

Préparation à l'oral

Exercice n° 19 - A

Thème : Arithmétique

L'exercice

1. Démontrer qu'il existe une infinité de nombres premiers.
2. Démontrer qu'il existe une infinité de nombres premiers de la forme $4k+3$, avec $k \in \mathbb{N}$. On pourra raisonner par l'absurde en supposant qu'il n'existe qu'un nombre fini p_1, \dots, p_n de premiers de la forme $4k+3$ et considérer l'entier $N = 4p_1 \times \dots \times p_n - 1$.
3. On suppose dans cette question qu'il n'existe qu'un nombre fini de nombres premiers p_1, \dots, p_n de la forme $4k+1$, avec $k \in \mathbb{N}$. On considère $N = 4(p_1 \times \dots \times p_n)^2 + 1$. Soit p un nombre premier impair.
 - (a) (*) Soient $f, g : \mathbb{Z}/p\mathbb{Z}^* \rightarrow \mathbb{Z}/p\mathbb{Z}^*$ données par $f(x) = x^2$ et $g(x) = x^{\frac{p-1}{2}}$.
En notant $\text{Ker } g = \{x \in \mathbb{Z}/p\mathbb{Z}^* \mid g(x) = 1\}$, montrer que $\text{Im } f = \text{Ker } g$.
 - (b) En déduire que -1 est un carré modulo p si et seulement si p est de la forme $4k+1$ avec $k \in \mathbb{N}$.
 - (c) Montrer que si p divise N , alors -1 est un carré modulo p .
 - (d) Conclure.

Notion mise en jeu : Nombres premiers.

Il est attendu notamment que la candidate ou le candidat sache démontrer que tout entier possède un diviseur premier.