pgcdsoustrac(a,b):
    while a-b!=0:
        if a>b:
            c=a-b
            a=c
        if b>a:
            c=b-a
            b=c
    return a
```

Exercice 4 (★★★☆) Nombres de Mersenne

Soit $n \in \mathbb{N}^*$. Le n-ième nombre de Mersenne est l'entier naturel

$$M_n = 2^n - 1.$$

1. En utilisant l'algorithme d'Euclide, calculer pgcd (M_{12}, M_8), puis pgcd (M_{14}, M_{10}). Quelle conjecture peut-on émettre ?

2. Soient m et n deux entiers tels que $0 < m \leqslant n$. On pose $D = \text{pgcd}\,(M_n,M_m)$.
Montrer que si r est le reste de la division euclidienne de n par m, alors M_r est le reste de la division euclidienne de M_n par M_m. En déduire que $D = M_{\text{pgcd}(n,m)}$.

3. Lorsque n et m sont premiers entre eux, que peut-on dire de M_n et M_m ?

Exercice 5 (★★★☆) Une équation diophantienne

Dans $\mathbb{Z}^2$, nous considérons l'équation

$$x + y - 1 = \text{pgcd}(x,y) \tag{E}$$

1. Justifier que si (x,y) est une solution de (E), alors $\text{pgcd}(x,y) = 1$.

2. En déduire que si (x,y) est une solution de (E), alors x est impair.

3. Déterminer l'ensemble de solutions de l'équation (E).

Exercice 6 (★★★☆) Racines n-ièmes de l'unité et divisibilité

Nous verrons au chapitre 26 que l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est défini par

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

Soient m et n deux entiers naturels non nuls.

1. Montrer que si m divise n, alors $\mathbb{U}_m \subset \mathbb{U}_n$.

2. Prouver que $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{\text{pgcd}(m,n)}$. Examiner le cas où m et n sont premiers entre eux.

Exercice 7 (★★★★) PGCD de deux nombres de Fermat

Un nombre de Pierre de Fermat, noté F_n, est un entier naturel défini par

$$\forall\, n \in \mathbb{N}, \quad F_n = 2^{2^n} + 1.$$

Nous souhaitons déterminer le pgcd de deux nombres de Fermat distincts.
Soient $n \in \mathbb{N}$ et $p \in \mathbb{N}^*$.

1. Proposer un script Python qui restitue $\text{pgcd}\,(F_n,F_{n+p})$. Quelle conjecture peut-on énoncer ?

2. Preuve de cette conjecture.
Le binôme de Newton est pré-requis. Nous donnerons une autre preuve lors de l'exercice 8 qui suit.

a) Justifier l'égalité

$$F_{n+p} - 1 = (F_n - 1)^{2^p}.$$

b) En déduire que F_n divise $F_{n+p} - 2$.

c) Quel est le $\text{pgcd}\,(F_{n+p},F_n)$? Conclure.

Exercice 8 (★★★★) Une autre preuve de l'exercice précédent

Les données sont celles de l'exercice 7.

1. Nous considérons le polynôme P défini sur $\mathbb{R}$ par

$$P(x) = x^{2^p} - 1.$$

Justifier qu'il existe un polynôme Q tel que, pour tout réel x,

$$P(x) = (x+1)Q(x).$$

2. Établir que $P\left(2^{2^n}\right) = F_{n+p} - 2$. Conclure.

Exercice 9 (★★★☆) PGCD puissance n

1. Soient a et b deux entiers relatifs premiers entre eux. Prouver que, quel que soit $n \in \mathbb{N}^*$,a^n et b^n sont premiers entre eux.
2. Soient a et b deux entiers relatifs non nuls. Établir que, quel que soit $n \in \mathbb{N}^*$,

$$\text{pgcd}\,(a^n,b^n) = (\text{pgcd}(a,b))^n.$$

Exercice 10 (★★★★) Une application de l'exercice précédent

1. Pour tout $n \in \mathbb{N}^*$, nous posons $S_n = \sum_{k=1}^{n} k^3$. Justifier que, quel que soit $n \in \mathbb{N}^*$, $S_n = \left(\frac{n(n+1)}{2}\right)^2$.
2. Déterminer, pour tout $n \in \mathbb{N}^*$, $D_n = \text{pgcd}\,(S_n,S_{n+1})$.
3. Prouver, pour tout $n \in \mathbb{N}^*$, que les entiers D_n et S_{n+2} sont premiers entre eux.

Exercice 11 (★★★☆) Divisibilité des coefficients binomiaux

Nous rappelons que, quels que soient les entiers naturels n et k tels que $0 \leqslant k \leqslant n$,

$$\binom{n}{k} \in \mathbb{N}.$$

Soient $p \in \mathbb{N}^*$ et $k \in \mathbb{N}^*$ tels que $1 \leqslant k \leqslant p$.

1. Justifier l'égalité

$$k \times \binom{p}{k} = n \times \binom{p-1}{k-1}.$$

En déduire que si p et k sont premiers entre eux, alors

$$\binom{p}{k} \equiv 0\ [p].$$

2. Nous supposons que l'entier p est un nombre premier. Monter que, quels que soient les entiers a et b,

$$(a+b)^p \equiv a^p + b^p\ [p].$$

Exercice 12 (★★★☆) Le théorème chinois : un exemple

1. Résoudre dans $\mathbb{Z}^2$ l'équation

$$35x - 4y = 1 \tag{E}$$

2. On désigne par S l'ensemble des entiers relatifs n tels que

$$\begin{cases} n \equiv 1\ [5] \\ n \equiv 5\ [7] \end{cases}$$

Montrer que si $n \in S$, alors 35 divise $4n+1$.

3. Prouver que $S = \{-9 + 35k \mid k \in \mathbb{Z}\}$.
4. Vrai ou Faux ? $S = \{n \in \mathbb{Z} \mid n \equiv 26\ [35]\}$.

Exercice 13 (★★★☆) Le théorème chinois : cas général

Soient p et q deux entiers naturels non nuls. Les entiers relatifs a et b étant donnés, nous considérons le système de congruences

$$\begin{cases} x \equiv a\ [p] \\ x \equiv b\ [q] \end{cases}$$

1. Prouver que si p et q sont premiers entre eux, alors ce système admet au moins une solution x_0 appartenant à $\mathbb{Z}$.

2. Montrer que si x est une solution quelconque du système, alors

$$x \equiv x_0\ [pq].$$

3. En déduire l'ensemble des solutions du système proposé.

Exercice 14 (★★★★) Critère d'Eisenstein

Soient p et q deux entiers relatifs premiers entre eux.

1. Justifier que, quel que soit $n \in \mathbb{N}^*$,p est premier avec q^n et q est premier avec p^n.

Nous considérons un polynôme P dont le degré est l'entier $n \geqslant 1$, à coefficients entiers relatifs qui est défini, quel que soit le réel x, par

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \text{ avec } a_n \in \mathbb{Z}^* \text{ et } a_0 \in \mathbb{Z}^*.$$

1. Montrer que si la fraction irréductible $\frac{p}{q}$, avec $p \in \mathbb{Z}^*$ et $q \in \mathbb{Z}^*$ est une racine du polynôme P, alors

$$p \text{ divise } a_0 \text{ et } q \text{ divise } a_n.$$

2. *Application 1.* L'équation

$$5x^3 + 3x^2 - 4x - 14 = 0$$

admet-elle des solutions rationnelles ?

3. *Application 2.* On admet que le réel $\cos\frac{\pi}{9}$ est une solution de l'équation

$$4x^3 - 3x = \frac{1}{2}.$$

Cette solution est-elle rationnelle ?

Exercice 15 (★★★☆) Chiffrement de Hill : un exemple

Les 26 lettres de l'alphabet sont numérotées de 0 à 25 selon 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

Le chiffrement de Hill consiste à associer à un couple de deux entiers (x_1,x_2) qui sont compris entre 0 et 25, un couple (y_1,y_2) tel que par exemple

$$\begin{cases} y_1 \equiv 5x_1 + 13x_2\ [26] \\ y_2 \equiv 2x_1 + 7x_2\ [26] \end{cases}$$

La clé de chiffrement est constituée dans notre exemple des quatre entiers $a = 5$,$b = 13$,$c = 2$,$d = 7$, qui sont compris entre 0 et 25.

Pour coder un mot, on le partage en blocs de deux lettres. Si le nombre de lettres est impair, on peut supprimer la dernière lettre ou compléter le dernier bloc par une lettre choisie au hasard.

1. Coder le mot CODE.

2. Décodage. Justifier que

$$\begin{cases} 7y_1 - 13y_2 \equiv 9x_1 \ [26] \\ -2y_1 + 5y_2 \equiv 9x_2 \ [26] \end{cases}$$

Prouver qu'il existe un entier u compris entre 0 et 25 satisfaisant à

$$9u \equiv 1 \ [26].$$

En déduire

$$\begin{cases} x_1 \equiv 21y_1 + 13y_2 \ [26] \\ x_2 \equiv 20y_1 + 15y_2 \ [26] \end{cases}$$

Décoder le mot NCTVFP.

Exercice 16 (★★★☆) Inverse modulo n

Soient $a \in \mathbb{Z}^*$ et $n \in \mathbb{N}^*$ premiers entre eux.

1. Prouver qu'il existe un unique entier $u \in [\![0,n-1]\!]$ tel que

$$au \equiv 1 \ [n].$$

2. En déduire que si $y \equiv ax + b \ [n]$, avec $b \in \mathbb{Z}$, alors

$$x \equiv u(y - b) \ [n].$$

Exercice 17 (★★★☆) Chiffrement de Hill : Cas général

Le contexte est celui de l'exercice 15.

La clé de chiffrement est constituée de quatre entiers a,b,c,d, qui sont compris entre 0 et 25.

Nous associons à un couple de deux entiers (x_1,x_2) qui sont compris entre 0 et 25, un couple (y_1,y_2) tel que

$$\begin{cases} y_1 \equiv ax_1 + bx_2 \ [26] \\ y_2 \equiv cx_1 + dx_2 \ [26] \end{cases} \quad (1)$$

1. Justifier que le système (1) implique

$$\begin{cases} (ad - bc)x_1 \equiv dy_1 - by_2 \ [26] \\ (ad - bc)x_2 \equiv -cy_1 + ay_2 \ [26] \end{cases} \quad (2)$$

2. On pose $\delta = ad - bc$. Montrer que si $ad - bc \neq 0$ et 26 sont premiers entre eux, alors le système (2) a un ensemble non vide de solutions.

En utilisant la question 1. de l'exercice précédent, justifier qu'il existe un entier δ' compris entre 0 et 25 tel que

$$\delta \times \delta' \equiv 1 \ [26]$$

En déduire que (2) implique

$$\begin{cases} x_1 \equiv \delta' (dy_1 - by_2) \ [26] \\ x_2 \equiv \delta' (-cy_1 + ay_2) \ [26] \end{cases}$$

Réciproquement, justifier que le couple (x_1,x_2) satisfait au système (1).

3. En s'inspirant de l'algorithme donné au paragraphe 12.2.2 du cours, proposer un script Python qui permet de coder ou de décoder un bloc de deux lettres.

Exercice 18 (★★★☆) Coefficients de Bezout : algorithme

Soient a et b deux entiers naturels non nuls tels que b ne divise pas a. Nous savons que l'algorithme d'Euclide, appliqué aux entiers a et b, restitue une suite finie de restes (r_k), avec $0 \leqslant k \leqslant n+1$ et $n \in \mathbb{N}^*$ telle que

$$\text{pgcd}(a,b) = r_n \text{ et } r_{n+1} = 0$$

Nous souhaitons, quel que soit l'entier k compris entre 0 et n, construire deux suites (u_k) et (v_k) d'entiers relatifs réalisant l'égalité

$$au_k + bv_k = r_k.$$

1. En posant $u_0 = 1$ et $v_0 = 0$, puis $u_1 = 0$ et $v_1 = 1$, vérifier que

$$a = r_0 \text{ et } b = r_1.$$

2. La division euclidienne de a par b restitue un quotient q_2 et un reste r_2. Justifier que

$$u_2 = 1 \text{ et } v_2 = -q_2.$$

De la même façon, prouver que

$$r_3 = au_3 + bv_3, \text{ avec } u_3 = u_1 - u_2q_3 \text{ et } v_3 = v_1 - v_2q_3.$$

3. Établir, quel que soit l'entier $k \in [\![1,n]\!]$, qu'il existe deux entiers relatifs u_k et v_k tels que

$$au_k + bv_k = r_k, \text{ avec } u_{k+1} = u_{k-1} - u_kq_{k+1} \text{ et } v_{k+1} = v_{k-1} - v_kq_{k+1}$$

En déduire que

$$au_n + bv_n = \text{pgcd}(a,b).$$

4. Les entiers a et b étant donnés, proposer un script en Python qui restitue le pgcd(a,b), ainsi qu'un couple (u,v) qui est une solution particulière de l'équation

$$au + bv = \text{pgcd}(a,b)$$
