Réponses de Michel Lafond (Dijon) et Pierre Renfer (Saint-Georges d'Orques).

La lettre p désignera toujours un nombre premier. Pour $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$, on notera abusivement k la classe de k dans $\mathbb{Z}/n\mathbb{Z}$, en mentionnant toujours qu'une égalité a lieu dans $\mathbb{Z}/n\mathbb{Z}$ si tel est le cas. On dira que l'entier $k \in \mathbb{Z}$ est un carré modulo n si l'équation $x^2 = k$ admet (au moins) une solution x dans $\mathbb{Z}/n\mathbb{Z}$.

On rappelle sans démonstration le résultat suivant (dont on trouvera une preuve dans tout bon livre d'arithmétique ou par exemple dans l'excellent ouvrage « Exercices de mathématiques pour l'agrégation » de **Serge Francinou** et **Hervé Gianella**, publié chez Masson).

Théorème 1 (Théorème des deux carrés)

Un entier $n \in \mathbb{N}^*$ peut s'écrire comme somme de deux carrés d'entiers si et seulement si, dans sa décomposition en facteurs premiers, les facteurs premiers congrus à 3 *modulo* 4 *apparaissent avec un exposant pair.*

On va montrer qu'un entier $n \in \mathbb{N}^*$ est pythagoricien si et seulement si, dans la décomposition de n en produit de facteurs premiers, le facteur 2 et les facteurs premiers congrus à 3 modulo 4 apparaissent avec un exposant au plus égal à 1.

• On commence par montrer qu'un entier n divisible par p^2 avec $p = 2$ ou p congru à 3 modulo 4 ne peut être pythagoricien. Soit n un tel entier et p un tel facteur premier de n. Si, pour tout $k \in \mathbb{Z}/n\mathbb{Z}$, l'équation $k = x^2 + y^2$ a une solution $(x,y) \in (\mathbb{Z}/n\mathbb{Z})^2$, alors, pour tout $k \in \mathbb{Z}/p^2\mathbb{Z}$, l'équation $k = x^2 + y^2$ a une solution $(x,y) \in (\mathbb{Z}/p^2\mathbb{Z})^2$. Or si $p = 2$, l'équation $3 = x^2 + y^2$ n'a pas de solution dans $\mathbb{Z}/4\mathbb{Z}$, puisque, dans $\mathbb{Z}/4\mathbb{Z}$, les carrés valent 0 ou 1, donc la somme de deux carrés vaut 0, 1 ou 2, jamais 3. Et si $p \equiv 3 \bmod 4$, l'équation $p = x^2 + y^2$ ne peut avoir de solution dans $\mathbb{Z}/p^2\mathbb{Z}$. Sinon, il existerait trois entiers a, b, $c \in \mathbb{Z}$ tels que $p = a^2 + b^2 - cp^2$, soit encore $a^2 + b^2 = p(1 + cp)$. Mais alors l'entier $p(1 + cp)$ serait divisible par p et pas par p^2, tandis que p doit apparaître dans $a^2 + b^2$ avec un exposant pair, d'où la contradiction.

La suite de ce texte est consacré à la contraposée : tout entier n, divisible ni par 4 ni par aucun nombre p^2 avec p premier congru à 3 modulo 4, est pythagoricien.

• On commence par le cas où n est un nombre premier p. Le cas $p = 2$ est évident. Pour $p \geq 3$, l'idée classique est de remarquer qu'il y a $\dfrac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$. En effet, l'application définie sur $\mathbb{Z}/p\mathbb{Z} - \{0\}$ par $g \mapsto g^2$ a pour image l'ensemble des

carrés non nuls. Et tout carré non nul possède exactement deux antécédents, puisque dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $a^2 = b^2$ impose $(a - b)(a + b) = 0$, soit $a = b$ ou $a = -b$. Il y a donc $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$, soit $\frac{p+1}{2}$ carrés en ajoutant 0. Soit alors $k \in \mathbb{Z}/p\mathbb{Z}$. Les ensembles $\{k - x^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\}$ et $\{y^2 \mid y \in \mathbb{Z}/p\mathbb{Z}\}$, tous deux de cardinal $\frac{p+1}{2}$, ne peuvent être disjoints. Il existe donc $x, y \in \mathbb{Z}/p\mathbb{Z}$ tels que $k - x^2 = y^2$. Ainsi, tout $k \in \mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés.

• Pour étendre le résultat au cas où $n = p^\alpha$, où p est un nombre premier, $p \equiv 1 \bmod 4$, et α est un entier, $\alpha \geq 2$, on énonce un petit lemme :

Lemme 1

Soit p un nombre premier, $p \geq 3$, $\alpha \in \mathbb{N}^*$ et $k \in \mathbb{Z}$ non divisible par p. Alors k est un carré modulo p si et seulement si k est un carré modulo p^α.

Si k est un carré modulo p^α, comme α est supérieur ou égal à 1, alors k est un carré modulo p. Pour montrer l'autre sens, on suppose que l'équation $x^2 = k$ a au moins une solution x dans $\mathbb{Z}/p\mathbb{Z}$. On va montrer par récurrence sur $\alpha \in \mathbb{N}^*$ que l'équation $x^2 = k$ a au moins une solution x dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. Pour $\alpha = 1$, c'est l'hypothèse. On suppose le résultat établi à un rang $\alpha \geq 1$. Il existe donc deux entiers X, $m \in \mathbb{Z}$ tels que $k = X^2 + mp^\alpha$. Pour $\lambda \in \mathbb{Z}$,

$$\begin{aligned}\left(X + \lambda p^\alpha\right)^2 &= X^2 + 2\lambda X p^\alpha + \lambda^2 p^{2\alpha} \\ &= k + \left(2\lambda X - m\right) p^\alpha + \lambda^2 p^{2\alpha}.\end{aligned}$$

Comme $2\alpha \geq \alpha + 1$,

$$\left(X + \lambda p^\alpha\right)^2 = k + \left(2\lambda X - m\right) p^\alpha \mod p^{\alpha+1}.$$

Comme k n'est pas divisible par p et comme $p \geq 3$, l'entier 2X est premier à p, donc est inversible dans $\mathbb{Z}/p\mathbb{Z}$, ce qui permet de choisir l'entier $\lambda \in \mathbb{Z}$ tel que $2\lambda X \equiv m \bmod p$. En posant $Y = X + \lambda p^\alpha \in \mathbb{Z}$, on obtient $Y^2 \equiv k \bmod p^{\alpha+1}$, ce qui clôt la démonstration.

• Comme annoncé, on montre maintenant que p^α est pythagoricien (toujours avec p premier, $p \equiv 1 \bmod 4$ et $\alpha \in \mathbb{N}^*$). Soit $k \in \mathbb{Z}$. On veut montrer que $k = x^2 + y^2 \bmod p^\alpha$ a une solution $(x,y) \in \mathbb{Z}^2$. Pour cela, on écrit $k = p^j k'$ avec $j \in \mathbb{N}$ et k' premier avec p. On sait (par le théorème des deux carrés) que p^j est somme de deux carrés dans $\mathbb{Z}$ (donc dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ en réduisant modulo p^α). On sait également que le produit de sommes de deux carrés est encore une somme de deux carrés dans $\mathbb{Z}$ (donc dans $\mathbb{Z}/p^\alpha\mathbb{Z}$), en vertu de l'identité de Lagrange : pour $a, b, c, d \in \mathbb{Z}$,

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

ll suffit donc de montrer que k' est somme de deux carrés modulo p^α. Puisque tout nombre premier est pythagoricien (traité plus haut), il existe $(x_0, y_0) \in \mathbb{Z}^2$ tel que $k' = x_0^2 + y_0^2 \mod p$. Si y_0 n'est pas divisible par p, l'entier $k' - x_0^2$ est un carré modulo p, donc modulo p^α : il existe $y \in \mathbb{Z}$ tel que $k' - x_0^2 = y^2$, ce qui conclut. Le cas où x_0 n'est pas divisible par p est semblable. Enfin, le cas où p divise à la fois x_0 et y_0 est exclu car sinon, p diviserait k'.

• Enfin, on montre que si deux entiers m, $n \in \mathbb{N}^*$, premiers entre eux, sont pythagoriciens, alors leur produit mn est pythagoricien. Soit $k \in \mathbb{Z}$. Puisque m et n sont pythagoriciens, il existe quatre entiers $a, b, c, d \in \mathbb{Z}$ tels que

$$k \equiv a^2 + b^2 \mod m$$

et

$$k \equiv c^2 + d^2 \mod n.$$

Puisque m et n sont premiers entre eux, il existe $\lambda, \mu \in \mathbb{Z}$ tels que

$$\lambda m + \mu n = 1.$$

On considère alors

$$\mathrm{A} = \lambda mc + \mu na \text{ et } \mathrm{B} = \lambda md + \mu nb.$$

Alors

$$\mathrm{A} = \lambda mc + \mu na = \lambda mc + (1 - \lambda m)a,$$

donc $\mathrm{A} \equiv a \mod m$, tandis que

$$\mathrm{A} = \lambda mc + \mu na = (1 - \mu n)c + \mu na,$$

donc $\mathrm{A} \equiv c \mod n$. De même $\mathrm{B} \equiv b \mod m$ et $\mathrm{B} \equiv d \mod n$. Donc

$$\mathrm{A}^2 + \mathrm{B}^2 \equiv a^2 + b^2 \mod m,$$

soit

$$\mathrm{A}^2 + \mathrm{B}^2 \equiv k \mod m,$$

et de même,

$$\mathrm{A}^2 + \mathrm{B}^2 \equiv k \mod n.$$

Enfin, puisque m et n sont premiers entre eux,

$$\mathrm{A}^2 + \mathrm{B}^2 \equiv k \mod mn,$$

ce qu'il fallait démontrer.

• Si maintenant n n'est divisible ni par 2 ni par aucun p^2 avec $p \equiv 3 \mod 4$, on écrit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$, l'ensemble $\mathcal{P}$ désignant l'ensemble des nombres premiers. Chaque facteur $p^{v_p(n)}$ étant pythagoricien, le produit n l'est encore.

En commentaires, on peut remarquer que le lemme 1 est un cas particulier du lemme de Hensel : soit P un polynôme à coefficients dans l'anneau $\mathbb{Z}_p$ des entiers p-adiques et $a_0 \in \mathbb{Z}_p$ tel que $P(a_0) \equiv 0 \bmod p$ et $P'(a_0) \not\equiv 0 \bmod p$. Alors, il existe $a \in \mathbb{Z}_p$ tel que $P(a) = 0$ et $a \equiv a_0 \bmod p$. Le lemme s'obtient en prenant $P(X) = X^2 - k$ (d'où la nécessité du $p \neq 2$). Et le calcul des entiers A et B ci-dessus résulte bien sûr du théorème des restes chinois.