EXERCICE 1

On se place dans l'anneau $\mathbb{Z}/23\mathbb{Z}$. On note U le groupe multiplicatif constitué de ses éléments inversibles.

1. Pourquoi $\mathbb{Z}/23\mathbb{Z}$ est-il un corps ? Combien U possède-t-il d'éléments ? Donner l'inverse de $\dot{5}$.

2. **a.** Quelles sont les valeurs possibles de l'ordre d'un élément x de U ?
b. Déterminer avec un minimum de calculs l'ordre de $\dot{5}$ dans U (*indication :* $\dot{5}^2 = \dot{2}$).
c. Prouver que U est un groupe monogène.
d. Rappeler le petit théorème de Fermat.
En déduire que $\dot{5}$ n'est pas un carré dans $\mathbb{Z}/23\mathbb{Z}$.
e. Prouver que l'équation $x^2 - 6x + 4 = 0$ ne possède pas de racine dans $\mathbb{Z}/23\mathbb{Z}$.

3. **a.** Donner l'ordre de $\dot{10}$ dans U.
b. En déduire l'existence d'un multiple de 23 qui, en base 10, ne s'écrit qu'avec des 1, et expliciter un tel nombre.

EXERCICE 2

Cet exercice étudie le problème (très concret pour une fois !) dit « des timbres-poste ». Son énoncé est des plus simples : on se donne deux types de timbres, des timbres à a centimes et d'autres à b centimes (a et b entiers premiers entre eux supérieurs ou égaux à 2). La question est de déterminer le plus grand entier $N(a,b)$ tel qu'il n'est pas possible d'affranchir une lettre à $N(a,b)$ centimes avec ces deux types de timbres.

On dira d'un entier positif n qu'il est « affranchissable » s'il est possible d'affranchir une lettre à n centimes avec nos timbres à a et b centimes, autrement dit si $\exists\, x,y \in \mathbb{N} \ / \ xa + yb = n$.

On cherche donc dans cet exercice un entier $N(a,b)$ tel que $N(a,b)$ ne soit pas affranchissable, mais tel que tout entier $n > N(a,b)$ soit affranchissable.

1. On prend ici $a = 3$ et $b = 7$.
a. Quelles sont les valeurs de $n \in [\![1,15]\!]$ qui sont affranchissables ?
b. Prouver, grâce à ce qui précède, que tout entier $n \geq 12$ est affranchissable.
c. Déterminer $N(3,7)$.

a et b désignent désormais deux entiers plus grands que 2, premiers entre eux, avec $a < b$.

2. **a.** Prouver que si n est un entier affranchissable, alors $n + a$ l'est aussi.
b. En déduire que si a entiers consécutifs sont affranchissables, alors tous les entiers suivants le sont.

3. Soit $p \in \mathbb{Z}$.
a. Prouver l'existence d'un couple d'entiers (u_0, v_0) tel que $u_0 a + v_0 b = p$.
b. Déterminer, en fonction de u_0 et de v_0 *tous* les couples d'entiers (u,v) tels que $ua + vb = p$.

c. On se donne deux réels α et β vérifiant $\alpha < \beta$. Quelle condition simple suffit-il d'imposer à α et β pour être certains de l'existence d'un entier compris entre α et β ?

d. En écrivant les conditions pour que les entiers u et v de la question **3.b.** soient positifs, prouver que si $p \geq ab$, alors p est affranchissable.

4. On pose $c = (a-1)(b-1)-1 = ab-a-b$

a. Donner une solution particulière *très simple* (elle doit se trouver à vue) de l'équation $ua+vb=c$.

b. En déduire toutes les solutions (u,v) de cette même équation.

c. Prouver que c n'est pas affranchissable.

5. **a.** Prouver que les entiers $ab+1$, $ab+2$,..., $ab+a-1$ sont tous affranchissables, ainsi que $ab+a$.

b. Prouver que tout affranchissement d'une lettre à n centimes avec $n = ab+1$, $ab+2$,..., $ab+a-1$ nécessite à la fois un timbre à a centimes **et** un timbre à b centimes.

c. En déduire que les entiers $ab+1-a-b$, $ab+2-a-b$,..., $ab-b$ sont affranchissables.

6. Déterminer $N(a,b)$.

EXERCICE 3

L'objet de cet exercice est l'étude de la complexité du calcul du pgcd de deux entiers naturels a et b par l'algorithme d'Euclide. On étudiera pour ce faire quelques propriétés de la suite de Fibonacci définie par :

$$F_0 = 0 \quad ; \quad F_1 = 1 \quad ; \quad \forall n \geq 0, \quad F_{n+2} = F_{n+1} + F_n .$$

1. **a.** Calculer F_n pour $n \leq 10$.

b. Prouver que la suite (F_n) devient strictement croissante à partir du rang 2, que c'est une suite d'entiers, et qu'elle tend vers $+\infty$.

c. Postuler et prouver une relation entre F_{n+1}^2 et le produit $F_n F_{n+2}$.

d. Donner une expression de F_n en fonction de n.

e. En déduire l'encadrement suivant, ainsi qu'un équivalent de F_n quand n tend vers l'infini :

$$\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - 1\right) \leq F_n \leq \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n + 1\right).$$

2. Prouver que pour tout entier $n \geq 1$, les nombres de Fibonacci F_n et F_{n+1} sont premiers entre eux.

On rappelle que l'algorithme d'Euclide de calcul du pgcd de deux entiers a et b $(a > b)$ consiste à effectuer les divisions euclidiennes successives suivantes, jusqu'à l'obtention d'un premier reste nul, et dans lesquelles $a_0 = a$ et $a_1 = b$:

$$\begin{aligned}
a_0 &= q_1 a_1 + a_2 \quad \text{avec} \quad 0 < a_2 < a_1 \\
a_1 &= q_2 a_2 + a_3 \quad \text{avec} \quad 0 < a_3 < a_2 \\
&\vdots \\
a_{n-1} &= q_n a_n + a_{n+1} \quad \text{avec} \quad 0 < a_{n+1} < a_n \\
a_n &= q_{n+1} a_{n+1} + a_{n+2} \quad \text{avec} \quad a_{n+2} = 0 .
\end{aligned}$$

On sait que le pgcd de a et b est égal au dernier reste non nul a_{n+1}. On dit alors que l'algorithme d'Euclide s'effectue en $n+1$ divisions. Les notations précédentes seront gardées dans la suite de cet exercice.

3. **a.** Prouver que pour tout entier $k \geq 2$, le nombre de Fibonacci F_k est le reste de la division de F_{k+2} par F_{k+1}.

b. En déduire que l'algorithme d'Euclide pour F_{n+2} et F_{n+1} s'effectue en $n+1$ divisions.

4. **a.** Prouver les inégalités $q_k \geq 1$ pour $1 \leq k \leq n+1$ et, par récurrence, $a_k \geq F_{n+2-k}$ pour $0 \leq k \leq n+2$.

b. En déduire, si l'algorithme d'Euclide s'effectue en $n+1$ divisions, que $a \geq F_{n+2}$, $b \geq F_{n+1}$ et :

$$\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - 1\right) \leq b\,.$$

c. En supposant que l'écriture décimale de b compte p chiffres (autrement dit que $10^{p-1} \leq b < 10^p$), prouver alors que le nombre $n+1$ de divisions de l'algorithme d'Euclide est majoré par $5p+2$ (Théorème de Lamé).