Théorème des deux carrés

Francinou-Gianella-Nicoas, *Oraux X-ENS Algèbre 1*, page 145

Exercice :
Soit p un nombre premier impair.

1. Montrer que si p est une somme de deux carrés d'entiers, on a nécessairement $p \equiv 1[4]$.

   On suppose à présent que p congru est à 1 modulo 4.

2. Dénombrer les carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.
3. En déduire qu'il existe $n \in \mathbb{Z}$ tel que $n^2 \equiv -1[p]$
4. Démontrer qu'il existe $(a,b) \in \mathbb{Z}^2$ tels que
$$0 < \sqrt{b} < \sqrt{p} \quad \text{et} \quad \left| b\frac{n}{p} - a \right| \leq \frac{1}{\sqrt{p}}$$
5. Montrer que $p = (bn - ap)^2 + b^2$.

1. Modulo 4, un carré est congru à 0 ou 1. Si un entier est somme de deux carrés, il sera donc congru modulo 4 à 0, 1 ou 2.

   Comme p est un entier premier impair, il ne peut être congru ni à 0 ni à 2 (car il serait alors divisible par 2). Il s'ensuit qu'un entier premier impair, somme de deux carrés d'entiers est congru à 1 modulo 4.

2. p étant premier, $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ est un corps. On a donc, si $x, y \in \mathbb{K}^*$,
$$x^2 = y^2 \Leftrightarrow (x-y)(x+y) = 0 \Leftrightarrow x = y \text{ ou } x = -y$$
   Par conséquent, à tout carré de $\mathbb{K}^*$, correspondent exactement deux antécédents dans $\mathbb{K}^*$ par l'application $x \mapsto x^2$ (on a bien pour $x \in \mathbb{K}^*$, $x \neq -x$ puisque la caractéristique de $\mathbb{K}$ est $p > 2$). Il y a donc $\dfrac{Card(\mathbb{K}^*)}{2} = \dfrac{p-1}{2}$ carrés dans $\mathbb{K}^*$.

3. Il suffit de prouver que -1 est un carré dans $\mathbb{K}$. Si $x \in \mathbb{K}^*$ est un carré, on peut écrire $x = y^2$ avec $y \in \mathbb{K}^*$ et d'après le petit théorème de Fermat,
$$x^{(p-1)/2} = y^{2(p-1)/2} = y^{p-1} = 1$$
   Donc x est racine du polynôme $P = X^{(p-1)/2} - 1$. Les $\dfrac{p-1}{2}$ carrés non nuls de $\mathbb{K}$ sont donc racines de P. Or, P a au plus $\dfrac{p-1}{2}$ racines (distinctes ou confondues) dans le corps $\mathbb{K}$. Nécessairement P est scindé et ses racines sont exactement les carrés de $\mathbb{K}^*$.
   Comme $p \equiv 1[4]$, on a que $\dfrac{p-1}{2}$ est pair, ainsi $(-1)^{(p-1)/2} = 1$ et -1 est un carré dans $\mathbb{K}$.

4. Posons $N = E(\sqrt{p}) + 1$ et $\xi = \dfrac{n}{p}$. Considérons les N réels $x_k = k\xi - E(k\xi)$ de l'intervalle $[0,1[$ pour $0 \leq k \leq N-1$ et les N intervalles $\left[0, \dfrac{1}{N}\right[$, $\left[\dfrac{1}{N}, \dfrac{2}{N}\right[$, $\ldots$, $\left[\dfrac{N-1}{N}, 1\right[$.

   - Supposons d'abord que l'un des x_k soit dans $\left[\dfrac{N-1}{N}, 1\right[$. Comme $x_0 = 0$, on a $k > 0$ et si on pose $b = k$ et $a = E(k\xi) + 1$, on obtient :
$$0 < b \leq N - 1 < \sqrt{p} \qquad \text{et} \qquad \left| b\frac{n}{p} - a \right| = |x_k - 1| \leq \frac{1}{N} \leq \frac{1}{\sqrt{p}}$$
     l'inégalité $N - 1 < \sqrt{p}$ étant stricte car $\sqrt{p} \notin \mathbb{N}$.

- Dans le cas contraire, les N réels x_k sont dans les $N-1$ intervalles $\left[\frac{k}{N}, \frac{k+1}{N}\right[$ avec $0 \leq k \leq N-2$. D'après le principe des tiroires, il existe k et l distincts tels que x_k et x_l soient dans le même intervalle. Supposons par exemple $k < l$. Notons alors $b = l - k$ et $a = E(l\xi) - E(k\xi)$. On a de nouveau

$$0 < b \leq N - 1 < \sqrt{p} \qquad \text{et} \qquad \left| b\frac{n}{p} - a \right| = |(l-k)\xi - (E(l\xi) - E(k\xi))| = |x_l - x_k| \leq \frac{1}{N} \leq \frac{1}{\sqrt{p}}$$

Dans tous les cas, nous avons démontré l'existence de $(a, b) \in \mathbb{Z}^2$ tel que

$$0 < b < \sqrt{p} \qquad \text{et} \qquad \left| b\frac{n}{p} - a \right| \leq \frac{1}{\sqrt{p}}$$

5. Les inégalités obtenues dans la question précédente impliquent que

$$0 < b^2 < p \quad \text{et} \quad (bn - ap)^2 \leq p \quad \text{et donc} \quad 0 < (bn - ap)^2 + b^2 < 2p$$

D'autre part, on a $n^2 + 1 \equiv 0[p]$ et donc

$$(bn - ap)^2 + b^2 = b^2(n^2 + 1) - 2admp + a^2p^2 \equiv 0[p]$$

Comme cet entier appartient à $]0, 2p[$, cela implique l'égalité :

$$(bn - ap)^2 + b^2 = p$$

Conclusion : Tout nombre premier impair est somme de deux carrés d'entiers si et seulement s'il est congru à 1 modulo 4.