

Travaux dirigés sur l'arithmétique - corrigé -

Problème : le théorème des deux carrés

1. On pose $p = 1 + 4k$, avec k un entier naturel. Le triplet $(1, k, 1)$ appartient à S par exemple.
2. Il est clair que l'intersection $S_1 \cap S_2$ est vide. De plus, la réunion $S_1 \cup S_2$ est incluse dans S .

Ensuite, soit (a, b, c) dans S .

Si par l'absurde, on avait $a = b + c$, alors :

$$p = 4(b + c)b + c^2 = (2b + c)^2$$

contredisant le fait que l'entier p soit premier. On en déduit :

$$S = S_1 \sqcup S_2.$$

Enfin, les triplets $(1, k, 1)$ et $(k, 1, 1)$ sont dans S . Comme l'entier $p = 1 + 4k$ est un nombre premier, alors l'entier k est supérieur ou égal à 1.

▷ Si $k = 1$, alors $p = 5$ et on a :

$$(1, 1, 1) \in S_2 \text{ et } (1, 1, -1) \in S_1.$$

▷ Sinon, on ne peut avoir $k = 2$, donc $k \geq 3$ et dans ce cas :

$$(k, 1, 1) \in S_1 \text{ et } (1, k, 1) \in S_2.$$

Dans les deux cas, les ensembles S_1 et S_2 ne sont pas vides.

On a bien affaire à une partition de S en $\{S_1, S_2\}$.

3. On vérifie que l'application :

$$\varphi : \left\{ \begin{array}{ll} S_1 & \longrightarrow S_2 \\ (a, b, c) & \longmapsto (b, a, -c) \end{array} \right.$$

est bien définie et est une bijection.

En effet, pour tout $(a, b, c) \in S_1$, alors $a > b + c$ et $p = 4ab + c^2$. On en déduit :

$$a - c > b \text{ et } p = 4ba + (-c)^2.$$

L'élément $(b, a, -c)$ est bien dans S_2 .

Il est facile de voir que l'application :

$$\psi : \left\{ \begin{array}{ccc} S_2 & \longrightarrow & S_1 \\ (a, b, c) & \longmapsto & (b, a, -c) \end{array} \right.$$

est encore bien définie et que :

$$\varphi \circ \psi = \text{id}_{S_2}, \text{ puis } \psi \circ \varphi = \text{id}_{S_1}.$$

Les applications φ et ψ sont bijectives, réciproques l'une de l'autre.

4. On montre déjà que l'application f est bien définie de S_1 vers S_1 .

En effet, si $(a, b, c) \in S_1$, alors :

$$4(a - b - c)b + (-2b - c)^2 = 4ab + c^2 = p^2.$$

De plus, comme $a > b + c$, on peut écrire :

$$a - b - c - (b + (-2b - c)) = a.$$

L'entier naturel a ne peut pas être nul car sinon, on aurait $c^2 = p$, mais p est premier. Donc, $a > 0$.

Conclusion, $f(a, b, c) \in S_1$.

D'autre part, pour tout $(a, b, c) \in S_1$, on a :

$$\begin{aligned} f \circ f(a, b, c) &= f(a - b - c, b, -2b - c) \\ &= ((a - b - c) - b + 2b + c, b, -2b - (-2b - c)) \\ &= (a, b, c). \end{aligned}$$

La fonction f est bien une involution de S_1 .

5. Soit (a, b, c) un point fixe éventuel pour la fonction f . Alors, $f(a, b, c) = (a, b, c)$, donc :

$$\begin{cases} a - b - c = a \\ b = b \\ -2b - c = c \end{cases}$$

imposant $b = -c$. Par conséquent,

$$p = 4ab + b^2 = b(4a + b).$$

L'entier b est un diviseur positif de p , avec $4a + b > 1$, donc $b = 1$ et $(a, b, c) = (k, 1, -1)$, où k est l'entier tel que $p = 4k + 1$.

Réciproquement, le triplet $(k, 1, -1)$ est bien un point fixe de l'application f sur simple vérification.

La fonction f n'admet qu'un seul point fixe.

6. La relation $\mathcal{R}$ sur l'ensemble S_1 définie par :

$$\forall (x, y) \in S_1^2, x\mathcal{R}y \iff \{x, f(x)\} = \{y, f(y)\}$$

est clairement une relation d'équivalence.

De plus, il est facile de voir que pour tout $x \in S$, la classe d'équivalence de x est l'ensemble :

$$\dot{x} = \{x, f(x)\}.$$

Il y a donc un nombre fini de classes d'équivalence, ce nombre étant noté par exemple $m \in \mathbb{N}^*$ et chaque classe d'équivalence comporte deux éléments sauf une.

On note $C_1, \dots, C_{m-1}$ les classes à deux éléments et C_m celle à un seul élément.

Comme ces classes partitionnent l'ensemble S_1 , il est facile de voir que l'ensemble S_1 comporte exactement $2(m-1) + 1 = 2m - 1$ éléments. L'ensemble S_2 étant en bijection avec S_1 comporte lui aussi $2m - 1$ éléments.

Conclusion, l'ensemble $S = S_1 \sqcup S_2$ comporte $4m - 2$ éléments, entier bien congru à 2 modulo 4.

7. On introduit sur l'ensemble S_3 la relation $\mathcal{S}$ par :

$$\forall ((a, b, c), (a', b', c')) \in S_3^2, (a, b, c)\mathcal{S}(a', b', c') \iff$$

$$\{(a, b, c), (b, a, c), (a, b, -c), (b, a, -c)\} = \{(a', b', c'), (b', a', c'), (a', b', -c'), (b', a', -c')\}.$$

La relation $\mathcal{S}$ est clairement une relation d'équivalence et pour tout (a, b, c) dans S_3 , la classe de (a, b, c) est l'ensemble $\{(a, b, c), (b, a, c), (a, b, -c), (b, a, -c)\}$ comportant exactement quatre éléments puisque $a \neq b$ et $c \neq 0$, l'égalité $p = 4ab$ ne pouvant avoir lieu.

En notant r le nombre de classes d'équivalence modulo $\mathcal{S}$, alors l'ensemble S_3 comporte exactement $4r$ éléments.

8. L'inclusion $S_3 \subset S$ est évidente.

Il est impossible que les ensembles S_3 et S soient égaux, sinon en prenant les cardinaux, on aurait :

$$2 = 0, \text{ dans } \mathbb{Z}/4\mathbb{Z},$$

ce qui est faux. On en déduit qu'il existe $(a, b, c) \in S \setminus S_3$. Ainsi, $a = b$ et :

$$4a^2 + c^2 = (2a)^2 + c^2,$$

qui est la somme de deux carrés.