∽ EXERCICES 6 BIS ∽
BEZOUT

Exercice 1 : On cherche les solutions entières de l'équation :

$$(\mathrm{E}) : 7x + 13y = 1$$

1. Déterminer une solution $(x_0 ; y_0)$ de (E).
2. Montrer qu'une solution $(x ; y)$ de (E) vérifie l'équation :

$$7(x - x_0) = 13(y_0 - y)$$

3. Résoudre cette équation.

Exercice 2 : Léo prend le métro pour aller au travail. A la station Bézout, il doit changer de rame, la correspondance est sur le même quai. Il sait que son premier métro (Ligna A - durée du trajet 8 minutes) passe toutes les 7 minutes et le second (ligne B) toutes les 11 minutes. Ce matin il a pris son premier métro à 6 h 52, il est arrivé à $7h$ à la station Bézout et il a du attendre 6 minutes la rame de la ligne B.
Léo voudrait savoir à qu'elle heure partir entre $6h$ et $9h$ pour ne pas attendre la rame de la ligne B à la station Bézout.
On note x le nombre de rames de la ligne A et y le nombre de rames de la ligne B passées à la station Bézout **après** 7 h.

1. Montrer que, pour que l'attente soit nulle à la station Bézout, x et y doivent vérifier l'équation

$$(\mathrm{E}_1) : 7x - 11y = -12$$

2. Déterminer une solution particulière de (E_1).
3. Déterminer l'ensemble des solutions de (E_1).
4. Déterminer à quelles heures entre 6 h et 9 h, Léo peut prendre son premier métro pour ne pas attendre à la station Bézout.

Exercice 3 : **Métropole septembre 2017**

Partie A

Dans l'espace rapporté à un repère orthonormé $\left(\mathrm{O}; \vec{\imath}, \vec{\jmath}, \vec{k}\right)$, on considère les points A(1 ; 5 ; −2), B(7 ; −1 ; 3) et C(−2 ; 7 ; −2) et on note P le plan (ABC).

On cherche une équation cartésienne du plan 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 : $\mathrm{X} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ et $\mathrm{Y} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

1. Montrer que X vérifie la relation : MX = 73Y, où M est la matrice $\mathrm{M} = \begin{pmatrix} 1 & 5 & -2 \\ 7 & -1 & 3 \\ -2 & 7 & -2 \end{pmatrix}$.

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 : $X = NY$.

4. En déduire que le plan 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 P ayant pour équation cartésienne : $10x + 15y + 6z = 73$.

1. Soit $M(x\,;\,y\,;\,z)$ un point appartenant au plan 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 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 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 P si et seulement si $p + q + r = 1$.
   (d) En déduire qu'il existe exactement trois points du plan P dont les coordonnées sont des entiers naturels. Déterminer les coordonnées de ces points.

Exercice 4 : **Inspiré de Centres étrangers 2018**

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978.

Les questions 1 et 2 sont des questions préparatoires, la question 3 aborde le cryptage, la question 4 le décryptage.

1. **Calcul du reste dans la division euclidienne par** 55 **de certaines puissances de l'entier** 8 **:** Compléter sans calculatrice le tableau suivant :

Puissance de 8	8^2	8^4	8^6	8^7	8^{21}	8^{23}
Reste de la division euclidienne par 55 de la puissance de 8						

2. Dans cette question, on considère l'équation (E) $23x-40y=1$, dont les solutions sont des couples $(x\ ;\ y)$ d'entiers relatifs.
   (a) Justifier le fait que l'équation (E) admet au moins un couple solution.
   (b) Donner un couple, solution particulière de l'équation (E).
   (c) Déterminer tous les couples d'entiers relatifs solutions de l'équation (E).
   (d) En déduire qu'il existe un unique entier d vérifiant les conditions $0 \leqslant d < 40$ et $23d \equiv 1 \mod 40$.
3. **Cryptage dans le système RSA**
   — Une personne A choisit deux nombres premiers p et q,
   — Elle calcule les produits $\mathrm{N}=pq$ et $n=(p-1)(q-1)$. et choisit un entier naturel c premier avec n.
   — La personne A publie le couple $(\mathrm{N}\ ;\ c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté.
   — Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $\mathrm{N}-1$.
   Pour crypter un entier a de cette suite, on procède ainsi : on calcule le reste b dans la division euclidienne par N du nombre a^c, et le nombre crypté est l'entier b.

   Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres.
   On va l'envisager ici avec des nombres plus simples : $p=5$ et $q=11$.
   La personne A choisit également $c=23$.
   (a) Calculer les nombres N et n, puis justifier que la valeur de c vérifie la condition voulue.
   (b) Un émetteur souhaite envoyer à la personne A le nombre $a=8$.
   Déterminer la valeur du nombre crypté b.
4. **Décryptage dans le système RSA**
   — La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leqslant d < n$ et $cd \equiv 1 \mod n$.

— Elle garde secret ce nombre d qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique.

— Pour décrypter un nombre crypté b, la personne A calcule le reste a dans la division euclidienne par N du nombre b^d, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre a.

On admet l'existence et l'unicité de l'entier d, et le fait que le décryptage fonctionne.

Les nombres choisis par A sont encore $p = 5$, $q = 11$ et $c = 23$.

(a) Quelle est la valeur de d ?

(b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.

Exercice 5 : Centres étrangers - Pondichéry 2019

Le but de cet exercice est d'envisager plusieurs décompositions arithmétiques du nombre 40.

Partie A :

Les questions 1., 2. *et* 3. *sont indépendantes*

1. Sans justifier, donner deux nombres premiers x, et y tels que $40 = x + y$.
2. On considère l'équation $20x + 19y = 40$, où x et y désignent deux, entiers relatifs.
   Résoudre cette équation.
3. Le nombre 40 est une somme de deux carrés puisque : $40 = 2^2 + 6^2$. On veut savoir si 40, est aussi différence de deux carrés, autrement dit s'intéresser à l'équation $x^2 - y^2 = 40$, où x et y désignent deux entiers naturels.
   (a) Donner la décomposition de 40 en produit de facteurs premiers.
   (b) Montrer que, si x et y désignent des entiers naturels, les nombres $x - y$ et $x + y$ ont la même parité.
   (c) Déterminer toutes les solutions de l'équation $x^2 - y^2 = 40$ où x et y désignent deux entiers naturels.

Partie B : « sommes » de cubes

Les questions 1. *et* 2. *sont indépendantes.*

Certains nombres entiers peuvent se décomposer en somme ou différence de cubes d'entiers naturels.
Par exemple :

$$
\begin{aligned}
13 &= 4^3 + 7^3 + 7^3 - 9^3 - 2^3 \\
13 &= -1^3 - 1^3 - 1^3 + 2^3 + 2^3 \\
13 &= 1^3 + 7^3 + 10^3 - 11^3
\end{aligned}
$$

Dans tout ce qui suit, on écrira pour simplifier « sommes » de cubes à la place de « sommes ou différence de cubes d'entiers naturels ».

Les deux premiers exemples montrent que 13 peut se décomposer en « somme » de 5 cubes. Le troisième exemple montre que 13 peut se décomposer en « somme » de 4 cubes.

1. (a) En utilisant l'égalité $13 = 1^3 + 7^3 + 10^3 - 11^3$, donner une décomposition de 40 en « somme » de 5 cubes.

   (b) On admet que pour tout entier naturel n on a :

   $$6n = (n+1)^3 + (n-1)^3 - n^3 - n^3$$

   En déduire une décomposition de 48 en « somme » de 4 cubes, puis une décomposition de 40 en « somme » de 5 cubes, différente de celle donnée en **1. a.**)

2. Le nombre 40 est une « somme » de 4 cubes : $40 = 4^3 - 2^3 - 2^3 - 2^3$.

   On veut savoir si 40 peut être décomposé en « somme » de 3 cubes.

   (a) Recopier et compléter sans justifier :

Reste de la division euclidienne de n par 9	0	1	2	3	4	5	6	7	8
Reste de la division euclidienne de n^3 par 9					1				

   (b) On déduit du tableau précédent que, pour tout entier naturel n, l'entier naturel n^3 est congru modulo 9 soit à 0, soit à 1, soit à -1.

   Prouver que 40 ne peut pas être décomposé en « somme » de 3 cubes.