Pour tout $n \in \mathbb{N}$ on note $\sigma(n)$ la somme de ses diviseurs, propres et non propres. On pose $S = \{n \mid \ 3 \mid n \text{ et } 3 \nmid \sigma(n) - n\}$. Notre but est de montrer que S est compris dans l'ensemble des nombres qui s'écrivent comme $x^2 + xy + y^2$ avec $x, y \in \mathbb{N}$, appeleés par certains auteurs nombres de Löschian.

Définition 1 *On note* $j = \exp(\frac{2i\pi}{3})$ *et on considère l'anneau* $\mathbb{Z}[j]$. *Pour tout* $\alpha = a + bj \in \mathbb{Z}[j]$ *on appelle norme de* α *la quantité* $N(\alpha) := |\alpha|^2$ *où* $|\alpha|$ *désigne le module de* α. *On dit qu'un entier* n *est une norme s'il existe* $\alpha \in \mathbb{Z}[j]$ *tel que* $n = N(\alpha)$

Proposition 1 *L'anneaux* $\mathbb{Z}[j]$ *a les propriétés suivantes.*

1. *Pour tous* $\alpha, \beta \in \mathbb{Z}[j]$ *on a* $N(\alpha\beta) = N(\alpha)N(\beta)$. *En particulier, l'ensemble des normes est multiplicatif.*

2. *Pour tout* $\alpha \in \mathbb{Z}[j]$ *il existe* $\beta \in \mathbb{Z}[j]$ *tel que* $N(\alpha) = N(\beta)$ *et* $\beta = x + jy$ *avec* $x, y \geq 0$.

3. *Les éléments de* $\mathbb{Z}[j]$ *de norme* 1 *sont exactement les unités.*

preuve:

1. On a $N(a)N(b) = |a|^2|b|^2 = |ab|^2 = N(ab)$. En particulier on voit que le produit $N(a)N(b)$ de deux normes est une norme: $N(ab)$.

2. On a $N(j) = |j|^2 = 1$. Une analyse des cas montre qu'au moins un des nombres $\alpha, j\alpha, j^2\alpha, -\alpha, -j\alpha, -j^2\alpha$ vérifie les conditions sur β. Géométriquement, cela revient à faire une rotation pour qu'un nombre complexe soit dans le premier quartier.

3. Si $u = a + bj$ et $N(u) = 1$, alors $1 = N(a + bj) = (a + bj)(a + j^2b)$, donc $u \mid 1$ et u est une unité. Si u est une unité, alors il existe v tel que $uv = 1$. En prenant les normes, on a $1 = N(u)N(v)$, donc $N(u) = 1$.

□

Proposition 2 *Pour tout* p *premier autre que* 3, *on a:*

$$p \text{ est une norme} \Leftrightarrow p \equiv 1[3].$$

preuve: On considère le polynôme $f = X^2 + X + 1$ et $K := \frac{\mathbb{Q}[X]}{<f>}$ son corps de rupture. La théorie des corps cyclotomiques montre que l'anneau d'entiers de K est $\mathbb{Z}[j]$. Le même argument qui montre que $\mathbb{Z}[i]$ est euclidien montre que $\mathbb{Z}[j]$ est euclidien, donc principal. Par conséquent un premier $p \in \mathbb{Z}$ est réductible dans $\mathbb{Z}[j]$

si et seulement si $p\mathbb{Z}[j]$ se décompose. Or il est connu qu'un premier se décompose sur le corps de rupture d'un polynôme f si et seulement si f est irréductible modulo p (factorisation d'un premier en idéaux). Dans notre cas $deg(f) = 2$, donc f est réductible si et seulement s'il a une racine, ce qui équivaut à $(\frac{disc(f)}{p}) = 1$. Or $disc(f) = 1^2 - 4 \cdot 1 = -3$ et alors $(\frac{disc(f)}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (\frac{-1}{p})(-1)^{\frac{p-1}{2}}(\frac{p}{3})$ par la loi de réciprocité quadratique. Finalement $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$, d'où $(\frac{disc(f)}{p}) = (\frac{p}{3})$ qui vaut 1 si et seulement si p est congruent à 1 modulo 3. Donc un premier p est réductible sur $\mathbb{Z}[j]$ si et seulemet s'il est congruent à 1 mod 3.

Soit maintenant $p \in \mathbb{Z}$ premier, réductible dans $\mathbb{Z}[j]$. Alors $p = \alpha\beta$ avec $\alpha, \beta \in \mathbb{Z}[j]$ tels qu'aucun d'entre eux n'est une unité. En prenant la norme on a: $p^2 = N(\alpha)N(\beta)$. Comme α et β ne sont pas des unités,on a $N(\alpha), N(\beta) > 1$. La seule possibilité est $N(a) = N(b) = p$. Donc p est une norme. Réciproquement, si p est une norme, il esiste $a, b \in \mathbb{Z}$ tels que $N(a + bj) = p$. Cela équivaut à $(a + bj) \cdot (a + bj^2) = p$. Comme $N(a + bj) = N(a + bj^2) = p > 1$, ni $a + bj$, ni $a + bj^2$ n'est une unité, donc p est réductible. Ainsi p est une norme si et seulemt s'il est réductible sur $\mathbb{Z}[j]$.

En regroupant les deux faits, on prouve la proposition. □

Proposition 3 *Un entier n est une norme si et seulement si, pour tout premier p congruent à 2 mod 3, $val_p(n)$ est paire.*

preuve: Soit n tel que tous ses diviseurs premiers congruents à 2 nodulo 3 apparaîssent avec des exposants pairs. Alors $n = 3^{val_3(n)} n_0 m^2$ avec $m \in \mathbb{N}$ et n_0 un produit de premiers $p \equiv 1[3]$. Comme l'ensemble des normes est multiplicatif, grâce à la proposition 2 on déduit que n_0 est une norme. Ensuit, $m^2 = m^2 + m \cdot 0 + 0^2$, donc m^2 est une norme. Finalement $3 = 1 + 1 + 1$ est une norme, donc n est une norme.

Réciproquement, on procède par récurrence sur la somme des exposants des premiers $q \equiv 2[3]$. Si n est une norme qui n'a pas de facteurs premiers congruents à 2 modulo 3 alors il n'y a rien à démontrer. Soit $n = N(a + bj)$ une norme et q un diviseur premier de n tel que $q \equiv 2[3]$ (si q n'existe pas, il n'y a rien à prouver). On note $n_0 = \frac{n}{q}$. Alors on a $n_0 q = (a + bj)(a + j^2 b)$ pour $a, b \in \mathbb{Z}$. D'après la proposition 2, q est irréductible dans $\mathbb{Z}[j]$, donc premier. On déduit que q divise $a + bj$ ou $a + bj^2$. Quitte à répéter les arguments avec j^2 à la place de j on peut supposer $q \mid (a + bj)$. Il existe donc $x, y \in \mathbb{Z}$ tels que $q \cdot (x + jy) = a + bj$. En prenant la norme on a $q^2 N(x + jy) = n$. Comme n_1 a des valuations plus petites que n, l'hypothèse de récurrence nous garantit que tous les facteurs congruents à 2 mod 3 de n_1 apparaîssent avec des exposants pairs. Donc il en est de même pour n. □

On peut maintenent montrer le résultat principal.

Théorème 1 *Tout entier n tel que $3 \mid n$ et $3 \nmid \sigma(n)-n$ s'écrit comme x^2+xy+y^2 avec $x, y \in \mathbb{N}$.*

preuve: Soit n tel que $3 \mid n$ et $3 \nmid \sigma(n)$. Soit $n = 3^v \Pi_{i=1}^k p_i^{t_i} \pi_{j=1}^l q_j^{s_j}$ la décomposition de n en facteurs premiers. On a $\sigma(n) \not\equiv 0[3]$ si et seulement si, pour tout i on a $\sigma(p_i^{t_i}) \not\equiv 0[3]$ et pour tout j on a $\sigma(q_j^{s_j}) \not\equiv 0[3]$. Soit $i \leq k$. Alors $\sigma(p_i^{t_i}) = 1 + p_i + \ldots + p_i^{t_i} \equiv 1 + \ldots + 1[3] \equiv t_i + 1[3]$. Donc $\sigma(p_i^{t_i}) \equiv 0[3]$ si et seulement si $t_i \equiv 2[3]$. Soit $j \leq l$. Alors $\sigma(q_j^{s_j}) = 1+q_j+\ldots+q_j^{s_j} \equiv 1-1+1-1+\ldots+(-1)^{s_j}[3]$. Or cette dernière expression est nulle si et seulement si $s_j \equiv 1[2]$. En particulier, si $3 \nmid \sigma(n)$, alors tout les s_j sont pairs. D'après la proposition 3, n est une norme. Grâce au point 2. de la proposition 1, n s'écrit comme $n = x^2 + xy + y^2$ avec $x, y \in \mathbb{N}$. $\square$