Pierre Lissy

April 29, 2010

On considère l'anneau des entiers de Gauss $Z[i]$, noté A. On commence par remarquer que ectanneau est stable par conjugaison. Introduisons sur cet anneau la norme arithmétique: $N(a+ib) = a^2+b^2$. C'est une fonction multiplicative compatible avec l'inverse. Elle nous permet de calculer les inversibles.

Lemme 1. *Les inversibles de A sont $1, -1, i, -i$.*

Proof. Ces éléments sont évidemment inversibles. Reste à voir si c'est les seuls. Mais si z est inversible, alors $N(zz^{-1}) = N(z)N(z)^{-1} = 1$ donc N(z) est un inversible de $\mathbb{Z}$, ie $N(z) = 1$ (car $N \geqslant 0$). donc $a^2+b^2 = 1$ avec a et b entier ce qui implique bien évidemment ($a = 0$ et $b = 1, -1$) ou ($b = 0$, $a = 1, -1$) □

Lemme 2. *On pose Σ l'ensemble des entiers somme de deux carrés. Alors $n \in \Sigma \Leftrightarrow n = N(z), z \in A$ et Σ est stable par produit.*

Proof. La première équivalance est claire. La norme appartient toujours à Σ, et inversement si $n = a^2+b^2$, alors $z = a+ib$ convient. Si $n' \in \Sigma$, alors $n' = N(z')$ et donc $nn' = N(z)N(z') = N(zz')$ et donc $nn' \in \Sigma$ en vertu de l'équivalence. □

Ceci nous permet de nous ramener à l'étude des p premiers qui appartiennent à *Sigma*.

Lemme 3. *A est euclidien pour le stathme N.*

Proof. C'est évident. On pose $z/z' = x = u+iv$ avec $u \in Q$ et $v \in Q$. On pose s et t les entiers les plus proches de u et v,ainsi que $q = s+it$. Alors $q \in A$ et $N(x-q) = (s-t)^2+(t-u)^2 \leqslant 1/4+1/4 < 1$, donc $N(z-qz') < N(z)$ par multiplicativité de N et donc on a bien ce qu'on veut. □

Lemme 4. *p premier est dans Σ ssi $p = 2$ ou p est pas congru à 1 modulo 4.*

Proof. Condition nécessaire: si $p = a^2+b^2$, alors dans tous les cas, on a a^2 et b^2 qui sont congrus à 0 ou 1 modulo 4 donc leur somme est congrue à 0,1,2 modulo 4. Donc soit $p = 2$ soit (comme p est impair) il est congru à 1 modulo 4. Inversément, on démontre d'abord que $p \in \Sigma$ ssi p n'est pas irréductible dans $Z[i]$. Le sens direct est encore une fois évident: $p = (a+ib)(a-ib)$ et les deux éléments sont non inversibles. Pour le sens réciproque, si $p = zz'$, alors on a $N(p) = p^2 = N(z)N(z')$. Donc comme les éléments inversibles sont les éléments de norme 1, on a $p = N(z)$ et $p = N(z')$, et ainsi $p \in \Sigma$. A partir de là, l'anneau A étant principal, p est non irréductible équivaut à dire que (p) est non premier, ce qui équivaut à dire que $A/(p)$ est non intègre. Mais $A \simeq Z[X]/(X^2+1)$, docn en utilisant le morphisme $f : a+ib \mapsto a+bX+(X^2+1,p)$, on voit que $A/(p) \simeq Z[X]/(X^2+1,p)$, puis en utilisant $P[p] \in Z_p[X] \mapsto P+(X^2+1,p)$ on a finalement $A/(p) \simeq Z_p[X]/(X^2+1)$. Donc ce quotient est non intègre ssi ce n'est pas un corps (on rappelle que les quotients des anneaux principaux sont soit des corps soit non intègres) ssi X^2+1 n'est pas irréductible sur Z_p ssi il a une racine dans Z_p ssi -1 est un carré dans F_p, et on sait que ceci est vérifié ssi $p \equiv 1[4]$ ou $p = 2$. □

On en déduit Σ en entier. Un élément est dans Σ ssi les $v_p(a)$ avec $p \equiv 3[4]$ sont paires. En effet, la condition est suffisante car un carré est toujours dans Σ, et qu'on a la stabilité par produit. Elle est nécessaire. En effet, soit $p \equiv 3[4]$. Montrons par récurrence que $V_p(n)$ pair. Si elle vaut 0 c'est pair. Sinon, p divise $n = a^2+b^2$ mais comme p est irréductible dans A, ceci implique que p divise $a+ib$ ou $a-ib$. Mais dans les deux cas, p étant entier, ceci implique que p divise a et p divise b. $a = pa'$ et $b = pb'$. Donc p^2 divise a^2+b^2, ie p^2 divise n. On a alors $n = p^2(a'^2+b'^2)$ et n/p^2 reste un carré, ceci implique $v_p(n/p^2)$ pair par hypothèse de récurrence, c'est donc aussi le cas de $v_p(n) = v_p(N/p^2)+2$.