

Travaux dirigés sur l'arithmétique

Problème : le théorème des deux carrés

Soit p un nombre premier congru à 1 modulo 4. On considère l'ensemble :

$$S = \{(a, b, c) \in \mathbb{N}^2 \times \mathbb{Z} \mid 4ab + c^2 = p\}.$$

1. Montrer que l'ensemble S est non vide.
2. Montrer que les ensembles

$$S_1 = \{(a, b, c) \in S \mid a > b + c\}$$

et

$$S_2 = \{(a, b, c) \in S \mid a < b + c\}$$

partitionnent l'ensemble S .

3. Expliciter une bijection $\varphi : S_1 \longrightarrow S_2$.
4. Montrer que l'application $f : (a, b, c) \longmapsto (a - b - c, b, -2b - c)$ est une involution de S_1 .
5. Chercher les points fixes de cette involution.
6. En déduire que le cardinal de S est congru à 2 modulo 4.
7. Montrer que l'ensemble $S_3 = \{(a, b, c) \in S \mid a \neq b\}$ a un cardinal divisible par 4.
8. En déduire que p est une somme de deux carrés.