UPS. L3 Mathématiques Fondamentales. Algèbre. Devoire. 2009/2010

Sommes de deux carrés et entiers de Gauss. Corrigé.

Soit $Q \subset \mathbb{N}$ l'ensemble des entiers qui peuvent s'écrire comme somme de deux carrés $Q = \{a^2 + b^2 \mid a, b \in \mathbb{N}\}$.

---

1. Montrer que si $n \in Q$, alors $n \not\equiv 3 \mod 4$.

Solution. Pour tout $a \in \mathbb{Z}$, $a^2 \equiv 0$ ou $1 \mod 4$ parce que $a \equiv 0, 1, 2$ ou $-1 \mod 4$ et on a $0^2 = 0$, $(\pm 1)^2 = 1$, $2^2 = 4 \equiv 0 \mod 4$. Donc, si $n = a^2 + b^2$ alors $n \equiv 0 + 0$, $0 + 1$, $1 + 0$ ou $1 + 1 \mod 4$.

---

2. En utilisant $\mathbb{Z}[i]$, montrer que Q est stable par produit.

Solution. Soit $m = a^2 + b^2$ et $n = c^2 + d^2$. Posons $z = a + ib$, $w = c + id$, $zw = e + if$ (i.e. $e = ac - bd$ et $f = ad + bc$). Alors on a $m = z\bar{z}$ et $n = w\bar{w}$. Donc, $mn = (z\bar{z})(w\bar{w}) = (zw)(\overline{zw}) = e^2 + f^2 = (ac - bd)^2 + (ad + bc)^2$.

Par conséquent, on va essayer de répondre à la question : *Quels sont les nombres premiers qui s'écrivent comme somme de deux carrés ?* On a vu que si p est une somme de deux carrés, alors $p \not\equiv 3 \mod 4$, i.e. $p = 2$, ou $p \equiv 1 \mod 4$. On va démontrer la réciproque. Le chemin sera détourné, et fera de jolis détours par l'algèbre que vous venez d'apprendre.

Rappel : $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme $d(a + bi) = a^2 + b^2$. Tout élément de $\mathbb{Z}[i]$ a donc une décomposition unique en produit de facteurs premiers dans $\mathbb{Z}[i]$. Mais attention, un nombre $p \in \mathbb{Z}$ qui est premier dans $\mathbb{Z}$ (5 par exemple) peut ne pas être premier dans $\mathbb{Z}[i]$ ($5 = (1 + 2i)(1 - 2i)$).

---

3. Montrer par contre que si $p \in \mathbb{Z}$ est premier dans $\mathbb{Z}[i]$, alors p est premier dans $\mathbb{Z}$.

Solution. Supposons que p n'est pas premier dans $\mathbb{Z}$. Alors $p = nm$ où $m > 1$ et $n > 1$. On a bien $m = m + 0i \in \mathbb{Z}[i]$ et $n = n + 0i \in \mathbb{Z}[i]$. Montrons que m n'est pas inversible dans $\mathbb{Z}[i]$ (pareil pour n). Supposons qu'il existe $x \in \mathbb{Z}[i]$ tel que $mx = 1$ alors $|x| = 1/|m| < 1$ ce qui n'est pas possible.

---

4. Soit p un nombre premier de $\mathbb{Z}$. Montrer que si p n'est pas irreductible dans $\mathbb{Z}[i]$, alors p s'écrit $p = \pi\overline{\pi}$ avec π irréductible dans $\mathbb{Z}[i]$. *Indication :* soit π un facteur premier de p dans $\mathbb{Z}[i]$, et montrer que $\pi\overline{\pi}$ divise p. En déduire l'équivalence :
(i) p est une somme de deux carrés
(ii) p n'est pas premier dans $\mathbb{Z}[i]$

Solution. Supposons que p n'est pas irreductible dans $\mathbb{Z}[i]$. Alors il existe un facteur premier π de p dans $\mathbb{Z}[i]$ tel que $|\pi| > 1$, donc il existe $z \in \mathbb{Z}[i]$ tel que $p = z\pi = \bar{z}\bar{\pi}$, donc $\bar{\pi}$ aussi divise p. Or, $\bar{\pi}$ est premier (si $\pi = xy$ alors $\bar{\pi} = \bar{x}\bar{y}$), ce qui implique que $\pi\bar{\pi}$ divise p. Alors $\pi\bar{\pi} = p$ parce que p est premier, $\pi\bar{\pi} \in \mathbb{Z}$, $\pi\bar{\pi} = |\pi|^2 > 1$ et $\pi\bar{\pi}$ divise p.

Montrons que (i) $\Longleftrightarrow$ (ii).

(i) $\Longrightarrow$ (ii). Si $p = a^2+b^2$ alors $p = \pi\bar{\pi}$ pour $\pi = a+ib$. Or, si π est inversible alors $|\pi| = 1$ ce qui implique que $|\bar{\pi}| = 1$ et $p = |\pi\bar{\pi}| = 1$.

(ii) $\Longrightarrow$ (i). Supposons que p n'est pas premier dans $\mathbb{Z}[i]$. Alors $p = \pi\bar{\pi}$ pour $\pi \in \mathbb{Z}[i]$. Soit $\pi = a + ib$. Alors $p = a^2 + b^2$.

---

5. a. Montrer que $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1)$ où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

b. En déduire que p est premier dans $\mathbb{Z}[i]$ si et seulement si $X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$.

En déduire l'équivalence
(i) p est une somme de deux carrés
(ii) p n'est pas premier dans $\mathbb{Z}[i]$
(iii) -1 est un carré dans $\mathbb{F}_p$.

Solution.

a. Définissons un homomorphisme d'anneaux $\varphi : \mathbb{Z}[i]/(p) \to \mathbb{F}_p[X]/(X^2+1)$. Soit z un élément de $\mathbb{Z}[i]/(p)$ représenté par $a + ib$. Alors on définit $\varphi(z)$ comme $a + bX$ oú a et b sont considérés comme éléments de $\mathbb{F}_p$.

Montrons que φ est bien défini. Si $a'+ib'$ est un autre représentant de z, alors $(a-a')+i(b-b') \in (p)$, i.e. $a'+ib' = a+ib+(c+id)p = (a+cp)+i(b+dp)$. Donc, $a' + b'X = (a + cp) + (b + dp)X = a + bX$ (parce que $a = a + cp$ et $b = b + dp$ en tant qu'éléments de $\mathbb{F}_p$).

Montrons que φ est un homomorphisme d'anneaux. Pour $z = a + ib$ et

$w = c + id$, il est évident que $\varphi(z+w) = \varphi(z) + \varphi(w)$ et on a $\varphi(z)\varphi(w) = (a+bX)(c+dX) = (ac+bdX^2) + (ad+bc)X = (ac-bd) + (ad+bc)X = \varphi(ac-bd+i(ad+bc)) = \varphi(zw)$.

Montrons que $\ker\varphi = 0$. Soit z un élément de $\ker\varphi$ représenté par $a+ib$. Alors $\varphi(z) = a+bX = 0$ dans $\mathbb{F}_p[X]/(X^2+1)$, ce qui implique que $a = b = 0$ dans $\mathbb{F}_p$, i.e. $a \equiv b \equiv 0 \mod p$, donc $a + ib \in (p)$.

Montrons que $\operatorname{im}\varphi = \mathbb{F}_p[X]/(X^2+1)$. Tout élément de $\mathbb{F}_p[X]/(X^2+1)$ s'écrit sous la forme $a+bX$ où $0 \leq a, b < p$. Donc, il est égal à $\varphi(a+ib)$.

b. $\big(p$ est premier dans $\mathbb{Z}[i]\big) \iff \big(\mathbb{Z}[i]/(p)$ est un corps$\big) \iff \big(\mathbb{F}_p[X]/(X^2+1)$ est un corps$\big) \iff \big(X^2+1$ est irréductible dans $\mathbb{F}_p[X]\big)$.

L'équivalence (i) $\iff$ (ii) $\iff$ (iii) : On a (i) $\iff$ (ii) d'après l'exercice 4 et on a (ii) $\iff$ (iii) d'après l'exercice 5b.

---

6. Soit G un groupe abélien fini d'ordre n. On note m l'exposant de G - le nombre minimal tel que $g^m = 1$ pour tout $g \in G$.

Rappel : D'après le théorème de structure, G est isomorphe au produit $(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_s\mathbb{Z})$ où $m_1 | m_2 | \ldots | m_s$.

a. Montrer que m divise n et que si $m = n$, alors G est cyclique (indication : utiliser le théorème de structure).

b. Montrer que le groupe $\mathbb{F}_p^*$ est cyclique (indication : combien de racine peut avoir le polynôme $X^m - 1$?) Soit G un groupe abélien fini d'ordre n.

Solution.

a. D'après le théorème de classification, il suffit de considérer le cas où $G = (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_s\mathbb{Z})$. Alors on a $n = d_1 \ldots d_s$ et $m = d_s$. Donc $m = n$ implique $s = 1$, $d_1 = m = n$ et donc $G = \mathbb{Z}/n\mathbb{Z}$.

b. Soit m l'exposante du groupe multiplicatif du corp $\mathbb{F}_p^*$. Alors, tout élément de $\mathbb{F}_p^*$ et racine du polynôme $X^m - 1$. Or, le nombre des racines d'un polynôme ne dépasse pas le degré, donc $|\mathbb{F}_p^*| \leq m$.

D'après la question a), $m \leq |\mathbb{F}_p^*|$, donc $m = |\mathbb{F}_p^*|$ ce qui implique que le groupe $\mathbb{F}_p^*$ est cyclique.

---

7. On se demande donc pour quels nombres premier, -1 est un carré.

a. Quelle est la réponse pour $p = 3, 5, 7$?

b. On suppose p impair. Montrer que -1 est un carré dans $\mathbb{F}_p$ ssi le groupe $\mathbb{F}_p^*$ contient un élément d'ordre 4 (indication : montrer que -1 est le seul élément d'ordre 2 dans $\mathbb{F}_p^*$).

c. En utilisant le fait que $\mathbb{F}_p^*$ est un groupe *cyclique* d'ordre $p-1$, montrer que -1 est un carré mod p ssi $p = 2$ ou $p \equiv 1 \mod 4$.

En déduire l'équivalence
(i) p est une somme de deux carrés ;
(ii) p n'est pas premier dans $\mathbb{Z}[i]$;
(iii) -1 est un carré dans $\mathbb{F}_p$;
(iv) $p = 2$ ou $p \equiv 1 \mod 4$.

Solution.

a. On a $-1 = 2^2 \mod 5$, mais -1 n'est carré ni mod 3 ni mod 7. En effet, les carrés mod 3 sont : $0^2 = 0$, $(\pm 1)^2 = 1$; les carrés mod 7 sont : $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9 \equiv 2$.

b. -1 est le seul élément d'ordre 2 dans $\mathbb{F}_p^*$ parce que le polynôme $X^2 - 1$ ne peut pas avoire plus que $\deg(X^2 - 1) = 2$ racines (il a déjà ± 1 comme racines).

Supposons qu'il existe un élément x d'ordre 4. Alors x^2 est un élément d'ordre 2, donc $x^2 = -1$.

Réciproquement, supposons, qu'il existe x tel que $x^2 = -1$. Alors l'ordre de x et 4.

c. Si $p \equiv 1 \mod 4$, alors $k = (p-1)/4$ est est entier. Soit a le générateur du groupe $\mathbb{F}_p^*$. Alors $(a^{2k})^2 = a^{4k} = a^{p-1} = 1$, Or, $a^{2k} \neq 1$. Donc, $a^{2k} = -1$ parce'qu il n'y a pas d'autres éléments dont le carré est egal à 1. Donc, pour $b = a^k$, on a $b^2 = a^{2k} = -1$.

Si $p \not\equiv 1 \mod 4$ alors -1 n'est un carré mod p d'après l'exercice 1.

Cela implique l'equivalence (iii) $\iff$ (iv). Les equivalences (i) $\iff$ (ii) $\iff$ (iii) sont déjà établits dans les exercices 4 et 5.

---

8. On retourne au problème initial. Soit $n \in \mathbb{N}$. Montrer que $n \in Q$ si et seulement si, dans sa décomposition en facteurs premiers (dans $\mathbb{Z}$) $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, les puissances des facteurs premiers égaux à $3 \mod 4$ sont paires.

En déduire que $4410 = 2{\times}9{\times}5{\times}49$ est une somme de deux carrés (lesquels ?), alors que $924 = 4 \times 3 \times 7 \times 11$ ne l'est pas.

Solution. On note $P_\pm$ l'ensemble de nombres premiers p tels que $p \equiv \pm 1 \mod 4$.

1) ("seulement si"). Soit $n \in Q$. Alors $n = z\bar{z}$ pour $z \in \mathbb{Z}[i]$. Soit $z = p_1^{\alpha_1} \dots p_k^{\alpha_k} \pi_1^{\beta_1} \dots \pi_l^{\beta_l}$ la décomposition de n en facteurs premiers dans $\mathbb{Z}[i]$ où $p_1, \dots, p_k \in \mathbb{Z}$ et $\pi_1, \dots, \pi_l \notin \mathbb{Z}$. Soit $q_j = \pi_j \bar{\pi}_j$. Alors $p_1, \dots, p_k \in P_-$ et $q_1, \dots, q_l \in P_+ \cup \{2\}$ (d'après l'équivalence (ii)⇔(iv) dans l'exercice 5). La décomposition de n en facteurs premiers (dans $\mathbb{Z}$) est $n = z\bar{z} = p_1^{2\alpha_1} \dots p_k^{2\alpha_k} q_1^{\beta_1} \dots q_l^{\beta_l}$. On voit bien que tous les éléments de P_- y entre en puissences paires.

2) ("si"). Soit $n = p_1^{2\alpha_1} \dots p_k^{2\alpha_k} q_1^{\beta_1} \dots q_l^{\beta_l}$. Alors tout q_j se dćompose comme $q_j = \pi_j \bar{\pi}_j$, $\pi_j \in \mathbb{Z}[i]$. Donc, $n = z\bar{z}$ pour $z = p_1^{\alpha_1} \dots p_k^{\alpha_k} \pi_1^{\beta_1} \dots \pi_l^{\beta_l}$. Donc, $n \in Q$.

On a $4410 = 2 \times 9 \times 5 \times 49 = (1+i)(1-i) \times 3^2 \times (2+i)(2-i) \times 7^2 = \big(3{\times}7{\times}(1{+}i)(2{+}i)\big)\big(3{\times}7{\times}(1{-}i)(2{-}i)\big) = \big(21{\times}(1{+}3i)\big)\big(21{\times}(1{-}3i)\big) = (21+63i)(21-63i) = 21^2 + 63^2$. alors que $924 = 4 \times 3 \times 7 \times 11 \notin Q$ parce que 3 et 7 y entrent un puissances impairs.