UNE FAMILLE D'ÉQUATIONS DIOPHANTIENNES

On souhaite établir le résultat suivant.

Théorème Soit p un nombre premier non congru à 1 ou -1 modulo 8. L'équation $4x^4 - py^2 = 1$ d'inconnue $(x, y) \in \mathbb{N}^2$ admet $(1, 1)$ pour seule solution si $p = 3$ et n'en possède pas sinon.

On pourrait montrer plus généralement avec des outils de niveau MPSI — mais on ne le fera pas — que le cas où p est congru à 1 ou -1 modulo 8 n'apporte qu'une solution supplémentaire : $p = 7$, $x = 2$ et $y = 3$.

On **ADMET** le résultat étudié en TD selon lequel pour tous $x, y \in \mathbb{N}$ premiers entre eux, si xy est un carré parfait, x et y en sont aussi.

1) Soient $x, y, z \in \mathbb{N}^*$ et p un nombre premier. On suppose que x et y sont premiers entre eux et que $xy = pz^2$. Montrer l'existence de deux entiers $a, b \in \mathbb{N}$ pour lesquels soit $x = pa^2$ et $y = b^2$, soit $x = a^2$ et $y = pb^2$.

On **ADMETTRA** dans la partie **2** le théorème suivant, démontré dans la partie **3**.

Théorème **(Loi complémentaire de Gauss)** Pour tout nombre premier p impair : $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \; [p]$.

1 RÉSOLUTION D'UNE ÉQUATION INTERMÉDIAIRE

2) Soient $x, y \in \mathbb{N}$. On suppose que $x^4 - 2y^2 = 1$.

a) Montrer que x est impair.

On peut ainsi noter n l'entier naturel pour lequel $x = 2n + 1$.

b) Factoriser y^2 en fonction de n. En déduire que $n(n+1)$ est un carré parfait.

c) Déterminer x et y.

2 DÉMONSTRATION DU THÉORÈME PRINCIPAL

Soient $x, y \in \mathbb{N}$ et p un nombre premier non congru à 1 ou -1 modulo 8. On suppose que $4x^4 - py^2 = 1$.

3) Montrer par l'absurde que $2x^2 \not\equiv 1 \; [p]$.

4) **a)** Montrer l'existence de deux entiers $a, b \in \mathbb{N}$ pour lesquels : $2x^2 + 1 = pa^2$ et $2x^2 - 1 = b^2$.

b) Montrer l'existence de trois entiers $c, d \in \mathbb{N}$ et $\varepsilon \in \{-1, 1\}$ pour lesquels : $2x + \varepsilon b = pc^2$ et $2x - \varepsilon b = d^2$.

c) Simplifier $\left(pc^2 + d^2\right)^2 - 2\left(pc^2 - d^2\right)^2$, puis montrer que : $8d^4 - \left(pc^2 - 3d^2\right)^2 = 8$.

d) En déduire que $pc^2 - 3d^2$ est divisible par 4, puis que : $p = 3$ et $x = y = 1$.

3 DÉMONSTRATION DE LA LOI COMPLÉMENTAIRE DE GAUSS

Cette dernière partie est facultative.

5) Soit p un nombre premier impair. On pose $r = \dfrac{p-1}{2}$.

a) Montrer que l'application $k \longmapsto p - k$ est bijective de $[\![1, r]\!] \cap (2\mathbb{Z} + 1)$ sur $[\![r+1, p-1]\!] \cap 2\mathbb{Z}$.

b) En déduire que : $\displaystyle\prod_{k=1}^{r} \left((-1)^k k\right) \equiv 2^r r! \; [p]$.

c) En déduire la loi complémentaire de Gauss.

6) Pour la beauté du geste, montrer que l'ensemble des nombres premiers congrus à -1 modulo 8 est infini.