(1)

Sur le théorème des deux carrés.

On va ici donner une démonstration simple d'une caractérisation des entiers qui sont somme de deux carrés. Pour cela, on va étudier la structure arithmétique de $\mathbb{Z}[i]$, le point clé étant de donner la liste des irréductibles de cet anneau (une fois établie la factorialité).

Luc Abergel - Lycée Janson de Sailly - 106 Rue de la Pompe, 75116 Paris
lucabergel@cegetel.net
Site https://jds-mpstar1.e-monsite.com

1. Généralités.

On va ici rappeler quelques points simples et essentiels à la fois pour l'étude arithmétique de l'anneau des entiers de Gauss.

Définition 1. — *Anneau des entiers de Gauss.*
On note $A = \mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$ muni des lois usuelles de $\mathbb{C}$.
On note $N\ :\ A \to \mathbb{N}^*$ l'application qui à $z = a + ib$ associe $z\overline{z} = a^2 + b^2$ dont on rappelle qu'elle est multiplicative ($N(zz') = N(z)N(z')$). On dispose de plus d'une notion de divisibilité notée $d|z$ s'il existe $q \in A$ tel que $z = qd$ (pour $d \neq 0 \in A$).

Rappel 1. — *Carrés modulo p.*
Soit p premier impair. On rappelle que -1 est un carré dans l'anneau $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p = 1 \mod 4$.

Une démonstration de ce résultat est proposée en annexe.

1.1. A^*. —

Proposition 1. — *Inversibles de A.*
Le groupe A^* des inversibles de $(A, .)$ est l'ensemble des racines quatrièmes de l'unité, à savoir $\{\pm 1, \pm i\}$.

Démonstration. —

- Si $z \in A$ est inversible, alors il existe $z' \in A$ tel que $zz' = 1$ et donc $N(z)N(z') = 1$. Ainsi, $N(z) = 1$.

(1) Merci à Marc Tastet pour les corrections.

- Réciproquement, si $N(z) = 1$, alors $z\overline{z} = 1$ est $\overline{z} \in A$ est l'inverse de z.
- Dans le cas de l'anneau des entiers de Gauss, les éléments vérifiant $N(z) = 1$ sont clairement les racines quatrièmes de l'unité.

□

On dit que $z, z' \in A$ sont conjugués sous l'action de A^* s'il existe $\alpha \in A^*$ tel que $z = \alpha z'$. On note alors $z \sim z'$.

1.2. Division euclidienne. — On dispose dans A d'une division euclidienne.

Proposition 2. — *Approximation d'un élément de $\mathbb{Q}[i]$ par un élément de A.*
Soit $Z \in \mathbb{Q}[i]$. Il existe $z \in A$ (non unique) tel que $|Z - z| < 1$.

Démonstration. — Soit $Z = x + iy \in \mathbb{Q}[i]$. On choisit a et b dans $\mathbb{Z}$ tels que $[x - a| \leq 1/2$ et $|y - b| \leq 1/2$. On pose $z = a + ib \in A$ et on a alors $|Z - z| \leq 1/\sqrt{2} < 1$ comme demandé. □

Proposition 3. — *Division euclidienne.*
Soit $(z, d) \in A^2$ avec $d \neq 0$. Il existe alors $(q, r) \in A^2$ tels que $z = dq + r$ et $N(r) < N(d)$.

Démonstration. — Il suffit de poser $Z = \frac{z}{d} \in \mathbb{Q}[i]$ et de choisir $q \in A$ tel que $|Z - q| < 1$. On pose alors $r = z - qd \in A$ qui convient. □

1.3. Conséquence. — On dispose donc de la propriété de factorialité dans A, donc par exemple une notion de PGCD, et du théorème de Gauss : si $d|zz'$ et si $\mathrm{PGCD}(d, z) = 1$, alors $d|z'$.

2. Irréductibles de A.

Commençons par le cas trivial $p = 2$.

Proposition 4. — *Le cas $p = 2$.*
$2 = (1 + i)(1 - i)$ et $1 + i$ et $1 - i$ sont conjugués sous l'action de A^*.

Proposition 5. — *Le cas p premier avec $p = 3 \mod 4$.*
Si p est premier avec $p = 3 \mod 4$, alors p est irréductible dans A.

Démonstration. — Si on avait $\pi = a+ib|p$, alors on aurait $N(a+ib) = a^2+b^2|N(p) = p^2$. Mais comme on suppose π et $\frac{p}{\pi} \notin A^*$, on ne peut avoir que $N(\pi) = p$, soit $a^2 + b^2 = p$. Ainsi $a^2 + b^2 = 0 \mod p$. Si $b \neq 0 \mod p$, alors $\left(ab^{-1}\right)^2 = -1 \mod p$, ce qui est impossible par le rappel. Donc $p|b$ puis $p|a$, et $p|\pi$ ce qui est contradictoire avec l'hypothèse π diviseur non trivial de p. On remarquera que cet argument donne l'irréductibilité de $+i$. □

Proposition 6. — *Le cas p premier avec $p = 1 \mod 4$.*
Si p est premier avec $p = 1 \mod 4$, alors $p = \pi\overline{\pi}$ et π et $\overline{\pi}$ sont irréductibles non conjugués.

Démonstration. —

- Vérifions que p est réductible :
  On dispose par le rappel de $x \in \mathbb{Z}$ tel que $x^2+1 = 0 \mod p$. Donc $p|(x+i)(x-i)$. Si p était irréductible, on aurait alors par exemple $p|x+i$, soit $x+i = pq$ pour un $q \in A$. Mais alors $x-i = p\overline{q}$ et p diviserait également $x-i$, donc p diviserait leur différence, soit $p|2 = (1+i)(1-i) \sim (1+i)^2$ et finalement p diviserait $1+i$ ce qui est clairement impossible, p est donc bien réductible.
- Montrons que $p = \pi\overline{\pi}$ avec π et $\overline{\pi}$ irréductibles :
  Soit donc π un diviseur non trivial de p. On a encore $N(\pi)|N(p) = p^2$ avec $N(\pi) \neq 1, p^2$, soit $N(\pi) = p$. Si $d \in A$ divise π, alors à nouveau $N(d)|N(\pi) = p$, soit $N(d) = 1$ ou p et donc d est un diviseur trivial de π. On conclut de même quant à l'irréductibilité de $\overline{\pi}$.
- π et $\overline{\pi}$ ne sont pas conjugués :
  Si on pose $\pi = a+ib$, on a alors $\overline{\pi} = a-ib$. On vérifie que s'ils étaient conjugués, on aurait par exemple $(a-ib) = i(a+ib)$ ce qui donnerait $b = -a$ et π étant irréductible, cela imposerait $a = \pm 1$ ce qui n'est le cas que pour $p = 2$.

□

Proposition 7. — *Irréductibles de A à conjugaison près.*
Les irréductibles de A sont $1+i$, les p premiers tels que $p = 3 \mod 4$, les deux diviseurs non triviaux (non conjugués) de p premier tels que $p = 1 \mod 4$. Les autres irréductibles sont les conjugués de ceux précédemment cités.

Démonstration. — Soit z un irréductible de A et soit p un nombre premier divisant $N(z)$.

- Si $p = 3 \mod 4$, alors p et z sont irréductibles et $p|z\overline{z}$, donc par exemple $p|z$ et z et p sont conjugués.
- Si $p = 1 \mod 4$. Notons π un facteur irréductible de p. $\pi|p$ et $p|z\overline{z}$, donc par exemple $\pi|z$ et à nouveau π et z sont conjugués.

□

3. Le théorème des deux carrés.

Théorème 1. — *Entiers somme de deux carrés.*
Un entier n est somme de deux carrés si et seulement si ses facteurs premiers p tels que $p = 3 \mod 4$ ont un exposant pair.

Démonstration. — On veut décrire l'ensemble des entiers $n = N(z)$ tels que $z \in A$. Par factorialité, on écrit z comme un produit d'irréductibles.

- Il y a le facteur $1+i$ à un certain exposant α (éventuellement égal à 0) qui donne $N((1+i)^\alpha)$, soit une puissance quelconque de 2.
- Il y a les p premiers tels que $p = 3 \mod 4$ à un certain exposant α qui donne $N(p^\alpha) = p^{2\alpha}$.
- Il y a les π diviseurs de p premier tel que $p = 1 \mod 4$ à un certain exposant α qui donne $N(\pi^\alpha) = p^\alpha$, soit une puissance quelconque de p.

On obtient bien la forme recherchée. □

4. Rappel

Rédigeons ici que -1 est un carré mod p (pour p premier impair) si et seulement si $p = 1 \mod 4$.

- Si $x^2 + 1 = 0 \mod p$ avec p premier :
  Écrivons $p = 1 + 2k$. Dans $\mathbb{Z}/p\mathbb{Z}$, on a $x^2 = -1$ et par le petit théorème de Fermat $x^{2k} = 1$, soit $(-1)^k = 1 \mod p$, ce qui donne bien k pair.
- Réciproquement, soit $p = 1 + 4k$ premier.
  Tous les éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont solutions de $X^{4k} = 1$, donc de $X^{2k} = \pm 1$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif, l'équation $x^{2k} = 1$ admet au plus $2k$ solutions dans $\mathbb{Z}/p\mathbb{Z}^*$ qui est de cardinal $4k$. Il existe donc au moins un x vérifiant $x^{2k} = -1$ et -1 est bien un carré mod p.

• *E-mail :* lucabergel@cegetel.net