DM 8, corrigé

PROBLÈME
Théorème de Fermat-Euler

Question préliminaire :

Soit $k \geq 1$ un entier impair. On teste rapidement pour $k = 1$, il n'y a que 0 dans $\left]-\frac{1}{2}, \frac{1}{2}\right[$, donc un seul entier. Si $k = 2$, il n'y a que $-1, 0, 1$ dans $\left]-\frac{3}{2}, \frac{3}{2}\right[$. On conjecture donc qu'il ne va y avoir que k entiers dans l'intervalle $\left]-\frac{k}{2}, \frac{k}{2}\right[$.

Pour le prouver, puisque k est impair, on remarque que les entiers dans l'intervalle $\left]-\frac{k}{2}, \frac{k}{2}\right[$ sont les entiers contenus dans $[\![-\frac{k}{2} + \frac{1}{2}, \frac{k}{2} - \frac{1}{2}]\!]$. Or, le nombre d'entiers dans $[\![a, b]\!]$ est $b - a + 1$. On en déduit que le nombre d'entiers dans $[\![-\frac{k}{2} + \frac{1}{2}, \frac{k}{2} - \frac{1}{2}]\!]$ est :

$$\frac{k}{2} - \frac{1}{2} - \left(-\frac{k}{2} + \frac{1}{2}\right) + 1 = k.$$

Puisqu'il y a k entiers consécutifs dans cet intervalle, on en déduit que pour tout n entier, il existe un unique n_0 dans cet intervalle tel que $n \equiv n_0\ [k]$. On a alors bien $|n_0| < \frac{k}{2}$.

Partie I.

1) Les possibilités pour x $[4]$ sont $0, 1, 2, 3$. Les possibilités pour x^2 $[4]$ sont donc $0, 1, 0, 1$. Supposons alors que p s'écrive comme une somme de deux carrés. Les possibilités pour p $[4]$ sont donc 0, 1 ou 2. Or, puisque p est impair, la seule possibilité est 1. Ceci entraine que $p \equiv 1\ [4]$.

2) On suppose désormais que $p \equiv 1\ [4]$.

a) Soit $a \in [\![1, p-1]\!]$. Puisque $a < p$ et que p est premier, il n'admet aucun facteur de p dans sa décomposition en facteurs premiers. On en déduit que $a \wedge p = 1$. D'après le théorème de Bezout, il existe donc $u, v \in \mathbb{Z}$ tels que $au + pv = 1$. Ceci entraine, en considérant cette égalité modulo p que $au \equiv 1\ [p]$.

b) Soit u_0 l'unique entier de $[\![0, p-1]\!]$ tel que $u_0 \equiv u\ [p]$. On a alors $au_0 \equiv 1\ [p]$. De plus, on a $u_0 \neq 0$ car sinon, on aurait $au_0 \equiv 0\ [p]$, ce qui est absurde. Ceci entraine que $u_0 \in [\![1, p-1]\!]$.

On a donc montré l'existence du u_0. Il reste à montrer l'unicité. Supposons qu'il existe $u_1 \in [\![1, p-1]\!]$ tel que $au_1 \equiv 1\ [p]$. On a alors $au_0 \equiv au_1\ [p]$, ce qui revient à $a(u_0 - u_1) \equiv 0\ [p]$. On en déduit que :

$$p | a(u_0 - u_1).$$

Or, $a \wedge p = 1$ donc d'après le théorème de Gauss, on a $p | (u_0 - u_1)$. On a donc $u_0 \equiv u_1\ [p]$. Or, puisque u_0 et u_1 sont dans $[\![1, p-1]\!]$, on en déduit que $u_0 = u_1$ d'où l'unicité.

c) On va procéder par double implication.

($\Leftarrow$) Si $a \equiv 1$ $[p]$ ou $a \equiv -1$ $[p]$, alors on a directement $a^2 \equiv 1$ $[p]$ (on a le droit de multiplier des modulos).

($\Rightarrow$) Réciproquement, supposons que $a^2 \equiv 1$ $[p]$. On a alors $a^2 - 1 \equiv 0$ $[p]$, c'est à dire $p|(a^2-1)$. On a donc $p|(a-1)(a+1)$. Or, p est premier. On en déduit que $p|(a-1)$ ou $p|(a+1)$, ce qui entraine $a - 1 \equiv 0$ $[p]$ ou $a + 1 \equiv 0$ $[p]$ et donc $a \equiv 1$ $[p]$ ou $a \equiv -1$ $[p]$.

d) Soit $a \in [\![1, p-1]\!]$ vérifiant $a = a^{-1}$. On a alors d'après la définition de a^{-1} que $a^2 \equiv 1$ $[p]$. D'après la question précédente, ceci entraine que $a \equiv 1$ $[p]$ ou $a \equiv -1$ $[p]$. Or, les seuls éléments de $[\![1, p-1]\!]$ qui vérifient ceci sont $a = 1$ et $a = p-1$. On a donc la propriété voulue.

e) On a $(p-1)! = 1 \times 2 \times 3 \times \ldots \times (p-2) \times (p-1)$. On effectue donc le produit de tous les éléments de $[\![1, p-1]\!]$. Or, si a est différent de 1 et de $p-1$, il admet un inverse a^{-1} qui est différent de a et qui est aussi dans $[\![1, p-1]\!]$. On peut donc regrouper dans le produit chaque terme différent de 1 et de $(p-1)$ avec son inverse. Ceci donne donc, puisque $aa^{-1} \equiv 1$ $[p]$ que toutes les paires que l'on regroupe sont toutes égales à 1 modulo p. On en déduit que :

$$\begin{aligned} (p-1)! &\equiv 1 \times (p-1) \ [p] \\ &\equiv -1 \ [p]. \end{aligned}$$

3) En suivant l'indication de l'énoncé, on va écrire :

$$(p-1)! = 1 \times 2 \times \ldots \times \frac{p-1}{2} \times \left(\frac{p-1}{2} + 1\right) \times \ldots \times (p-2) \times (p-1).$$

Or, de la même idée que dans la question préliminaire, on a $p - 1 \equiv -1$ $[p]$, $p - 2 \equiv -2$ $[p]$, ..., jusqu'à :

$$\begin{aligned} \frac{p-1}{2} + 1 &\equiv \frac{p-1}{2} + 1 - p \ [p] \\ &\equiv -\frac{p-1}{2} \ [p]. \end{aligned}$$

Ceci entraine que la seconde partie du produit est congrue modulo p à $(-1)^k \left(\frac{p-1}{2}\right)!$ où k est le nombre de termes dans le produit, c'est à dire $k = \frac{p-1}{2}$ (puisque l'on prend la moitié des termes et que l'on a $p-1$ termes dans le produit). Puisque $p \equiv 1$ $[4]$, ceci entraine que k est pair et on a donc la deuxième partie du produit qui est congrue modulo p à $\left(\frac{p-1}{2}\right)!$. On en déduit finalement que :

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

4) Posons $x = \left(\frac{p-1}{2}\right)!$. On a bien $x \in \mathbb{Z}$ (on a même $x \in \mathbb{N}$). D'après les deux questions précédentes, on a $(p-1)! \equiv x^2$ $[p]$ et $(p-1)! \equiv -1$ $[p]$. Ceci entraine que $x^2 \equiv -1$ $[p]$, soit $x^2 + 1 \equiv 0$ $[p]$.

Or, d'après la question préliminaire, puisque p est impair, il existe $x_0 \in \mathbb{Z}$ tel que $|x_0| < \frac{p}{2}$ tel que $x \equiv x_0$ $[p]$. On a donc bien $x_0^2 + 1 \equiv x^2 + 1$ $[p]$, d'où $x_0^2 + 1 \equiv 0$ $[p]$.

Partie II.

5)

a) Soit $k \in \mathbb{Z}$ tel que $x_0^2 + 1 = kp$. On a bien $1 \leq k$ puisque $0 < x_0^2 + 1$. De plus, on a $|x_0| < \frac{p}{2}$ donc par stricte croissance de $x \mapsto x^2$ sur $\mathbb{R}_+$, on a $x_0^2 < \frac{p^2}{4}$. On en déduit que $kp < 1 + \frac{p^2}{4}$. En divisant par $p > 0$, on obtient :

$$k < \frac{1}{p} + \frac{p}{4}.$$

Puisque p est premier impair, on a $p > 2$ et donc $\frac{1}{p} < 1 < \frac{p}{2}$. On a donc :

$$k < \frac{3p}{4} < p.$$

On a bien le résultat voulu.

b) Vérifions que $k \in E$. En prenant $a = |x_0|$ et $b = 1$, on a $a, b \in \mathbb{N}$ et $a^2 + b^2 = kp$. Puisque $k \in [\![1, p-1]\!]$, on a bien $k \in E$. On en déduit que E est non vide. E est non vide minoré et c'est une partie de $\mathbb{N}^*$, il admet donc un minimum. Puisque $k < p$, on en déduit que ce minimum est aussi strictement plus petit que p.

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

a) On a $a^2 + b^2$ pair puisque m est pair. Or, si a et b ne sont pas de même parité, on a par exemple a pair et b impair (l'autre cas se traite de la même façon). On a donc a^2 pair et b^2 impair, ce qui entraine $a^2 + b^2$ impair : absurde ! On en déduit que a et b sont de même parité.

b) Puisque a et b sont de même parité, on en déduit que $\frac{a+b}{2}$ et $\frac{a-b}{2}$ sont entiers. On a de plus :

$$\begin{aligned} \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 &= \frac{a^2+2ab+b^2}{4} + \frac{a^2-2ab+b^2}{4} \\ &= \frac{a^2+b^2}{2} \\ &= \frac{m}{2}p. \end{aligned}$$

Or, on a $\frac{m}{2} < m$ et $\frac{m}{2} \in \mathbb{N}^*$ car m est un entier strictement positif. Le calcul précédent prouve que $\frac{m}{2} \in E$, ce qui absurde car $\frac{m}{2}$ est strictement plus petit que le minimum de E ! On en déduit que m est forcément impair.

7) On suppose l'absurde que $m \geq 3$.

a) On peut vérifier cette égalité en développant les deux expressions. On peut également voir cette égalité en posant $z_1 = \alpha + i\beta$ et $z_2 = \delta + i\gamma$. On a alors :

$$\begin{aligned} (\alpha^2+\beta^2)(\gamma^2+\delta^2) &= |z_1|^2 \times |z_2|^2 \\ &= |z_1 z_2|^2 \\ &= |(\alpha\delta - \beta\gamma) + i(\alpha\gamma + \beta\delta)|^2 \\ &= (\alpha\gamma + \beta\delta)^2 + (\alpha\delta - \beta\gamma)^2. \end{aligned}$$

b) Soient $a_0, b_0 \in \mathbb{Z}$ tels que $|a_0| < \frac{m}{2}$, $|b_0| < \frac{m}{2}$, et $a_0 \equiv a\ [m]$, $b_0 \equiv b\ [m]$ (tout existe d'après la question préliminaire puisque m est impair). On pose $n = a_0^2 + b_0^2$. Supposons par l'absurde que $n = 0$. Puisque n est une somme de termes positifs, on en déduit que $a_0 = b_0 = 0$. On a donc $a \equiv 0\ [m]$ et $b \equiv 0\ [m]$, ce qui entraine que m divise a et m divise b. Puisque $a^2 + b^2 = mp$, on en déduit en divisant par m^2 que :

$$\left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2 = \frac{p}{m}.$$

Or, on a à gauche une somme d'entiers (tout est entier et on élève au carré). On en déduit que m divise p, ce qui implique puisque p est premier et $m > 1$ que $m = p$. Or, on a montré à la question II.5.b que l'on avait $m < p$. On a donc une absurdité, ce qui entraine que $n \neq 0$.

c) Puisque $a^2 + b^2 = mp$, on a $a^2 + b^2 \equiv 0\ [m]$. Puisque $a_0 \equiv a\ [m]$ et $b_0 \equiv b\ [m]$, on en déduit que $n = a_0^2 + b_0^2 \equiv 0\ [m]$. On a donc $a_0^2 + b_0^2$ divisible par m, ce qui entraine qu'il existe $u \in \mathbb{N}$ (car tout est positif) tel que $n = um$. D'après la question précédente, $n \neq 0$ donc on a $1 \leq u$.

De plus, on a $a_0^2 < \dfrac{m^2}{4}$ (toujours par stricte croissante de $x \mapsto x^2$ sur $\mathbb{R}_+$) et $b_0^2 < \dfrac{m^2}{4}$ donc $n < \dfrac{m^2}{2}$. On a donc $um < \dfrac{m^2}{2}$, ce qui entraine $u < \dfrac{m}{2}$.

d) On a $um = n = a_0^2 + b_0^2$ et $mp = a^2 + b^2$. D'après l'identité de Lagrange, on a :

$$\begin{aligned}(um) \times (mp) &= (a_0^2 + b_0^2)(a^2 + b^2) \\ &= (a_0 a + b_0 b)^2 + (a_0 b - a b_0)^2.\end{aligned}$$

On en déduit que $m^2 up$ s'écrit comme une somme de deux carrés. De plus, on remarque que :

$$\begin{aligned}a_0 a + b_0 b &\equiv a^2 + b^2 \ [m] \\ &\equiv 0 \ [m]\end{aligned}$$

et que :

$$\begin{aligned}a_0 b - a b_0 &\equiv ab - ab \ [m] \\ &\equiv 0 \ [m]\end{aligned}$$

On a donc m qui divise $a_0 a + b_0 b$ et $a_0 b - a b_0$. Ceci entraine que $\dfrac{a_0 a + b_0 b}{m}$ et $\dfrac{a_0 b - a b_0}{m}$ sont entiers. Or, on a :

$$up = \left(\frac{a_0 a + b_0 b}{m}\right)^2 + \left(\frac{a_0 b - a b_0}{m}\right)^2.$$

up s'écrit donc comme une somme de deux carrés d'entiers.

e) On a $1 \leq u$ et u entier et up s'écrit comme une somme de deux carrés d'entiers donc $u \in E$. Or, on a $u < m$ donc on a construit un élément strictement plus petit que le minimum : absurde !

On en déduit que $m = 1$. Ceci prouve qu'il existe $a, b \in \mathbb{N}$ tels que $a^2 + b^2 = p$, ce qui montre bien que si $p \equiv 1$ [4], alors p s'écrit comme une somme de deux carrés d'entiers. L'autre sens a été montré dans la question I.1, on a bien montré l'équivalence demandée.