Sinon trois au moins des distances de z_0, z_1, z_2, z_3 aux demi-impairs les plus proches sont majorées par $\frac{1}{4}$.
On prend $t = \left([x_0]+\frac{1}{2}\right) + \left([x_1]+\frac{1}{2}\right)e_1 + \left([x_2]+\frac{1}{2}\right)e_2 + \left([x_3]+\frac{1}{2}\right)e_3$ et on a bien $N(s-t) \leq \frac{5}{8}$
Soit maintenant $(u,v) \in A \times (A-\{0\})$; d'après ce qui précède, $\exists q', q'' \in A$ tels que: $N(q'-uv^{-1}) \leq \frac{5}{8}$
$N(q''-v^{-1}u) \leq \frac{5}{8}$
On pose $r' = u - q'v$, $r'' = u - vq''$ et $N(r') \leq \frac{5}{8}N(v)$, $N(r'') \leq \frac{5}{8}N(v)$, ce qui donne deux inégalités strictes car $v \neq 0$.
Soit J un idéal à gauche de A, non nul. Soit $v \in J\setminus\{0\}$ tel que $N(v)$ soit minimal sur $J\setminus\{0\}$ (v existe car pour tout $z \in A$, $N(z)$ est de la forme $\frac{n}{4}$ où $n \in \mathbb{N}$. Soit u un autre élément de J. Il existe q' et r' dans A tels que:
$u = q'v + r'$, $N(r') < N(v)$
Comme J est un idéal à gauche de A, r' est élément de J et par conséquent $r' = 0$ sans quoi $N(r') < N(v)$ serait impossible. On a donc $J \subset Av$, d'où $J = Av$. De même tout idéal à droite est de la forme vA.

4/ D'après ce qui précède, il existe a et b entiers tels que p divise $1+a^2+b^2$. Considérons J l'idéal à gauche $Ap + A(1+ae_1+be_2)$, inclus dans A. J est distinct de A car les normes des éléments de J sont toutes divisibles par p. J est distinct de Ap car $1+ae_1+be_2 \notin Ap$.
Soit alors q tel que $J = Aq$; q n'est pas de norme 1 car $J \neq A$.
Il existe $q' \in A$ tel que $p = q'q$ et $N(q') \neq 1$ car $J \neq Ap$.
$N(q)\,N(q') = N(p) = p^2$ d'où $N(q) = N(q') = p$.
Supposons que q soit élément de A_1 ; alors p est bien somme de quatre carrés d'entiers. Sinon q s'écrit sous la forme:
$2(z_0 + z_1e_1 + z_2e_2 + z_3e_3) + \frac{\pm 1 \pm e_1 \pm e_2 \pm e_3}{2}$ où z_0, z_1, z_2, z_3 sont entiers.
Soit $z = \frac{\pm 1 \pm e_1 \pm e_2 \pm e_3}{2}$. $N(z) = 1$ et il est aisé de voir que $\bar{z}q \in A_1$
(on définit $\overline{(a+be_1+ce_2+de_3)} = a - be_1 - ce_2 - de_3$)
Comme $N(\bar{z}q) = p$, p peut encore s'écrire comme somme de quatre carrés d'entiers.
Remarquons en outre que 2 est aussi somme de quatre carrés d'entiers. Sachant que tout entier s'écrit comme produit de nombres premiers, il suffit d'utiliser le résultat du 1/ pour en déduire que tout nombre entier est somme de quatre carrés d'entiers.

Sommes de deux carrés ORAUX

A-22

1/ Soit x un réel et $N \in \mathbb{N}^*$; prouver qu'il existe des entiers p et q tels que : $1 \leq q \leq N$ et $|qx - p| \leq \frac{1}{N+1}$

2/ Soit $n \in \mathbb{N}^* \setminus \{1\}$ et $A \in \mathbb{N}^*$ tels que n divise $1+A^2$. Prouver que n est somme de deux carrés. [On pourra poser $B = (Aq-pn)^2 + q^2$ après avoir appliqué le 1/ à $x = \frac{A}{n}$ et $N = [\sqrt{n}]$ (partie entière)].

3/ Soient a et b deux entiers premiers entre eux tels que n divise a^2+b^2, prouver que n est somme de deux carrés.

4/ Soit p premier impair, prouver que $a \in \mathbb{F}_p^*$ est un carré dans $(\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z})$ si et seulement si : $a^{\frac{p-1}{2}} = 1$ (modulo p). Quand -1 est-il un carré dans $\mathbb{F}_p$? Déduire du 2/ que :
(p est somme de deux carrés) $\Leftrightarrow$ $p \equiv 1$ modulo 4.

5/ Prouver que tout produit de somme de deux carrés est somme de deux carrés. Prouver que si n est somme de deux carrés et si p premier $\equiv 3$ modulo 4 divise n, alors l'exposant de p dans la décomposition en facteurs premiers de n est pair.

6/ En déduire une CNS pour que $n \in \mathbb{N}$ soit somme de deux carrés.

E.N.S.

1/ Considérons les $N+1$ nombres $nx - [nx]$, $0 \leq n \leq N$, rangés dans l'ordre croissant $0 = a_0 \leq a_1 \leq \ldots \leq a_N < 1$. Posons $b_i = a_{i+1} - a_i$ pour $i = 0, \ldots, N-1$ et $b_N = 1 - a_N$. Les b_i sont > 0 et $b_0 + \ldots + b_N = 1$, donc pour l'un au moins des indices i, $0 \leq b_i \leq \frac{1}{N+1}$ (principe des tiroirs).
Donc, il existe $j, k \in \{0, 1, \ldots N\}$ tels que : $|jx - kx - p'| \leq \frac{1}{N+1}$ où p' est un entier convenable. $j \neq k$
Le 1/ en résulte facilement.

2/ On suit l'indication : $B = (1+A^2)q^2 + p^2n^2 - 2Aqpn$ donc n divise B,
mais : $\left|\begin{array}{l} |Aq - pn| \leq \frac{n}{N+1} < \sqrt{n} \\ q \leq N \leq \sqrt{n} \end{array}\right.$
donc : $\left|\begin{array}{l} B < 2n \\ n \text{ divise } B \end{array}\right.$ donc $n = B = (Aq-pn)^2 + q^2$

3/ D'après Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tel que: $au + bv = 1$. On a :
$(a^2+b^2)(u^2+v^2) = (au+bv)^2 + (av-bu)^2 = 1 + (av-bu)^2$
donc n divise $1 + (av-bu)^2$. Le 2/ donne le résultat.

4/ C'est archi-classique et a été fait dans l'exercice précédent. On note que
p premier impair $\Rightarrow$ $p \equiv 1\,(4)$ ou $p \equiv 3\,(4)$ et on vérifie que:
$(p \equiv 1(4)) \Rightarrow (\exists \alpha \in \mathbb{N}$, p divise $1+\alpha^2$ et donc p est somme de deux carrés)
$(p \equiv 3(4)) \Rightarrow (p$ n'est pas somme de deux carrés)

5/ On a l'identité de Lagrange : $(a^2+b^2)(c^2+d^2) = (ad+bc)^2 + (ac-bd)^2$.
Soit n somme de 2 carrés et p premier $\equiv 3(4)$ divisant n.
$n = a^2+b^2$. Soit $d = a \wedge b$, alors $\frac{n}{d^2} = a'^2 + b'^2$ avec $\left|\begin{array}{l} a' \wedge b' = 1 \\ da' = a \\ db' = b \end{array}\right.$

Si l'exposant de p était impair alors, p divisant $\frac{n}{d^2} = a'^2+b'^2$, le 3/ impliquerait que p serait somme de 2 carrés, ce qui est faux. Cette contradiction montre que l'exposant de p est pair.

6/ En combinant le 4/ et le 5/, on obtient :
(n est somme de 2 carrés) $\Leftrightarrow$ (tout diviseur premier impair de n qui apparaît avec un exposant impair dans la décomposition de n en facteurs premiers est $\equiv 1(4)$.)
Ainsi : $7\times5 = 35$ n'est pas somme de 2 carrés.

A-23

On appelle réseau de $\mathbb{R}^2$ tout ensemble $H = \mathbb{Z}\vec{u} + \mathbb{Z}\vec{v}$ où $(\vec{u},\vec{v})$ est une base de $\mathbb{R}^2$. $(\vec{u},\vec{v})$ est appelée une $\mathbb{Z}$-base de H.

1/ Soit $e=(e_1,e_2)$ la base canonique de $\mathbb{R}^2$. Prouver que $|\det(\vec{u},\vec{v})| = |\det_e(\vec{u},\vec{v})|$ ne dépend pas du choix de la $\mathbb{Z}$-base de H. On note V(H) cet invariant. C'est l'aire du parallélogramme délimité par $\vec{u}$ et $\vec{v}$.

2/ Soit $R>0$ et B(0,R) la boule fermée de centre 0 et de rayon R. On suppose : $\pi R^2 > V(H)$. Prouver qu'il existe $x,y \in B(0,R)$, $x \neq y$ tel que : $x-y \in H$. [[On introduira $P_H = \{t\vec{u}+t'\vec{v},\ 0\le t<1,\ 0\le t'<1\}$ Comme $\mathbb{R}^2$ est la réunion disjointe des $h+P_H$ pour $h\in H$, on écrira $m[B(0,R)] = \sum_{h\in H} m[(h+P_H)\cap B(0,R)]$ où m(A) désigne l'aire d'un sous-ensemble A quarrable de $\mathbb{R}^2$. On supposera que les $(B(0,R)-h)\cap P_H$ sont deux à deux disjoints pour $h\in H$ et on utilisera le fait que : $m[A] = m[A-h]$ si A est quarrable]].

3/ On suppose : $\pi R^2 > 2^2 V(H)$. Prouver que : $H\cap B(0,R) \neq \{0\}$. [[On appliquera le 2/ à $B(0,\frac{R}{2})$]].

4/ Soit p premier congru à 1 modulo 4, prouver qu'il existe $\alpha\in\mathbb{N}$ tel que : $1+\alpha^2 \equiv 0\ (p)$.

5/ On pose : $H = \mathbb{Z}(1,\alpha)\oplus\mathbb{Z}(0,p)$. Quel est V(H) ? Prouver qu'il existe $(a,b)\in\mathbb{Z}^2$ tel que : $0<a^2+b^2\le 2p$. [[On pourra poser $R=\sqrt{2p}$ et appliquer le 3/]].
Déduire du 4/ que : $p = a^2+b^2$.

E.N.S. Ulm

1/ Soit $(\vec{u}',\vec{v}')$ une autre $\mathbb{Z}$-base de $\mathbb{R}$. Soit P la matrice de passage de $(\vec{u},\vec{v})$ à $(\vec{u}',\vec{v}')$. P et P^{-1} sont à coefficients dans $\mathbb{Z}$, donc $|\det P| = 1$.
On a : $|\det_e(\vec{u},\vec{v})| = |\det_{(\vec{u}',\vec{v}')}(\vec{u},\vec{v})|\,|\det_e(\vec{u}',\vec{v}')| = \det_e(\vec{u}',\vec{v}')$, donc $|\det(\vec{u},\vec{v})|$ ne dépend pas du choix de la $\mathbb{Z}$-base.

2/ On a : $m[B(0,R)] = \pi R^2 = \sum_{h\in H} m[(h+P_H)\cap B(0,R)]$, cette somme est finie.
On a : $m[(h+P_H)\cap B(0,R)] = m[P_H\cap(B(0,R)-h)]$.
Si les $P_H\cap(B(0,R)-h)$ étaient deux à deux disjoints alors on aurait :
$m(P_H) \ge \sum_{h\in H} m[P_H\cap(B(0,R)-h)]$ cette somme est finie.
Or ceci contredit le fait que : $m[B(0,R)] > m(P_H)$, donc :
$\exists h,h'\in H,\ h\neq h',\ \exists x,y\in B(0,R),\ \exists p\in P_H,\ x-h = y-h' = p$ donc : $x\neq y$ et $x-y\in H$.

3/ D'après 2/, il existe $x,y\in B(0,\frac{R}{2})$, $x\neq y$, $x-y\in H$. On a : $2x, 2y\in B(0,R)$ qui est convexe et symétrique par rapport à 0. Donc : $x-y = \frac{1}{2}(2x-2y)\in B(0,R)$
Donc : $H\cap B(0,R)\neq\{0\}$.

4/ c'est classique. p est premier ≥ 3, $\Psi\left|\begin{array}{ccc}\mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ u & \longmapsto & u^2\end{array}\right.$ est un morphisme de groupes de noyau $\{1,-1\}$ ($1\neq -1$ dans $\mathbb{F}_p$ car $p\neq 2$). On a : $\operatorname{card}\mathbb{F}_p^* = p-1$
donc $\operatorname{card}\operatorname{Im}\Psi = \frac{p-1}{2}$. $= \operatorname{card}(\ker\Psi)\operatorname{card}\operatorname{Im}\Psi$.
$\forall x\in\mathbb{F}_p^*$, on a : $x^{p-1}=1$, $X^{p-1}-1$ admet donc $p-1$ racines distinctes.
$X^{p-1}-1 = (X^{\frac{p-1}{2}}-1)(X^{\frac{p-1}{2}}-1)$
$\forall v\in\operatorname{Im}\Psi$, on a : $v^{\frac{p-1}{2}} = 1$. Or $X^{\frac{p-1}{2}}-1$ a au plus $\frac{p-1}{2}$ zéros et $\operatorname{Im}\Psi \subset$ {zéros de $X^{\frac{p-1}{2}}-1$}. Donc : (v est un carré dans $\mathbb{F}_p^*$) $\Leftrightarrow$ ($v^{\frac{p-1}{2}}-1=0$)
Si $p\equiv 1(4)$ alors : $(-1)^{\frac{p-1}{2}} - 1 = 0(p)$ donc -1 est un carré, donc il existe $\alpha\in\mathbb{N}$ tel que $p\mid 1+\alpha^2$

5/ $V(H) = \left|\det\begin{pmatrix}1 & 0\\ \alpha & p\end{pmatrix}\right| = p$. On a : $\pi\sqrt{2p}^2 = 2\pi p > 2^2 p$. Le 3/ assure qu'il existe $a'(1,\alpha) + b'(0,p) \in \left(B(0,\sqrt{2p})\cap H\right)\setminus\{0\}$ avec $a'\in\mathbb{Z}$, $b'\in\mathbb{Z}$. On a donc :
$0 < \|a'(1,\alpha) + b'(0,p)\|^2 = a'^2 + (a'\alpha+pb')^2 \le 2p$
On a : $a'^2 + (a'\alpha+pb')^2 = a'^2 + a'^2\alpha^2 + p^2b'^2 + 2a'\alpha pb'$.
p divise $a'^2(1+\alpha^2)$ donc p divise $a'^2 + (a'\alpha+pb')^2$.
Comme : $0 < a'^2 + (a'\alpha+pb')^2 \le 2p$ et $p\ge 3$, on a : $a'^2 + (a'\alpha+pb')^2 = p$

A-24

Pour $n\in\mathbb{N}^*$, on note $\Psi(n)$ le nombre d'entiers $\in\{1,\dots,n\}$ premiers à n.

1/ Prouver que : $n = \sum_{d\mid n}\Psi(d)$ (raisonner dans $\mathbb{Z}/n\mathbb{Z}$)

2/ Pour $n\in\mathbb{N}^*$, on pose : $\Phi_n(X) = \prod_{i=1}^{\Psi(n)}(X-\xi_i)$, où $\xi_1,\dots,\xi_{\Psi(n)}$ sont les générateurs du sous-groupe de $(\mathbb{C}^*,\times)$ engendré par $e^{2i\pi/n}$. Prouver que $X^n-1 = \prod_{d\mid n}\Phi(d)$.

3/ Soit K un corps fini, soit Z son centre. On pose $q = \operatorname{card} Z$; vérifier que Z est un corps ; prouver que $\operatorname{card} K$ est de la forme q^n. Soit $x\in K$ et $K_x = \{y\in K \mid yx = xy\}$. Prouver que $\operatorname{card} K_x = q^d$, où d divise n.