Les exercices I à IV de ce travail de synthèse sur l'arithmétique sont à rendre pour le Mardi 10 Janvier. La suite des exercices, facultative, s'adresse aux élèves souhaitant réfléchir davantage est à rendre au plus tard le 17 Janvier. Vous pouvez vous grouper par binôme.

Exercice I

Dans cet exercice, on appelle numéro du jour de naissance le rang de ce jour dans le mois et numéro du mois de naissance, le rang du mois dans l'année.
Par exemple, pour une personne née le 14 mai, le numéro du jour de naissance est 14 et le numéro du mois de naissance est 5.

Partie A

Lors d'une représentation, un magicien demande aux spectateurs d'effectuer le programme de calcul (A) suivant :
« Prenez le numéro de votre jour de naissance et multipliez-le par 12. Prenez le numéro de votre mois de naissance et multipliez-le par 37. Ajoutez les deux nombres obtenus. Je pourrai alors vous donner la date de votre anniversaire ».
Un spectateur annonce 308 et en quelques secondes, le magicien déclare : « Votre anniversaire tombe le 1er août ! ».

1. Vérifier que pour une personne née le 1er août, le programme de calcul (A) donne effectivement le nombre 308.

2. **a.** Pour un spectateur donné, on note j le numéro de son jour de naissance, m celui de son mois de naissance et z le résultat obtenu en appliquant le programme de calcul (A).
   Exprimer z en fonction de j et de m et démontrer que z et m sont congrus modulo 12.

   b. Retrouver alors la date de l'anniversaire d'un spectateur ayant obtenu le nombre 474 en appliquant le programme de calcul (A).

Partie B

Lors d'une autre représentation, le magicien décide de changer son programme de calcul. Pour un spectateur dont le numéro du jour de naissance est j et le numéro du mois de naissance est m, le magicien demande de calculer le nombre z défini par $z = 12j + 31m$.
Dans les questions suivantes, on étudie différentes méthodes permettant de retrouver la date d'anniversaire du spectateur.

1. Première méthode :
   On considère l'algorithme suivant :

```
Variables :     j et m sont des entiers naturels
Traitement :    Pour m allant de 1 à 12 faire :
                    Pour j allant de 1 à 31 faire :
                        z prend la valeur 12j + 31m
                        Afficher z
                    Fin Pour
                Fin Pour
```

   Modifier cet algorithme afin qu'il affiche toutes les valeurs de j et de m telles que $12j + 31m = 503$.

2. Deuxième méthode :
   a. Démontrer que $7m$ et z ont le même reste dans la division euclidienne par 12.
   b. Pour m variant de 1 à 12, donner le reste de la division euclidienne de $7m$ par 12.
   c. En déduire la date de l'anniversaire d'un spectateur ayant obtenu le nombre 503 avec le programme de calcul (B).

3. Troisième méthode :
   a. Démontrer que le couple $(-2\ ;\ 17)$ est solution de l'équation $12x + 31y = 503$.
   b. En déduire que si un couple d'entiers relatifs $(x\ ;\ y)$ est solution de l'équation $12x + 31y = 503$, alors $12(x+2) = 31(17-y)$.
   c. Déterminer l'ensemble de tous les couples d'entiers relatifs $(x\ ;\ y)$, solutions de l'équation $12x + 31y = 503$.
   d. Démontrer qu'il existe un unique couple d'entiers relatifs $(x\ ;\ y)$ tel que $1 \leqslant y \leqslant 12$.
   En déduire la date d'anniversaire d'un spectateur ayant obtenu le nombre 503 avec le programme de calcul (B).

Exercice II

Partie A : Généralités

On considère l'équation

$$(E) : \quad 23x - 26y = 1,$$

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 $0 \leqslant a \leqslant 25$ 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 :

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

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

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 :

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

b. À l'aide de la partie B, montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_2), vérifie les équations du système

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

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 III

Soit a et b deux entiers naturels non nuls ; on appelle « réseau » associé aux entiers a et b l'ensemble des points du plan, muni d'un repère orthonormal, dont les coordonnées $(x\ ;\ y)$ sont des entiers vérifiant les conditions : $0 \leqslant x \leqslant a$ et $0 \leqslant y \leqslant b$. On note $R_{a,\,b}$ ce réseau.
Le but de l'exercice est de relier certaines propriétés arithmétiques des entiers x et y à des propriétés géométriques des points correspondants du réseau.

A - Représentation graphique de quelques ensembles

Dans cette question, les réponses sont attendues sans explication, sous la forme d'un graphique qui sera dûment complété sur la feuille annexe n° 1 à rendre avec la copie.
Représenter graphiquement les points $M(x\ ;\ y)$ du réseau $R_{8,8}$ vérifiant :

1. $x \equiv 2 \pmod 3$ et $y \equiv 1 \pmod 3$, sur le graphique 1 de la feuille annexe
2. $x + y \equiv 1 \pmod 3$, sur le graphique 2 de la feuille annexe ;
3. $x \equiv y \pmod 3$, sur le graphique 3 de la feuille annexe.

B - Résolution d'une équation

On considère l'équation (E) : $7x - 4y = 1$, où les inconnues x et y sont des entiers relatifs.

1. Déterminer un couple d'entiers relatifs $(x_0\ ;\ y_0)$ solution de l'équation (E).
2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).
3. Démontrer que l'équation (E) admet une unique solution $(x\ ;\ y)$ pour laquelle le point $M(x\ ;\ y)$ correspondant appartient au réseau $R_{4,7}$.

C - Une propriété des points situés sur la diagonale du réseau.

Si a et b sont deux entiers naturels non nuls, on considère la diagonale $[OA]$ du réseau $R_{a,\,b}$, avec $O(0\ ;\ 0)$ et $A(a\ ;\ b)$.

1. Démontrer que les points du segment $[OA]$ sont caractérisés par les conditions :

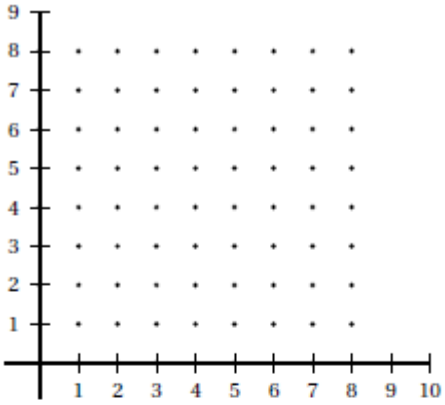
$$0 \leqslant x \leqslant a\ ;\ 0 \leqslant y \leqslant b\ ;\ ay = bx.$$

2. Démontrer que si a et b sont premiers entre eux, alors les points O et A sont les seuls points du segment $[OA]$ appartenant au réseau $R_{a,\,b}$.
3. Démontrer que si a et b ne sont pas premiers entre eux, alors le segment $[OA]$ contient au moins un autre point du réseau.
(On pourra considérer le pgcd d des nombres a et b et poser $a = da'$ et $b = db'$.)

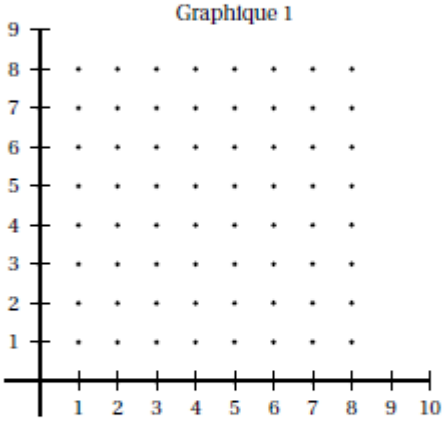
Combien le segment $[OA]$ contient-il de points du réseau $R_{a,b}$ dans ce cas-là ?

4. Déterminer, en fonction de a et b, le nombre de mailles du réseau $R_{a,b}$, que la diagonale $[OA]$ traverse. On appelle maille tout carré de côté 1 dont les sommets sont à coordonnées entières.

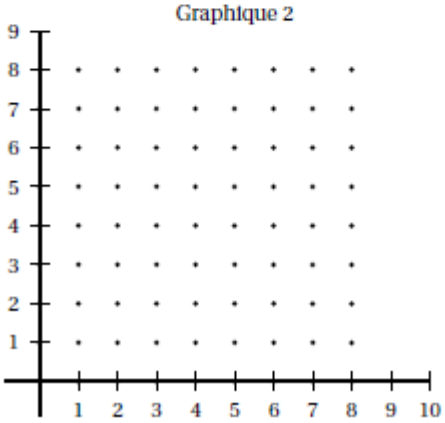
Annexe à l'exercice III



Graphique 1



Graphique 2



Graphique 3

Exercice IV

Ω désigne l'ensemble des entiers naturels compris entre 1 et 20 inclus.

Un élément a appartenant à Ω est dit inversible modulo 8 si et seulement si il existe un entier b tel que $ab \equiv 1\ (8)$. b est appelé ***un*** inverse de a modulo 8.

Déterminer une condition nécessaire et suffisante pour qu'un entier a appartenant à Ω soit inversible modulo 8, puis déterminer tous les éléments de Ω inversibles modulo 8. Donner pour chacun deux un inverse appartenant à Ω.

Exercice V

1) Démontrer que si a et b sont deux entiers premiers entre eux, alors a et b^2 sont premiers entre eux, puis que a^2 et b^2 sont premiers entre eux.

2) Soit n un entier naturel. On appelle nombre rationnel le quotient de deux nombres entiers.

a) Que dire de $\sqrt{n}$ lorsque n est un carré d'entier ?

b) Supposons que $\sqrt{n}$ soit un nombre rationnel : il existe donc des entiers p et q, tels que : $\sqrt{n} = \dfrac{p}{q}$.

i) Expliquer pourquoi on peut toujours se ramener au cas où p et q sont premiers entre eux. On suppose cette condition remplie pour la suite.

ii) Démontrer alors que $n = p^2$. On utilisera la question 1).

iii) En déduire une condition nécessaire et suffisante afin que $\sqrt{n}$ soit un nombre rationnel.

iv) En déduire que $\sqrt{n}$ est soit un entier naturel soit un nombre irrationnel.

Exercice VI

$a_0, a_1, \ldots\ldots a_n$ sont des nombres entiers relatifs avec $a_n \neq 0$ et n est un entier naturel supérieur ou égal à 1.

On considère la fonction polynôme F définie sur $\mathbb{R}$ par : $F(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots + a_1 x + a_0$.

Soit x un nombre rationnel écrit sous forme irréductible : $x = \dfrac{p}{q}$ avec p et q premiers entre eux.

1) Démontrer que si x est une racine de la fonction polynôme F, alors : p divise a_0 et q divise a_n.

2) On pose $F(x) = 3x^3 + 5x^2 - 21x + 10$.

a) Quelles sont *apriori* les valeurs de x rationnelles, solution de $F(x) = 0$. Les lister.

b) A l'aide d'une étude de fonction démontrer que l'équation $F(x) = 0$ admet exactement trois ***solutions réelles.***

c) Déterminer alors toutes les ***solutions rationnelles*** de $F(x) = 0$.