Une grande importance sera attachée a la rigueur du raisonnement, à la clarté et au soin de la présentation. L'usage des calculatrices n'est pas autorisé. Il est rappelé que tout résultat énoncé dans le texte peut être utilisé pour traiter la suite, même s'il n'a pu être démontré.

Exercice

1. Déterminer un couple $(u_0,\ v_0) \in \mathbb{Z}^2$, tel que

$$28u_0 + 15v_0 = 1$$

2. On considère l'équation

$$(E) : 28x + 15y = 5$$

   (a) Déterminer une solution particulière $(x_0,\ y_0) \in \mathbb{Z}^2$ de l'équation (E).

   (b) En déduire les solutions de l'équation (E) dans $\mathbb{Z}^2$.

Problème

On désigne par $\mathbb{Z}$ l'ensemble des entiers relatifs, $\mathbb{Q}$ l'ensemble des nombres rationnels, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ et $\mathbb{P}$ l'ensemble des entiers premiers.

— On rappelle que $(\mathbb{Q}, +, .)$ est un corps commutatif.

— Si $x \in \mathbb{Q}^*$, on note x^{-1} le symétrique de x par rapport à la multiplication. x^{-1} est appelé aussi l'inverse de x.

— $\forall a,\ b \in \mathbb{Z}$, on note $a \wedge b$: le plus grand commun diviseur de a et b (pgcd(a, b)).

— On rappelle le Théorème de Bézout : Soient $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$. Pour que $x_1, ..., x_n$ soient premiers entre eux, il faut et il suffit qu'il existe $(u_1, ..., u_n) \in (\mathbb{Z})^n$ tel que $\sum_{i=1}^{n} x_i u_i = 1$

A) Préliminaire

Soit p un entier premier.

1. Soit $a \in \mathbb{Z}^*$. Montrer qu'on a :

$$p \quad \text{divise} \quad a \quad \text{ou} \quad p \wedge a \quad = \quad 1$$

   (a) Soient $a, b \in \mathbb{Z}^*$. Montrer que

$$(p \wedge a \quad = \quad 1 \quad \text{et} \quad p \wedge b \quad = \quad 1) \Longleftrightarrow \quad p \wedge a.b = 1$$

(b) En déduire que si $a_1, ..., a_n \in \mathbb{Z}^*$, alors on a :

$$\forall i \in \{1, ..., n\}, \quad p \wedge a_i \quad = 1 \iff p \wedge \prod_{i=1}^{n} a_i = 1$$

B) Soit p un entier premier. On pose :

$$A_p = \left\{ \frac{a}{b} \text{ avec } (a,b) \in \mathbb{Z} \times \mathbb{Z}^* \text{ tels que si } a \neq 0, \text{ on } a : a \wedge b = 1 \text{ et } p \text{ ne divise pas } b \right\}$$

1. Soit $(a,b) \in (\mathbb{Z}^*)^2$ tel que $a \wedge b = 1$. Montrer que $\frac{a}{b} \in A_p \iff p \wedge b = 1$
2. Montrer que A_p est un sous anneau de $\mathbb{Q}$, contenant $\mathbb{Z}$
3. (a) Déterminer $\mathbb{U}(A_p)$: l'ensemble des éléments inversibles de A_p
   (b) Montrer que $(\mathbb{U}(A_p), .)$ est un groupe abélien
4. Montrer que $\forall x \in \mathbb{Q}^*$, on a :
$$x \in A_p \quad \text{ou} \quad x^{-1} \quad \in \quad A_p$$
5. Soit B un sous anneau de $\mathbb{Q}$, tel que $A_p \subset B$. Montrer que si $A_p \neq B$, alors B $= \mathbb{Q}$ (on pourra utiliser la question 4). En déduire les sous anneaux de $\mathbb{Q}$ contenant A_p
6. Soit $a \in \mathbb{Z}$ et posons n : le plus grand entier naturel tel que p^n divise a. Montrer que $a = p^n.a'$ avec $p \wedge a' = 1$
7. Pour tout $x \in \mathbb{Q}^*$, montrer qu'il existe un unique entier $n \in \mathbb{Z}$ tel que $x = p^n.u$ où u est un élément inversible de $A_p (u \in \mathbb{U}(A_p))$.
   On définit l'application v_p de $\mathbb{Q}$ dans $\mathbb{Z} \cup \{+\infty\}$, par : $\forall x \in \mathbb{Q}^*$, $v_p(x) = n$, où n est l'unique entier de la question précédente. On pose également $v_p(0) = +\infty$
8. On pose B=$\{0,\ 54,\ \frac{4}{27},\ \frac{8}{11},\ \frac{5}{6},\ \frac{18}{5},\ \frac{20}{3}\}$ et on suppose uniquement dans cette question que $p = 3$
   (a) Déterminer $v_3(x)$ pour chaque $x \in B$
   (b) Déterminer les ensembles $A_3 \cap B$ *et* $\mathbb{U}(A_3) \cap B$
9. Dans le reste du problème, p désigne un nombre premier
   (a) Déterminer les ensembles $(v_p)^{-1}\{0\}$ et $v_p(\mathbb{Q})$
   (b) v_p est-elle injective ? est-elle surjective ?
10. Montrer que pour tout $(x,\ y) \in \mathbb{Q} \times \mathbb{Q}$ on a :
    (a) $v_p(x.y) = v_p(x) + v_p(y)$
    (b) Pour tout $n \in \mathbb{Z}$, $v_p(x^n) = n.v_p(x)$
    (c) $v_p(x+y) \geq min[v_p(x),\ v_p(y)]$, avec égalité si $v_p(x) \neq v_p(y)$
11. Montrer que $A_p = \{x \in \mathbb{Q} \text{ tel que } v_p(x) \geq 0\}$
12. Montrer qu'on a $\mathbb{Z} = \bigcap_{p \in \mathbb{P}} A_p$