DM 8, pour le vendredi 20/01/2023, non ramassé

PROBLÈME
Théorème de Fermat-Euler

L'objectif de ce problème est de montrer le théorème suivant :

« Soit p un nombre premier impair. Alors p est somme de deux carrés si et seulement si $p \equiv 1\ [4]$. »

Question préliminaire :

Soit $k \geq 1$ un entier impair. Combien y-a-t-il d'entiers relatifs dans l'intervalle $\left]-\frac{k}{2}, \frac{k}{2}\right[$? Expliquer alors *sans démonstration* pourquoi pour tout entier $n \in \mathbb{Z}$, il existe un unique entier $n_0 \in \mathbb{Z}$ tel que $n \equiv n_0\ [k]$ et $|n_0| < \frac{k}{2}$.

Partie I.

1) Quelles sont les possibilités pour $x^2\ [4]$ quand $x \in \mathbb{Z}$? En déduire que si p est premier impair somme de deux carrés, alors $p \equiv 1\ [4]$.

Dans toute la suite, on suppose que p est premier impair et vérifie $p \equiv 1\ [4]$.

2) Soit $a \in [\![1, p-1]\!]$.
   a) Justifier que $a \wedge p = 1$ et en déduire qu'il existe $u \in \mathbb{Z}$ tel que $au \equiv 1\ [p]$.
   b) Montrer qu'il existe un unique $u_0 \in [\![1, p-1]\!]$ tel que $au_0 \equiv 1\ [p]$.

On notera alors $a^{-1} = u_0$ et on dira que a^{-1} est l'inverse de a modulo p.
   c) Montrer que $a^2 \equiv 1\ [p] \Leftrightarrow a \equiv 1\ [p]$ ou $a \equiv -1\ [p]$.
   d) En déduire que les seuls éléments $a \in [\![1, p-1]\!]$ vérifiant $a = a^{-1}$ sont $a = 1$ ou $a = p-1$.
   e) En regroupant les éléments de $[\![1, p-1]\!]$ par paires, montrer que :

$$(p-1)! \equiv -1\ [p].$$

3) Montrer que $(p-1)! \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2\ [p]$.

Dans le produit $(p-1)!$, on pourra se ramener à un produit d'entiers compris entre $-\frac{p}{2}$ et $\frac{p}{2}$.

4) Déduire des questions précédentes qu'il existe $x_0 \in \mathbb{Z}$ tel que $x_0^2 + 1 \equiv 0\ [p]$ et $|x_0| < \frac{p}{2}$.

Partie II.

On suppose toujours dans cette partie que p est un nombre premier impair tel que $p \equiv 1$ [4].

On pose $E = \{q \in \mathbb{N}^* \ / \text{ il existe } a, b \in \mathbb{N} \text{ tels que } a^2 + b^2 = qp\}$.

5) Soit $x_0 \in \mathbb{Z}$ tel que $x_0^2 + 1 \equiv 0$ [p] et $|x_0| < \dfrac{p}{2}$. *Cet élément existe d'après la partie précédente.*

a) Soit $k \in \mathbb{Z}$ tel que $x_0^2 + 1 = kp$. Vérifier que $1 \leq k < p$.

b) En déduire que E contient un élément compris entre 1 et $p-1$, puis que E admet un minimum.

On note alors m le minimum de E (qui est donc compris entre 1 et $p-1$) et on fixe a, b dans $\mathbb{N}$ tels que $a^2 + b^2 = mp$.

6) On suppose par l'absurde que m est pair.

a) Montrer que a et b ont même parité.

b) Obtenir une absurdité en développant $\left(\dfrac{a+b}{2}\right)^2 + \left(\dfrac{a-b}{2}\right)^2$.

7) On va à présent montrer que $m = 1$. On suppose par l'absurde que $m \geq 3$.

a) Établir l'identité de Lagrange :

$$(\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = (\alpha\gamma + \beta\delta)^2 + (\alpha\delta - \beta\gamma)^2.$$

b) Soient $a_0, b_0 \in \mathbb{Z}$ tels que $|a_0| < \dfrac{m}{2}$, $|b_0| < \dfrac{m}{2}$, et $a_0 \equiv a$ [m], $b_0 \equiv b$ [m]. On pose $n = a_0^2 + b_0^2$. Montrer que $n \neq 0$.

c) Montrer qu'il existe $u \in \mathbb{Z}$ tel que $n = um$, puis que $1 \leq u < \dfrac{m}{2}$.

d) Montrer que up est une somme de deux carrés d'entiers.

On pourra partir du produit $(um) \times (mp)$ et utiliser l'identité de Lagrange.

e) Conclure.