Université de Rennes 1 Année 2023/2024

Algèbre et arithmétique 1
PROBLÈME

Notations/conventions : On désigne par $\mathbb{Z}_{\geq n}$ l'ensemble des entiers supérieurs à n et $\mathbb{R}_{>0}$ (resp. $\mathbb{Q}_{>0}$) l'ensemble des réels (resp. rationnels) strictement positifs. On note $a \wedge b$ le pgcd de deux entiers a et b. On rappelle que tout rationnel s'écrit de manière unique sous la forme q/p avec p, q entiers premiers entre eux et $p > 0$.

1. (a) Un triplet $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$ est dit *pythagoricien* si $a^2+b^2 = c^2$. Donner un exemple de triplet pythagoricien.

> **Solution:** On a $3^2 + 4^2 = 9 + 16 = 25 = 5^2$ et $(3, 4, 5)$ est donc un triplet pythagoricien.

(b) Soit (a, b, c) un triplet pythagoricien. Montrer que $c \geq b + 1$. Peut on avoir égalité ? Montrer que $a^2 \geq 2b + 1$. Peut on avoir égalité ?

> **Solution:** On a $c^2 = b^2 + a^2 \geq b^2 + 1 > b^2$ et donc $c > b$ si bien que $c \geq b + 1$. L'égalité est atteinte dans le cas de $(3, 4, 5)$. On en déduit que $a^2 + b^2 = c^2 \geq (b + 1)^2 = b^2 + 2b + 1$ si bien que $a^2 \geq 2b + 1$. L'égalité est atteinte de nouveau avec $(3, 4, 5)$.

(c) Montrer que si (a, b, c) est un triplet pythagoricien, alors $(a, b, c) \in \mathbb{Z}^3_{\geq 3}$ (c'est à dire $a, b, c \geq 3$).

> **Solution:** Comme $c \geq b+1 \geq b$, il suffit de montrer que $a \geq 3$ et $b \geq 3$. Par symétrie, il suffit même de montrer que $a \geq 3$, ou de manière équivalente $a > 2$. On sait que $a^2 \geq 2b + 1 > 1$ et donc nécessairement $a > 1$. Par symétrie, on a aussi $b > 1$. Mais alors $a^2 \geq 2b + 1 > 4$ et donc finalement $a > 2$.

(d) Soit $n \in \mathbb{Z}_{\geq 1}$. Calculer

$$(2n^2 + 2n + 1)^2 - (2n^2 + 2n)^2.$$

En déduire que si $a \in \mathbb{Z}_{\geq 3}$ est impair, alors il existe un triplet pythagoricien de la forme (a, b, c).

> **Solution:** On calcule
>
> $$\begin{aligned}&(2n^2 + 2n + 1)^2 - (2n^2 + 2n)^2\\ =&(2n^2 + 2n + 1 - 2n^2 - 2n)(2n^2 + 2n + 1 + 2n^2 + 2n)\\ =&4n^2 + 4n + 1\\ =&(2n + 1)^2\end{aligned}$$
>
> Si $a \in Z_{\geq 3}$ est impair, il existe $n \in \mathbb{Z}_{\geq 1}$ tel que $a = 2n + 1$ et on peut poser $b = 2n^2 + 2n, c = 2n^2 + 2n + 1$.

(e) Soit $n \in \mathbb{Z}_{\geq 1}$. Calculer

$$(n^2+1)^2-(n^2-1)^2.$$

En déduire que si $b \in \mathbb{Z}_{\geq 3}$ est pair, alors il existe un triplet pythagoricien de la forme (a,b,c).

Solution: On calcule

$$\begin{aligned}&(n^2+1)^2-(n^2-1)^2\\=&(n^2+1-n^2+1)(n^2+1+n^2-1)\\=&4n^2\\=&(2n)^2\end{aligned}$$

Si $a \in Z_{\geq 3}$ est pair, il existe $n \in \mathbb{Z}_{\geq 2}$ tel que $b = 2n$ et on peut poser $a = n^2-1, c = n^2+1$.

2. (a) Soit $t \in \mathbb{R}$. Donner des équations du cercle $\mathcal{C}$ de centre $O\binom{0}{0}$ et de rayon 1 ainsi que de la droite D_t passant par $A\binom{-1}{0}$ et $B\binom{0}{t}$. Montrer que $A \in \mathcal{C} \cap D_t$.

Solution: Le cercle $\mathcal{C}$ a bien sûr pour équation $x^2+y^2=1$. D'autre part, si $M\binom{x}{y}$ est un point du plan, on a $\overrightarrow{AM}\binom{x+1}{y}$ et $\overrightarrow{AB}\binom{1}{t}$. On en déduit que la droite D_t a pour équation $y = t(x+1)$. On a $(-1)^2+0^2=1$ et $0 = t((-1)+1)$ si bien que $A \in \mathcal{C} \cap D_t$.

(b) Soit $t \in \mathbb{R}$. Montrer qu'il existe un unique point $M\binom{x}{y}$ tel que $(\mathcal{C} \setminus \{A\}) \cap D_t = \{M\}$. Exprimer x et y en fonction de t. Exprimer aussi t en fonction de x et y.

Solution: Soit $M\binom{x}{y}$ un point du plan distinct de A. On a

$$M \in \mathcal{C} \cap D_t \Leftrightarrow \begin{cases} x^2+y^2=1 \\ y=t(x+1) \end{cases} \Leftrightarrow \begin{cases} x^2+t^2(x+1)^2=1 \\ y=t(x+1). \end{cases}$$

Puisque $M \neq A$, on a $x \neq -1$ et donc $x+1 \neq 0$, si bien que nécessairement

$$t = \frac{y}{x+1}.$$

D'autre part, puisque $x+1 \neq 0$, on a

$$\begin{aligned}x^2+t^2(x+1)^2=1 &\Leftrightarrow x^2-1+t^2(x+1)^2=0\\&\Leftrightarrow (x+1)(x-1+t^2(x+1))=0\\&\Leftrightarrow x(1+t^2)-1+t^2=0\\&\Leftrightarrow x=\frac{1-t^2}{1+t^2}.\end{aligned}$$

En remplaçant dans la seconde équation, on trouve

$$y = t(x+1) = t\left(\frac{1-t^2}{1+t^2}+1\right) = t\left(\frac{1-t^2+1+t^2}{1+t^2}\right) = \frac{2t}{1+t^2}.$$

On voit donc qu'il existe un unique point $M\binom{x}{y}$ sur $\mathcal{C} \setminus \{A\}) \cap D_t$ qui est donné par

$$x = \frac{1-t^2}{1+t^2} \quad \text{et} \quad y = \frac{2t}{1+t^2}.$$

(c) Montrer que l'application

$$f : \mathcal{C} \setminus \{A\} \to \mathbb{R}, \quad M\binom{x}{y} \mapsto \frac{y}{x+1}$$

est bijective et déterminer son application réciproque g.

Solution: Si $t \in \mathbb{R}$, on désigne par $g(t)$ l'unique point de $\mathcal{C} \setminus \{A\}$ tel que $g(t) \in D_t$. On obtient ainsi une application $g : \mathbb{R} \to \mathcal{C} \setminus \{A\}$. Il résulte de la part précédente que, pour tout $t \in \mathbb{R}$, si on désigne les composantes de $g(t)$ par x et y, alors $g(t)$ est l'unique point de $\mathcal{C} \setminus \{A\}$ tel que $t = y/(x+1)$. Autrement dit,

$$\forall t \in \mathbb{R}, \forall M \in \mathcal{C} \setminus \{A\}, \quad f(t) = M \Leftrightarrow t = g(M).$$

Cela montre que f est bijective et que sa réciproque est g.

(d) Soit $t \in \mathbb{R}$ et $M\binom{x}{y} := g(t)$. Montrer que

$$t \in]0,1[\Leftrightarrow x, y \in \mathbb{R}_{>0}.$$

En déduire que

$$t \in \mathbb{Q} \cap]0,1[\Leftrightarrow x, y \in \mathbb{Q}_{>0}.$$

Solution: Supposons que $x, y > 0$. On a alors $t = y/(x+1) > 0$. Puisque $M \in \mathcal{C}$ et $x > 0$, on a $y \leq 1 < x + 1$ et donc aussi $t < 1$. Réciproquement, supposons que $0 < t < 1$, on a alors $t^2 < 1$ et donc $1 - t^2 > 0$, mais aussi $2t > 0$ si bien que

$$x = \frac{1-t^2}{1+t^2} > 0 \quad \text{et} \quad y = \frac{2t}{1+t^2} > 0.$$

Clairement, si $t \in \mathbb{Q}$, on a $x, y \in \mathbb{Q}$ et réciproquement. La seconde assertion en découle par intersection.

(e) Soient $(a,b,c) \in \mathbb{Z}^3_{\geq 1}$ et $M\binom{a/c}{b/c}$. Montrer que (a,b,c) est un triplet pythagoricien si et seulement si $M \in \mathcal{C}$ si et seulement s'il existe $p, q \in \mathbb{Z}$ premiers entre eux avec $0 < q < p$ tels que $M = g(q/p)$ (g est la réciproque de f ci-dessus).

Solution: La première assertion résulte du fait que

$$a^2 + b^2 = c^2 \Leftrightarrow \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

De plus, puisque $a/c, b/c \in \mathbb{Q}_{>0}$, on a $M \in \mathcal{C}$ si et seulement si il existe $t \in \mathbb{Q} \cap]0,1[$ tel que $M = f(t)$. Finalement, on sait que $t \in \mathbb{Q}$ si et seulement s'il existe $p, q \in \mathbb{Z}$ premiers entre eux avec $p > 0$ tels que $t = q/p$ et la condition $0 < t < 1$ est alors équivalente à $0 < q < p$.

(f) Soit $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$. Montrer que (a, b, c) est un triplet pythagoricien si et seulement s'il existe $p, q \in \mathbb{Z}$ premiers entre eux avec $0 < q < p$ tels que

$$\frac{a}{c} = \frac{p^2 - q^2}{p^2 + q^2} \quad \text{et} \quad \frac{b}{c} = \frac{2pq}{p^2 + q^2}.$$

Solution: Il suffit de traduire l'égalité $M = g(p/q)$ lorsque $M\binom{a/c}{b/c}$:

$$\frac{a}{c} = \frac{1 - (q/p)^2}{1 + (q/p)^2} = \frac{p^2 - q^2}{p^2 + q^2} \quad \text{et} \quad \frac{b}{c} = \frac{2q/p}{1 + (q/p)^2} = \frac{2pq}{p^2 + q^2}.$$

3. (a) Soit (a, b, c) un triplet pythagoricien. Montrer que $a \wedge b = a \wedge c = b \wedge c$.

Solution: On a $(a \wedge b)^2 = a^2 \wedge b^2$ et en particulier $(a \wedge b)^2 \mid a^2$ et $(a \wedge b)^2 \mid b^2$. Il en résulte que $(a \wedge b)^2 \mid a^2 + b^2 = c^2$ et donc $a \wedge b \mid c$. Puisque $a \wedge b \mid a$, cela implique que $a \wedge b \mid a \wedge c$. On montre de même (en utilisant $b^2 = c^2 - a^2$) que $a \wedge c \mid a \wedge b$ et on a donc égalité. Par symétrie, on aura aussi $a \wedge b = b \wedge c$.

(b) Un triplet pythagoricien (a, b, c) est dit *primitif* si a et b sont premiers entre eux. Montrer qu'alors a et c d'une part, ainsi que b et c d'autre part, sont aussi premiers entre eux.

Solution: En effet, on aura $a \wedge c = b \wedge c = a \wedge b = 1$.

(c) Montrer que si $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$ et $d \in \mathbb{Z}_{\geq 1}$, alors (a, b, c) est pythagoricien si et seulement si (da, db, dc) est pythagoricien. Réciproquement, montrer que si (a', b', c') est un triplet pythagoricien, il existe alors un unique triplet pythagoricien primitif (a, b, c) et un unique entier $d \in \mathbb{Z}_{\geq 1}$ tels que $(a', b', c') = (da, db, dc)$.

Solution: Tout d'abord, si $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$ et $d \in \mathbb{Z}_{\geq 1}$, on a

$$(da)^2 + (db)^2 = (dc)^2 \Leftrightarrow d^2(a^2 + b^2) = d^2c^2 \Leftrightarrow a^2 + b^2 = c^2.$$

La première assertion en résulte. Si, de plus, (a, b, c) est primitif, alors $d = d(a \wedge b) = da \wedge db$ d'ou l'unicité de d et donc aussi de (a, b, c) dans la réciproque. Montrons l'existence. On se donne donc un triplet pythagoricien (a', b', c'). Si $d := a' \wedge b'$, il existe alors $a, b \in \mathbb{Z}_{\geq 1}$ tels que $a' = da, b' = db$ et $a \wedge b = 1$. Mais on a vu qu'alors $d \mid c'$ et il existe donc $c \in \mathbb{Z}_{\geq 1}$ tel que $c' = dc$. On a donc $(a', b', c') = (da, db, dc)$ avec (a, b, c) primitif.

(d) Montrer que si $c \in \mathbb{Z}$ est pair, alors $c^2 \equiv 0 \mod 4$ et que si $a, b \in \mathbb{Z}$ sont impairs, alors $a^2 + b^2 \equiv 2 \mod 4$.

Solution: Si c est pair, alors il existe $k \in \mathbb{Z}$ tels que $c = 2k$ et on a donc

$$c^2 = (2k)^2 = 4k^2 \equiv 0 \mod 4.$$

Si a et b sont impairs, alors il existe $k, l \in \mathbb{Z}$ tels que $a = 2k+1$ et $b = 2l+1$. On a donc

$$a^2 + b^2 = (2k+1)^2 + (2l+1)^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 \equiv 2 \mod 4.$$

(e) Montrer que si (a, b, c) est un triplet pythagoricien, alors a ou b est pair. Montrer que si (a, b, c) est primitif, alors c est impair et a et b sont de parité différente (a impair et b pair par exemple).

Solution: Si a et b sont impairs, alors a^2 et b^2 sont impairs et donc $c^2 = a^2 + b^2$ est pair et c aussi. On aura donc $c^2 \equiv 0 \mod 4$ et $a^2 + b^2 \equiv 2 \mod 4$. Contradiction. Pour la seconde assertion, on peut maintenant supposer (par symétrie) que b est pair. Puisque a et b sont premiers entre eux, a est nécessairement impair. On a donc $c^2 = a^2 + b^2$ qui est impair et il en va donc de même de c.

(f) Soient $p, q \in \mathbb{Z}$ premiers entre eux avec $0 < q < p$,

$$a = p^2 - q^2, \quad b = 2pq \quad \text{et} \quad c = p^2 + q^2.$$

Montrer que (a, b, c) est un triplet pythagoricien et que $a \wedge b = 1$ ou 2. En déduire qu'il est primitif si et seulement si p et q sont de parité différente.

Solution: On a

$$a^2 + b^2 = (p^2 - q^2)^2 + (2pq)^2 = (p^2)^2 - 2p^2q^2 + (q^2)^2 + 4p^2q^2 = (p^2 + q^2)^2 = c^2.$$

Si $d = a \wedge b$, on a vu que $d \mid c$. On en déduit que $d \mid a + c = 2p^2$ et $d \mid a - c = 2q^2$ si bien que $d \mid 2p^2 \wedge 2q^2 = 2(p \wedge q)^2 = 2$ et donc $d = 1$ ou $d = 2$.
Si p et q sont de parité différente (resp. de même parité), alors $p + q$ et $p - q$ sont impairs (resp. pairs) et $a = p^2 - q^2 = (p + q)(p - q)$ aussi si bien que $d = 1$ (resp. $d = 2$ puisque b est pair).

(g) Montrer que, réciproquement, si (a, b, c) est un triplet pythagoricien primitif avec b pair, alors il existe $p, q \in \mathbb{Z}$ premiers entre eux avec $0 < q < p$ tels que

$$a = p^2 - q^2, \quad b = 2pq \quad \text{et} \quad c = p^2 + q^2.$$

Solution: On sait qu'il existe $p, q \in \mathbb{Z}$ premiers entre eux avec $0 < q < p$ tels que

$$(p^2+q^2)a = (p^2-q^2)c \quad \text{et} \quad (p^2+q^2)b = 2pqc$$

Comme $a \wedge c = 1$, on a $c \mid p^2+q^2$, il existe donc $d \in \mathbb{Z}_{\geq 1}$ tel que $p^2+q^2 = dc$. On en déduit que $p^2-q^2 = da$ et $2pq = db$. On sait alors que $d = 1$ ou 2 et il suffit de montrer que $d = 1$. Si $d = 2$, alors p^2-q^2 est pair, et p et q ont donc nécessairement la même parité si bien que $p+q$ et $p-q$ sont pairs et alors $4 \mid (p-q)(p+q) = p^2-q^2 = 2a$ si bien que $2 \mid a$, c'est à dire a est pair et donc b est impair. Contradiction.

(h) Donner cinq triplets pythagoriciens primitifs.

Solution: Avec les couples $(p,q) = (2,1),(3,2),(4,1),(4,3),(5,2)$, on obtient $(3,4,5),(5,12,13),(15,8,17),(7,24,25),(21,20,29)$.

4. Un nombre complexe z est un *nombre de Gauss* si $\mathrm{Re}(z), \mathrm{Im}(z) \in \mathbb{Z}$. Il est *pythagoricien* si $\mathrm{Re}(z), \mathrm{Im}(z), |z| \in \mathbb{Z}_{\geq 1}$. Il est *primitif* si $\mathrm{Re}(z)$ et $\mathrm{Im}(z)$ sont premiers entre eux. Montrer qu'un nombre de Gauss z est pythagoricien primitif avec $\mathrm{Im}(z)$ pair si et seulement s'il existe un nombre de Gauss w avec $\mathrm{Re}(w)$ et $\mathrm{Im}(w)$ premiers entre eux de parité différentes et $0 < \mathrm{Im}(w) < \mathrm{Re}(w)$ tels que $z = w^2$.

Solution: Soient $w = p+iq$ et $z = a+ib$ deux nombres de Gauss. On a

$$z = w^2 \Leftrightarrow a+ib = (p^2-q^2)+2ipq \Leftrightarrow \begin{cases} a = p^2-q^2 \\ b = 2pq \end{cases}$$

et bien sûr, en posant $c := |z|$, la condition supplémentaire $c = p^2+q^2$. On voit donc que notre condition est équivalente au fait que (a,b,c) est pythagoricien primitif avec b pair. Ce qui signifie que z est pythagoricien primitif avec $\mathrm{Im}(z)$ pair.