Algèbre Générale 1, L3 - Maths
Corrigé du TD 3

Fernanda Costa Jr

Exo.1.1 a) Si $x \in \mathbb{Z}$, puisque $m \wedge n = 1$, il existe $k, s \in \mathbb{Z}$ tels que (Bézout)

$$mk + ns = 1 \Rightarrow x = mkx + nsx \in n\mathbb{Z} + m\mathbb{Z}.$$

Donc $\mathbb{Z} \subset n\mathbb{Z} + m\mathbb{Z}$, càd, $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$.

Si $x \in n\mathbb{Z} \cap m\mathbb{Z}$, alors x est multiple commun de m et n. Puisque $m \wedge n = 1$, le plus petit commun multiple de m et n est $m \cdot n$. Donc x est multiple de mn, càd, $x \in mn\mathbb{Z}$. Si $x \in mn\mathbb{Z}$, alors $x \in m\mathbb{Z}$ et $x \in n\mathbb{Z}$, donc $x \in n\mathbb{Z} \cap m\mathbb{Z}$. Par conséquent, $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$.

b) On note que

$$[x]_{mn} = [y]_{mn} \Rightarrow x - y \in mn\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$$
$$\Rightarrow x - y \in m\mathbb{Z} \text{ et } x - y \in n\mathbb{Z}$$
$$\Rightarrow [x]_m = [y]_m \text{ et } [x]_n = [x]_n. \quad (\star)$$

Par conséquent, l'application

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$[x]_{mn} \longmapsto ([x]_n, [x]_m)$$

est bien définie. En effet, $(\star)$ montre que $\Phi([x]_{mn})$ ne dépend pas du représentant $x \in \mathbb{Z}$. Les opérations des classe d'équivalence coordonnée-par-coordonnée impliquent que Φ est un morphisme d'anneaux. Devoir : détailler.

c) Soit $[x]_{mn} \in \ker \Phi$. Alors $\Phi([x]_{mn}) = ([x]_n, [x]_m) = (0,0)$ donc $x \in n\mathbb{Z} \cap m\mathbb{Z} = mn\mathbb{Z}$, d'où $[x]_{mn} = 0$. Cela montre que Φ est injective. Puisque les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ont tous les deux mn éléments, Φ est aussi surjective. Par conséquent, Φ est un isomorphisme.

d) Étant donnés $a, b \in \mathbb{Z}$, puisque Φ est surjectif, il existe $x \in \mathbb{Z}$ tel que

$$([x]_n, [x]_m) = \Phi([x]_{mn}) = ([a]_n, [b]_m)$$

$$\Rightarrow \begin{cases} x = a\,[n] \\ x = b\,[m] \end{cases} \qquad (\star)$$

Si x et y sont deux solutions de $(\star)$, alors

$$\Phi([x]_{mn}) = \Phi([y]_{mn})$$

Par injectivité on trouve $[x]_{mn} = [y]_{mn}$, c'à d, $x - y \in mn\mathbb{Z}$.

e) Par essai-erreur on trouve

$$(-3)\cdot 21 + (8)\cdot 8 = 1.$$

$$\begin{cases} x \equiv 5\,[21] \\ x \equiv 9\,[8] \end{cases}$$

Donc $x_0 = 9\cdot(-3)\cdot 21 + 5\cdot 8\cdot 8$ est une solution. En effet :

$8\cdot 8 = \underbrace{1 - (-3\cdot 21)}_{\equiv 1\,[21]} \Rightarrow x_0 = 9\cdot \underbrace{(-3\cdot 21)}_{\equiv 0\,[21]} + 5\cdot \underbrace{(8\cdot 8)}_{\equiv 1\,[21]} \equiv 1\,[21]$

$(-3\cdot 21) = \underbrace{1 - 8\cdot 8}_{\equiv 1\,[8]} \Rightarrow x_0 = 9\cdot \underbrace{(-3\cdot 21)}_{\equiv 1\,[8]} + 5\cdot \underbrace{(8\cdot 8)}_{\equiv 0\,[8]} \equiv 9\,[8]$.

Si l'on calcule, on trouve

$$x_0 = -247.$$

D'après (d), les solutions sont

$$x = x_0 + 21 \cdot 8 \cdot k, \quad k \in \mathbb{Z}$$

$$\Rightarrow S = \{-247 + 168k : k \in \mathbb{Z}\}$$

ou $S = \{-79 + 168k : k \in \mathbb{Z}\}$

$-247 + 168 \cdot 1 = -79$

Exo 1.2 ② Pour commencer, on note que

$$[x]_\rho = [y]_\rho \Rightarrow x - y = \rho k, \ k \in \mathbb{Z}$$
$$\Rightarrow x - y = n_i k', \ k' \in \mathbb{Z}, \ i = 1, \dots, p$$
$$\Rightarrow [x]_{n_i} = [y]_{n_i}, \ i = 1, \dots, p$$

Donc

$$\Phi : \mathbb{Z}/\rho\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_p\mathbb{Z}$$
$$[x]_\rho \longmapsto ([x]_{n_1}, \dots, [x]_{n_p})$$

est bien défini. C'est clairement un morphisme. Soient $x, y \in \mathbb{Z}$ tels que

$$\Phi([x]_\rho) = \Phi([y]_\rho) \Rightarrow ([x]_{n_1}, \dots, [x]_{n_p}) = ([y]_{n_1}, \dots, [y]_{n_p})$$
$$\Rightarrow [x]_{n_i} = [y]_{n_i}, \ \forall i = 1, \dots, p$$
$$\Rightarrow x - y \in n_i\mathbb{Z}, \ \forall i = 1, \dots, p$$
$$\Rightarrow x - y \text{ multiple commun de } n_1, \dots, n_p$$
$$\Rightarrow x - y \text{ multiple de } n_1 \vee n_2 \vee \cdots \vee n_p = \rho$$
$$\Rightarrow x - y \in \rho\mathbb{Z}$$
$$\Rightarrow [x]_\rho = [y]_\rho.$$

Alors Φ est injectif. Puisque $\mathbb{Z}/e\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_p\mathbb{Z}$ ont le même nombre d'éléments ($e = \prod n_i$), Φ est aussi surjectif. Par conséquent, Φ est isomorphisme.

(b)

$$(\star) \begin{cases} x \equiv 8 \ [21] \\ x \equiv 6 \ [8] \\ x \equiv 2 \ [5] \end{cases}.$$

On résout d'abord

$$(\star') \begin{cases} x \equiv 8 \ [21] \\ x \equiv 6 \ [8]. \end{cases}$$

On cherche x tel que

$$x - 8 = 21p \quad \text{et} \quad x - 6 = 8q$$

pour certains $p, q \in \mathbb{Z}$. Alors

$$8 + 21p = x = 6 + 8q \Rightarrow 21p - 8q = -2.$$

Pour $p = -2$ et $q = -5$ on a bien une solution

$$x = 6 + 8(-5) = -34.$$

Toutes les solutions de $(\star')$ sont donc

$$x = -34 + 21 \cdot 8k = -34 + 168k, \ k \in \mathbb{Z}.$$

Soit, en notation de congruence,

$$x \equiv -34 \ [168]$$

Pour résoudre $(\star)$ on doit donc résoudre

$$\begin{cases} x \equiv -34 \ [168] \\ x \equiv 2 \ [5]. \end{cases}$$

On cherche encore une fois, des entiers x, p, q tel que

$$x = -34 + 168p = 2 + 59$$
$$\Rightarrow 168p - 59 = 36.$$

Une solution est $p = 72$ et $q = 2412$. Donc

$$x = -34 + 168p = 12062.$$

$$168 = 33 \times 5 + 3$$
$$5 = 1 \times 3 + 2$$
$$3 = 1 \times 2 + 1$$

$$1 = 3 - 1 \times 2$$
$$= 3 - 1 \times (5 - 1 \times 3)$$
$$= 2 \times 3 - 1 \times 5$$
$$= 2 \times (168 - 33 \times 5) - 1 \times 5$$
$$= 2 \times 168 - 66 \times 5 - 1 \times 5$$
$$\Rightarrow 1 = 2 \times 168 - 67 \times 5$$

$$\xrightarrow{\times 36} 36 = 36 \times 2 \times 168 - 36 \times 67 \times 5$$
$$\Rightarrow \underbrace{72}_{p} \times 168 - \underbrace{2412}_{q} \times 5 = 36$$

Les solutions ont donc la forme

$$x = 12062 + 168 \cdot 5k, \quad k \in \mathbb{Z}$$
$$\Rightarrow x = 12062 + 840k, \quad k \in \mathbb{Z}.$$
$$\Rightarrow x = 302 + 14 \times 840 + 840k, \quad k \in \mathbb{Z}$$
$$\Rightarrow x = 302 + 840(14 + k), \quad k \in \mathbb{Z}$$
$$\Rightarrow S_{(*)} = \{302 + 840k ; k \in \mathbb{Z}\}.$$

Exo. 2 a) D'après la division euclidienne, $(\mathbb{Z}, +, \times)$ est un anneau euclidien pour le stathme euclidien $d = Id_{\mathbb{Z}}$.

D'après la division polynomiale, $(\mathbb{K}[X], +, \times)$ est un anneau pour le stathme euclidien

$$d : \mathbb{K}[X]^* \longrightarrow \mathbb{N}$$
$$P \longmapsto \deg(P).$$

b) Soit $(A, +, \times)$ euclidien avec stathme d. Étant donné I idéal de A, on montre que I est principal.

Le cas $I = \{0\}$ est trivial. On suppose $I \neq \{0\}$ et on note que

$$\{ d(a) : a \in I \setminus \{0\} \} \subset \mathbb{N}$$

admet un plus petit élément (Principe du bon ordre). Soit $b \in I$ où $d(b) = \min \{ d(a) : a \in I \setminus \{0\} \}$.

Affirmation : $I = bA$.

L'inclusion $bA \subset I$ vient de la définition d'idéal. Soit $a \in I$. On veut montrer que $a \in bA$. Par définition d'anneau euclidien, il existe $q, r \in A$ tels que

$$\begin{cases} a = bq + r \\ r = 0 \quad \text{ou} \quad d(r) < d(b). \end{cases}$$

Alors $r = a - bq \in I$ et, puisque $d(r) < d(b) = \min \{ d(a) : a \in I \setminus \{0\} \}$ est impossible, on trouve que $r = 0$, d'où $a = bq \in bA$.

Cela montre que I est principal. Par conséquent, A est anneau principal

(c) Soient $a, b \in \mathbb{Z}[i] \times \mathbb{Z}[i] \setminus \{0\}$. On cherche des éléments $q, r \in \mathbb{Z}[i]$ tels que

$$\begin{cases} a = bq + r, \\ r = 0 \quad \text{ou} \quad d(r) < d(b). \end{cases}$$

On pose $a = a_1 + ia_2$, $b = b_1 + ib_2$.

Alors,

$$\frac{a}{b} = \frac{a_1+ia_2}{b_1+ib_2} = \frac{(a_1+ia_2)(b_1-ib_2)}{(b_1+ib_2)(b_1-ib_2)} = \frac{(a_1b_1+a_2b_2)+i(a_2b_1-a_1b_2)}{b_1^2+b_2^2}$$

$$= \frac{a_1b_1+a_2b_2}{b_1^2+b_2^2} + i\,\frac{a_2b_1-a_1b_2}{b_1^2+b_2^2} \in \mathbb{Q}[i].$$

$$= x + iy, \text{ où } \begin{cases} x = \dfrac{a_1b_1+a_2b_2}{b_1^2+b_2^2} \in \mathbb{Q}, \\ y = \dfrac{a_2b_1-a_1b_2}{b_1^2+b_2^2} \in \mathbb{Q}. \end{cases}$$

On note que $[x-\frac{1}{2}, x+\frac{1}{2}]$ et $[y-\frac{1}{2}, y+\frac{1}{2}]$ sont des intervales de taille 1, alors on peut trouver deux entiers $m \in [x-\frac{1}{2}, x+\frac{1}{2}] \cap \mathbb{Z}$ et $n \in [y-\frac{1}{2}, y+\frac{1}{2}] \cap \mathbb{Z}$. On pose

$$\alpha = x - m \qquad \text{et} \qquad \beta = y - n.$$

On trouve

- $|\alpha| \leq \frac{1}{2} \Rightarrow \alpha^2 \leq \frac{1}{4}$ (1)
- $|\beta| \leq \frac{1}{2} \Rightarrow \beta^2 \leq \frac{1}{4}$ (2)
- $x = \alpha + m$ et $y = \beta + n$. (3)

On voit que

$$\frac{a}{b} = x + iy \overset{(3)}{=} (\alpha+m) + i(\beta+n) = (m+in) + (\alpha+i\beta) \Longrightarrow$$

$$\Rightarrow a = b(m+in) + b(\alpha+i\beta) = bq + r, \qquad (4)$$

où

$$q = m+in \in \mathbb{Z}[i]$$
$$r = b(\alpha+i\beta) \in \mathbb{Z}[i]$$

(Le fait que $r \in \mathbb{Z}[i]$ vient de (4) : $r = a - bq \in \mathbb{Z}[i]$).

Il reste montrer que $d(r) < d(b)$ lorsque $r \neq 0$. On suppose donc $r \neq 0$. Alors

$$d(r) = d(b(\alpha+i\beta)) = d((b_1+ib_2)(\alpha+i\beta)) = d((b_1\alpha - b_2\beta) - i(b_2\beta + b_2\alpha))$$

$$= (b_1\alpha - b_2\beta)^2 + (b_1\beta + b_2\alpha)^2 = b_1^2\alpha^2 - 2b_1b_2\alpha\beta + b_2^2\beta^2 + b_1^2\beta^2 + 2b_1b_2\alpha\beta + b_2^2\alpha^2$$

$$= b_1^2\alpha^2 + b_2^2\alpha^2 + b_2^2\beta^2 + b_1^2\beta^2 = (b_1^2+b_2^2)(\alpha^2+\beta^2)$$

$$\overset{(1),(2)}{\leq} (b_1^2+b_2^2)\left(\frac{1}{4}+\frac{1}{4}\right) = (b_1^2+b_2^2)\cdot\frac{1}{2} < b_1^2+b_2^2 = d(b),$$

ce qu'il fallait démontrer.

Exo. 3 ⇒ On divise

$$(X+1)^2 = X^2 + 2X + 1$$

par

$$(X-1)^2 = X^2 - 2X + 1.$$

On trouve

$$\begin{array}{r|l} X^2+2X+1 & X^2-2X+1 \\ \hline -(X^2-2X+1) & 1 \\ \hline 0+4X+0 & \end{array} \Rightarrow (X+1)^2 = 1\times(X-1)^2 + 4X.$$

On divise X^2-2X+1 par $4X$. On trouve

$$\begin{array}{r|l} X^2-2X+1 & 4X \\ \hline -(X^2) & \frac{1}{4}X - \frac{1}{2} \\ \hline 0-2X+1 & \\ -(-2X) & \\ \hline 0+1 & \end{array} \Rightarrow (X-1)^2 = \left(\frac{1}{4}X - \frac{1}{2}\right)4X + 1$$

Alors,

$$\begin{aligned} 1 &= (X-1)^2 - \left(\frac{1}{4}X - \frac{1}{2}\right)4X \\ &= (X-1)^2 - \left(\frac{1}{4}X - \frac{1}{2}\right)\left((X+1)^2 - (X-1)^2\right) \\ &= (X-1)^2 - \left(\frac{1}{4}X - \frac{1}{2}\right)(X+1)^2 + \left(\frac{1}{4}X - \frac{1}{2}\right)(X-1)^2 \end{aligned}$$

$$\Rightarrow 1 = \left(\frac{1}{4}X + \frac{1}{2}\right)(X-1)^2 - \left(\frac{1}{4}X - \frac{1}{2}\right)(X+1)^2.$$

Donc il suffit de prendre

$$U(X) = 2\left(\frac{1}{4}X + \frac{1}{2}\right) = \frac{1}{2}X + 1$$

et

$$V(X) = 2\left(\frac{1}{4}X - \frac{1}{2}\right) = \frac{1}{2}X - 1.$$

b) De a) on obtient

$$U(X)(X-1)^2 + V(X)(X+1)^2 = 2 \Rightarrow$$

$$\Rightarrow U(X)(X-1)^2 - 1 = -V(X)(X+1)^2 + 1$$

On considère

$$P_0(X) = U(X)(X-1)^2 - 1 = -V(X)(X+1)^2 + 1.$$

Alors

$$U(X)(X-1)^2 = P_0(X) + 1 \Rightarrow (X-1)^2 \mid P_0(X) + 1$$

et

$$-V(X)(X+1)^2 = P_0(X) - 1 \Rightarrow (X+1)^2 \mid P_0(X) - 1.$$

c) On suppose P est une autre solution de (E). Alors

$$(X-1)^2 \mid P_0(X) + 1 \quad \text{et} \quad (X-1)^2 \mid P(X) + 1 \Rightarrow$$

$$\Rightarrow (X-1)^2 \mid (P_0(X)+1) - (P(X)+1) \Rightarrow$$

$$\Rightarrow (X-1)^2 \mid P(X) - P_0(X).$$

Donc 1 est une racine d'ordre au moins 2 de $P - P_0$. Simi

lairement, -1 est une racine d'ordre au moins 2 de $P - P_0$. Par conséquent,

$$P(X) - P_0(X) = Q(X)(X-1)^2(X+1)^2$$

pour un certain polynôme $Q \in \mathbb{R}[X]$, c'est-à-dire, $P - P_0$ est multiple de $(X-1)^2(X+1)^2$. Clairement la réciproque est vraie, càd, si $P - P_0$ est multiple de $(X-1)^2(X+1)^2$, alors P est solution de (E). En conclusion, les solutions de (E) sont de la forme

$$P = P_0 + Q(X-1)^2(X+1)^2, \quad Q \in \mathbb{R}[X].$$

Exo. 4

a) Devoir.

b) On voit que, pour $z = 2 + i\sqrt{5}$ on a

$$z \cdot \bar{z} = N(z) = 9 = 3 \cdot 3, \quad z \neq \pm 3.$$

Donc $3 \mid z \cdot \bar{z}$ mais $3 \nmid z$ ni $3 \nmid \bar{z}$, càd, 3 n'est pas premier.

À démontrer !

$3 \nmid z \Rightarrow z = 3(a + ib\sqrt{5}) = 3a + 3b\sqrt{5}$,
$a, b \in \mathbb{Z} \Rightarrow \begin{cases} 2 = 3a \\ 1 = 3b \end{cases}$ impossible

c) On suppose $3 = xy$, $x, y \in \mathbb{Z}[i\sqrt{5}]$. Alors

$$3 \cdot 3 = |3|^2 = |xy|^2 = |x|^2 |y|^2, \text{ avec } |x|^2, |y|^2 \in \mathbb{N}.$$

Par unicité de la décomposition en facteurs premiers sur $\mathbb{Z}$, on a trois possibilités :

(1) $|x|^2 = 1$ et $|y|^2 = 9 \Rightarrow |x| = 1 \Rightarrow x$ unité

(2) $|x|^2 = 9$ et $|y|^2 = 1 \Rightarrow y$ unité

(3) $|x|^2 = 3$ et $|y|^2 = 3$.

Les conclusions (1) et (2) sont souhaitées. On veut montrer que (3) est impossible. En effet, si $x = a+ib$ et $|x|^2 = 3$, alors

$$|x|^2 = a^2 + 5b^2 = 3 \Rightarrow b = 0 \quad (\text{sinon } a^2+5b^2 > 3)$$
$$\Rightarrow a^2 = 3 \quad \text{absurde car } b \text{ est premier dans } \mathbb{Z}.$$

Cela montre que 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$, CQFD.

d) Non car 3 est irréductible mais pas premier.

Exo. 5 a) Soit $z \in \mathbb{Z}[i]$ tel que $N(z) = z\cdot\bar{z}$ est premier. On considère $x, y \in \mathbb{Z}[i]$ tels que $z = xy$. On veut montrer que soit x est unité de $\mathbb{Z}[i]$ soit y l'est. On calcule

$$N(z) = N(xy) = N(x)\cdot N(y). \in \mathbb{N}$$

Puisque $N(z)$ est premier dans $\mathbb{N}$, on a $N(x) = 1$ ou $N(y) = 1$.

Les seuls éléments de $\mathbb{Z}[i]$ dont la norme est 1 sont $1, -1, i$ et $-i$, soit les unités de $\mathbb{Z}[i]$ (voir Exo. 9(b)-TD2).

Par conséquent, z est irreductible, CQFD.

b) $\underline{z = 7}$. On affirme que 7 est désormais irreductible.

On suppose $7 = xy$. Alors

$$49 = 7^2 = N(7) = N(xy) = N(x)N(y).$$

Comme pour l'exo précedent (4.(c)), on veut montrer que

le cas $N(x) = N(y) = 7$ est impossible. On pose $x = a+ib$. Alors, si $N(x) = 7$, on trouve

$$a^2 + b^2 = N(x) = 7.$$

Mais ceci est impossible car pour tout entier n, soit $n^2 \equiv 1\,[4]$ soit $n^2 \equiv 0\,[4]$, et donc la somme de deux carrés ne peut jamais être $\equiv 3\,[4]$, ce qui est le cas de $z = 7 \equiv 3\,[4]$. Cela montre que 7 est irréductible.

$\underline{z = 13}$. Comme pour $z = 7$, on regarde si $N(x) = 13$.

Maintenant oui : si $x = a+ib$,

$$a^2 + b^2 = N(x) = 13 \quad \text{si} \quad a = 2 \text{ et } b = 3.$$

Par conséquent,

$$13 = (2+3i)(2-3i),$$

où $2+3i$ et $2-3i$ sont irréductibles car

$$N(2+3i) = N(2-3i) = 13 \text{ premier dans } \mathbb{N}.$$

$\underline{z = 2(3+i)}$. On calcule

$$N(2(3+i)) = N(6+2i) = 36+4 = 40 = 2^3 \cdot 5.$$

On connaît les factorisations $2 = (1+i)(1-i)$ et $5 = (2+i)(2-i)$.

On voit que, parmi ces facteurs, $2-i$ divise $3+i$.

En effet, si on cherche $a+ib$ tel que $3+i = (2-i)(a+ib)$ on obtient $3+i = (2a+b) + i(2b-a)$ et donc

$$\left.\begin{cases} 2b-a = 1 \Rightarrow a = 2b-1 \\ 2a+b = 3 \Rightarrow 2(2b-1)+b = 3 \Rightarrow b = 1 \Rightarrow a = 1 \end{cases}\right\} a+ib = 1+i$$

Donc $2(3+i) = (1+i)^2(1-i)(2-i)$, ce qui est la factorisation cherchée.

$z = 12+i$. On calcule

$$N(z) = 12^2+1 = 145 = 5\cdot 29 = \underbrace{(2+i)(2-i)(5+2i)(5-2i)}_{\text{irréductibles.}}$$

Les facteurs de $12+i$ appartiennent à $\{2+i, 2-i, 5+2i, 5-2i\}$.

On voit que $2+i$ divise $12+i$. En effet

$$12+i = (2+i)(a+ib) \Rightarrow \begin{cases} 2a-b = 12 \\ 2b+a = 1 \end{cases} \Rightarrow a=5,\ b=-2.$$

Donc

irréductibles car $N(2+i)$ et $N(5-2i)$ sont des nombres premiers

$$12+i = (2+i)(5-2i)$$

est la décomposition de $12+i$ en facteurs premiers.

(c) On factorise $11+7i$. On a

$$N(11+7i) = 121+49 = 170 = 17\times 2\times 5.$$

Afin de factoriser 17, on cherche a, b tel que $a^2+b^2=17$.
On trouve $a=4$ et $b=1$, d'où $17 = (4+i)(4-i)$ et donc

$$N(11+7i) = 17\cdot 2\cdot 5 = (4+i)(4-i)(1+i)(1-i)(2+i)(2-i).$$

Les facteurs irréductibles de $11+7i$ appartiennent à l'ensemble $\{4+i, 4-i, 1+i, 1-i, 2+i, 2-i\}$. On voit que $4+i$ divise $11+7i$:

$$11+7i = (4+i)(a+ib) \Rightarrow \begin{cases} 4a-b = 11 \\ 4b+a = 7 \end{cases} \Rightarrow a+ib = 3+i.$$

On sait que $3+i = (2-i)(1+i)$ (voir partie b). Donc la factorisation de $11+7i$ est

$$11+7i = (4+i)(2-i)(1+i). \qquad (1)$$

Maintenant, on factorise $3+7i$. On calcule

$$N(3+7i) = 9+49 = 58 = 2\cdot 29 = (1+i)(1-i)(5+2i)(5-2i).$$

On voit que

$$3+7i = (1+i)(5+2i) \qquad (2)$$

est la factorisation de $3+7i$ en facteurs irréductibles. De (1) et (2) on voit que le pgcd de $11+7i$ et $3+7i$ (à une unité près) est $1+i$, CQFD.

Deuxième méthode de solution: division euclidienne

D'abord, il faut lire et comprendre l'Exercice 2(c).

On calcule

$$\frac{11+7i}{3+7i} = \frac{(11+7i)(3-7i)}{(3+7i)(3-7i)} = \frac{33+49+(-77+21)i}{9+49}$$

$$= \frac{82-56i}{58} = \frac{41}{29} - \frac{28}{29}i.$$

L'entier gaussien le plus proche de $\frac{41}{29} - \frac{28}{29}i$ est

$$q = 1-i. \quad \text{(candidat à quotient)}$$

En effet, $\frac{41}{29} \simeq 1,4137\ldots$ est proche de 1,

$\frac{-28}{29} \simeq -0,9655\ldots$ est proche de -1.

On calcule le reste pour le quotient q:

$$11+7i = q(3+7i)+r = (1-i)(3+7i)+r_1$$

$$\Rightarrow 11+7i = (3+7)+(7-3)i+r$$

$$\Rightarrow 11+7i = 10+4i+r \Rightarrow \boxed{r = 1+3i}$$

On a, donc,

$$11+7i = (1-i)(3+7i)+(1+3i).$$

On divise le dividende $3+7i$ par le reste $1+3i$. On a

$$\frac{3+7i}{1+3i} = \frac{(3+7i)(1-3i)}{(1+3i)(1-3i)} = \frac{(3+21)+i(-9+7)}{1+9} = \frac{24}{10} - \frac{2}{10}i$$

$$= \frac{12}{5} - \frac{1}{5}i \sim 2-0i$$

L'intier gaussien le plus proche est $q = 2-0i = 2$.

On calcule

$$3+7i = 2(1+3i)+r \Rightarrow r = 1+i.$$

$$\Rightarrow 3+7i = 2(1+3i)+(1+i).$$

Finalement, on divise $1+3i$ par $1+i$ et on trouve

$$\frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{(1+i)(1-i)} = \frac{(1+3)+i(-1+3)}{2} = 2+i$$

$$\Rightarrow 1+3i = (2+i)(1+i) + \text{reste null}.$$

Puisque le pgcd est le dernier reste non-null, on trouve

$$\text{pgcd}(11+7i, 3+7i) = 1+i.$$

#