,

1. Résolution de l'équation *diophantienne* $ax + by = c$.

1.a. Définition et existence

Une équation diophantienne est une équation à **coefficients entiers** dont on cherche les **solutions entières**.

Soit a, b et c trois entiers relatifs, les équations diophantiennes du premier degré sont du type :

$$ax + by = c.$$

Remarque : `Diophante d'Alexandrie` est un mathématicien grec du IIIe siècle.

1.b. existence de solutions

Une équation diophantienne du premier degré, de la forme $ax + by = c$, où a, b et c sont des entiers relatifs, admet des solutions **si, et seulement si,** c est un multiple du PGCD(a, b).

Exemples :

- L'équation $17x - 33y = 1$ admet des solutions car $\text{PGCD }(17, 33) = 1$.
- L'équation $8x - 4y = 3$ n'admet pas de solution car $\text{PGCD }(8, 4) = 2$ et 3 n'est pas un multiple de 2.

1.c. Méthode de résolution

- On cherche une solution particulière à l'équation.
- On recherche ensuite l'ensemble des solutions en soustrayant termes à termes l'équation et l'égalité de la solution particulière.
- On applique le **théorème de Gauss**, puis l'on vérifie que les solutions trouvées vérifient bien l'équation.

1.d. Exemple d'application

Déterminer l'ensemble des solutions de l'équation $(E) : 17x - 33y = 1$.

- On cherche une solution particulière de (E). Ici, il existe une solution évequive : le couple (2 ;1), car

$$17 \times 2 - 33 \times 1 = 34 - 33 = 1$$

.

- On recherche ensuite la solution générale de (E). On a :

$$\begin{cases} 17x & -33y & = 1 \\ 17 \times 2 & - 33 \times 1 & = 1 \end{cases}$$

Par soustraction termes à termes des deux égalités, on obtient :

$$17(x - 2) - 33(y - 1) = 0 \Leftrightarrow 17(x - 2) = 33(y - 1) \qquad \text{(E')}$$

33 divise $17(x - 2)$. Or $\text{PGCD }(17, 33) = 1$, donc d'après le théorème de **Gauss**, 33 divise $(x - 2)$.

Il existe donc $k \in \mathbb{Z}$ tel que $x - 2 = 33k$

En remplaçant dans (E'), on trouve $y - 1 = 17k$.

Les solutions de (E) sont de la forme :

$$\begin{cases} x = 2 + 33k \\ y = 1 + 17k, k \in Z. \end{cases}$$

On vérifie pour conclure que ces solutions vérifient effectivement l'équation.

$$\forall k \in \mathbb{Z}, \quad 17(2+33k) - 33(1+17k) = 1$$

Exercice 1

Rechercher (indépendemment) les solutions (entières) des équations diophantiennes :]

1. $4235x + 42y = 15$
2. $4235x + 42y = 14$

Exercice 2

Determiner tous les entiers relatifs tels que

$$11x \equiv 4(50)$$

.

Exercice 3

Determiner toutes les solutions $x \in \mathbb{Z}$ du système

$$\begin{cases} x \equiv 1(7) \\ x \equiv 9(15) \end{cases}$$

Exercice 4

Un théatre pratique les tarifs suivants : 19 euros l'entrée pour les abonnées et 29 euros l'entrée pour les autres. A la fin d'une séance, le montant des recettes s'élève à 818 euros.

La caissière a perdu le talon des billets, mais elle sait qu'en général, il y a environ deux fois moins d'abonnés que de non abonnés.

Peut-elle retrouver la répartition des spectateurs lors de cette séance ?

Exercice 5 : Chiffrement affine

Partie A : Un premier exemple

Afin de coder un message, on assimile chaque lettre de l'alphabet à un nombre entier

$$A \to 0 \ldots Z \to 25$$

Un chiffrement élémentaire est le chiffrement affine. On se donne une fonction de codage affine f , par exemple :

$$f(x) = 11x + 8$$

À une lettre du message :

- on associe un entier x entre 0 et 25;
- on calcule $f(x) = (11x + 8)[26]$
- on traduit y par une lettre.

Exemple :

Si l'on veut coder la lettre G par la fonction $f(x) = 11x + 8$, on passe par les étapes suivantes :

$$G \to x = 6 \Rightarrow 11 \times 6 + 8 = 74 \to 74 \equiv 22(26) \to y = 22 \to W$$

La lettre G est donc codée par la lettre W.

1. Coder la lettre W.
2. Existence d'une fonction de décodage.
   - Pourquoi le théorème de Bézout permet-il d'affirmer qu'il existe un entier relatif u tel que : $11u + 26v = 1$?
   - Montrer alors que l'équation $11x \equiv 1(26)$, puis que l'équation $11x \equiv j(26)$, j étant un entier naturel,

   admettent une solution.

3. Déterminer la fonction de décodage.
    - Montrer que pour tous entiers relatifs x et j, on a :

    $11x \equiv j(26) \Leftrightarrow x \equiv 19j(26)$.
- En déduire que la fonction $f^{-1}(y) = 19y + 4(26)$.
- Décoder la lettre L.

Partie 2 : Casser une fonction de cryptage

On a reçu le message suivant : `FMEYSEPGCB`.

Par une étude statistique de la fréquence d'apparition des lettres sur un passage plus important, on déduit que le chiffrement est affine, que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N.

Soit la fonction affine f définie par : $f(x) = ax + b$ où a et b sont des entiers naturels compris entre 0 et 25.

1 - Démontrer que a et b vérifient le système suivant :

$$\begin{cases} 4a + b \equiv 4(26) \\ 9a + b \equiv 13(26) \end{cases}$$

1. Démontrer que $5a \equiv 9(26)$, puis que $a \equiv 7(26)$.
2. En déduire que $b \equiv 2(26)$ et que f est définie par

$$f(x) = 7x + 2(26)$$

.

1. Démontrer que, pour tous relatifs x et z, on a :

$$7x \equiv z(26) \Leftrightarrow x \equiv 15z(26)$$

   .
2. En déduire que la fonction de décodage f^{-1} est définie par

$$f^{-1}(y) = 15y + 22(26)$$

   .
3. Décoder le message.

```python
def f(a,b,x):
    return (a*x+b)%26

def affine(a,b,chaine):
    chaine=chaine.upper()
    retour=[]
    for lettre in chaine:
        x=ord(lettre)-65
        y=f(a,b,x)
        retour.append(chr(y+65))
    return retour

print(affine(15,22,"FMEYSEPGCB"))
```

```
['T', 'U', 'E', 'S', 'G', 'E', 'N', 'I', 'A', 'L']
```