Corrigé DM n°2

PARTIE A

1) • Si $d<0$, $\sqrt{d} \notin \mathbb{Q}$

• Si $d>0$ (donc $d \geq 2$ par hypothèse), supposons par l'absurde $\sqrt{d} \in \mathbb{Q}$.

On aurait alors : $\sqrt{d} = \frac{a}{b}$ avec $(a,b) \in \mathbb{N}^* \times \mathbb{N}$ et $a \wedge b = 1$. D'où $a^2 = b^2 d$.

- si $a=1$, cela implique $b^2 d = 1$ d'où $b^2 = d = 1$ ce qui est exclu.

- si $a \geq 2$, alors a possède un diviseur premier p. Or $a^2 | b^2 d$ et $a^2 \wedge b^2 = 1$

donc, d'après le th. de Gauss, $a^2 | d$ puis $p^2 | d$, ce qui est exclu.

---

2) Si on a : $a + b\sqrt{d} = a' + b'\sqrt{d}$ avec $(a,a',b,b') \in \mathbb{Z}^4$, alors $a - a' = (b'-b)\sqrt{d}$.

Si on avait $b'-b \neq 0$, on aurait $\sqrt{d} = \frac{a-a'}{b'-b} \in \mathbb{Q}$, ce qui est exclu.

Donc $\underline{b=b'}$, puis $\underline{a=a'}$.

---

3) $\mathbb{Z}[\sqrt{d}]$ sous-anneau de $\mathbb{C}$ est facile : il suffit de vérifier que :

$$1 \in \mathbb{Z}[\sqrt{d}] \quad , \quad \forall (z,z') \in \mathbb{Z}[\sqrt{d}]^2 , \; z - z' \in \mathbb{Z}[\sqrt{d}] \text{ et } zz' \in \mathbb{Z}[\sqrt{d}]$$

---

4) • $\mathbb{Q}[\sqrt{d}]$ est un sous-corps de $\mathbb{C}$:

- $\mathbb{Q}[\sqrt{d}]$ sous-anneau de $\mathbb{C}$ se démontre comme ci-dessus.

- soit $a + b\sqrt{d} \neq 0 \in \mathbb{Q}[\sqrt{d}]$; alors $a - b\sqrt{d} \neq 0$ (car sinon, comme dans la question 2., on aurait $a=b=0$) d'où $\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2} = \underbrace{\frac{a}{a^2-db^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2-db^2}}_{\in \mathbb{Q}} \sqrt{d}$

est un e^{lt} de $\mathbb{Q}[\sqrt{d}]$.

• Il est clair que $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}[\sqrt{d}]$

• Enfin, si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Z}[\sqrt{d}]$, alors :

$$\mathbb{Z} \subset \mathbb{K} \Rightarrow \mathbb{Q} \subset \mathbb{K} \quad \text{et} \quad \sqrt{d} \in \mathbb{K} \Rightarrow \mathbb{Q}[\sqrt{d}] \in \mathbb{K}.$$

Ainsi, $\mathbb{Q}[\sqrt{d}]$ est bien le <u>plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Z}[\sqrt{d}]$</u>.

---

5) a) Soit $f : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}[\sqrt{d}]$, $z \longmapsto \bar{z}$. On vérifie facilement que :

$$f(1) = 1 \; ; \; \forall (z,z') \in \mathbb{Z}[\sqrt{d}]^2 \; , \; f(z+z') = f(z) + f(z') \text{ et } f(zz') = f(z)f(z')$$

Donc f est un endomorphisme de l'anneau $\mathbb{Z}[\sqrt{d}]$. Puisque $f \circ f = \mathrm{Id}_{\mathbb{Z}[\sqrt{d}]}$,

f est involutive, donc bijective : f <u>automorphisme</u>.

b). Si $z \in \mathbb{Z}[\sqrt{d}]$, $N(z) = z\bar{z} = a^2 - db^2 \in \mathbb{Z}$
($z = a + b\sqrt{d}$)

- Si $z, z' \in \mathbb{Z}[\sqrt{d}]$, $N(zz') = zz'\overline{zz'} = zz'\bar{z}\bar{z}' = z\bar{z}\,z'\bar{z}' = N(z)N(z')$

donc N est bien un morphisme de $(\mathbb{Z}[\sqrt{d}], \times)$ dans $(\mathbb{Z}, \times)$.

PARTIE B

1) • Si $z \in \mathbb{Z}[\sqrt{d}]$ est inversible, alors il existe $z' \in \mathbb{Z}[\sqrt{d}]$ tel que $zz' = 1$.
On a alors : $N(zz') = N(z)N(z') = 1$. Puisque $N(z) \in \mathbb{Z}$, on a donc $N(z) = \pm 1$

• Réciproquement, si $N(z) = \pm 1$ alors $z\bar{z} = \pm 1$, donc z est inversible, d'inverse $\pm \bar{z}$

---

2) a) Soit $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. z inversible $\Leftrightarrow N(z) = a^2 - db^2 = \pm 1$. Ici, $d < 0$, donc cela équivaut à $N(z) = 1$.

b) • Si $d = -1$, $a + ib \in \mathbb{Z}[i]$ est inversible ssi $a^2 + b^2 = 1$. Puisque $(a,b) \in \mathbb{Z}^2$, cela équivaut à $(a,b) \in \{(-1,0), (1,0), (0,-1), (0,1)\}$, soit $a + ib \in \{\pm 1, \pm i\}$
(groupe des racines quatrièmes de l'unité)

• Si $d \leq -2$, $a + ib\sqrt{-d} \in \mathbb{Z}[i\sqrt{-d}]$ est inversible ssi $a^2 - b^2 d = 1$, soit $a^2 = 1 + b^2 d$. On a donc $a^2 \leq 1 - 2b^2$ d'où nécessairement $b = 0$ puis $a = \pm 1$.
Le groupe des elts inversibles de $\mathbb{Z}[\sqrt{d}]$ est alors $(\{\pm 1\}, \times)$.

---

3) a) Soit z inversible, $z = a + b\sqrt{d}$ et $z > 1$. Puisque l'inverse de z est $\pm \bar{z}$, l'ensemble $\{z, \frac{1}{z}, -z, -\frac{1}{z}\}$ est formé des quatre nombres $\pm a \pm b\sqrt{d}$.
Or, puisque $z > 1$, le plus grand de ces 4 nombres est z (et ils sont tous distincts)
On en déduit : $a > 0$ et $b > 0$

b) • Si $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ est inversible et strict. supérieur à 1, on a $N(z) = \pm 1$ soit $a^2 - db^2 = \pm 1$. On a donc nécessairement $db^2 = a^2 \pm 1$, d'où $b\sqrt{d} = \pm\sqrt{a^2 \pm 1}$. Puisque $a > 0, b > 0$, on a nect $z = a + \sqrt{a^2 \pm 1}$ (avec $a \geq 1$, a entier)

• Pour trouver l'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$, il suffit de calculer les $b^2 d$ (pour $b \geq 1$) et de s'arrêter dès que l'on trouve $b^2 d =$ un carré ± 1.
On obtient, resp. pour $d = 2, 3, 5, 6$: $\omega = 1 + \sqrt{2},\ 2 + \sqrt{3},\ 2 + \sqrt{5},\ 5 + 2\sqrt{6}$.

c) • Soit z un elt inversible de $\mathbb{Z}[\sqrt{d}]$, $z > 0$ (cela a un sens, car $d > 0$)
Alors : $1 \leq z\omega^{-n} < \omega \Leftrightarrow 0 \leq \ln z - n\ln\omega < \ln\omega \Leftrightarrow n \leq \frac{\ln z}{\ln \omega} < n+1$

Il existe donc un (et un seul) entier $n \in \mathbb{Z}$ tq $1 \leq z\omega^{-n} < \omega$: il s'agit de $n = E\left(\frac{\ln z}{\ln \omega}\right)$.

- ω étant le + petit des éléments inversibles de $\mathbb{Z}[\sqrt{d}]$ qui sont strictement supérieurs à 1, on a : $z > 0$ inversible $\Rightarrow \exists n \in \mathbb{Z}$ tq $z\omega^{-n} = 1$, soit $z = \omega^n$.

On en déduit : $z < 0$ inversible $\Rightarrow \exists n \in \mathbb{Z}$ tq $z = -\omega^n$.

L'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{d}]$ est donc inclus dans l'ensemble $\{\pm\omega^n, n \in \mathbb{Z}\}$. L'inclusion inverse étant facile (car $N(\omega^n) = N(\omega)^n = \pm 1$), cela donne l'égalité demandée.

---

4) a) • On démontre d'abord, par une récurrence facile, que : $\forall n \in \mathbb{N}$: $\omega^n = a_n + b_n\sqrt{d}$

• L'équation (E) : $a^2 - db^2 = 1$ équivaut à, si $z = a + b\sqrt{d}$, $N(z) = 1$. z est donc inversible, donc $z = \pm\omega^n$, $n \in \mathbb{Z}$. Puisqu'on se limite à $(a,b) \in \mathbb{N}^{*2}$, cela implique $z = \omega^n$.

Réciproquement, $z = \omega^n = a_n + b_n\sqrt{d}$ convient car $N(\omega^n) = N(\omega)^n = 1$

<u>Les solutions de (E) sont donc les couples (a_n, b_n).</u>

• Pour les mêmes raisons, les solutions de (E') sont nécessairement de la forme $z = a_n + b_n\sqrt{d} = \omega^n$. Mais ici, ces valeurs ne conviennent pas car $N(\omega^n) = 1$, alors que (E') s'écrit $N(z) = -1$. Donc <u>(E') n'a pas de solution.</u>

b) Raisonnement similaire.

<u>PARTIE C :</u>

1) Pour $\forall u \in \mathbb{Q}$, il existe $a \in \mathbb{Z}$ tel que $|u - a| \leq \frac{1}{2}$: il suffit de choisir $a = E(u)$ ou $a = E(u) + 1$ (selon que $u - E(u) \leq \frac{1}{2}$ ou $u - E(u) \geq \frac{1}{2}$)

---

2) Soit $\alpha \in \mathbb{Q}[\sqrt{d}]$: $\alpha = u + u'\sqrt{d}$ avec $(u,u') \in \mathbb{Q}^2$. D'après ce qui précède, il existe $(a,a') \in \mathbb{Z}^2$ tq $|u - a| \leq \frac{1}{2}$ et $|u' - a| \leq \frac{1}{2}$. On a alors :

$$\alpha - z = (u-a) + (u'-a')\sqrt{d} \quad \text{d'où} \quad N(\alpha - z) = (u-a)^2 - d(u'-a')^2$$

– si $d \in \{-2, -1, 2\}$, on aura donc : $|N(\alpha - z)| \leq \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4}$

– si $d = 3$, on a : $-3(u'-a')^2 \leq N(\alpha - z) \leq (u-a)^2$ soit $-\frac{3}{4} \leq N(\alpha - z) \leq \frac{1}{4}$.

Dans tous les cas, on a bien : <u>$|N(\alpha - z)| < 1$.</u>

---

3) Soient $z, z' \in \mathbb{Z}[\sqrt{d}]$, $z' \neq 0$. Alors $\frac{z}{z'} \in \mathbb{Q}[\sqrt{d}]$. D'après la question précédente :

il existe $q \in \mathbb{Z}[\sqrt{d}]$ tel que $\left|N\left(\frac{z}{z'} - q\right)\right| < 1$. Posons $r = z - qz'$.

On a alors : $r \in \mathbb{Z}[\sqrt{d}]$ et $|N(r)| = \left|N\left(z' \cdot \left(\frac{z}{z'} - q\right)\right)\right| = \left|N(z') \cdot N\left(\frac{z}{z'} - q\right)\right| < N(z')$.

Il existe donc bien $(q, r) \in \mathbb{Z}[\sqrt{d}]^2$ tq $z = qz' + r$, avec $|N(r)| < |N(z')|$

---

4) $\mathbb{Z}[\sqrt{d}]$ étant inclus dans $\mathbb{C}$ est intègre. Pour montrer qu'il est principal, il suffit de montrer que tous ses idéaux sont principaux, i.e. engendrés par un élément.

Soit donc I idéal de $\mathbb{Z}[\sqrt{d}]$:

- si $I = \{0\}$, le résultat est acquis : $I = 0 . \mathbb{Z}[\sqrt{d}]$
- si $I \neq \{0\}$: l'ensemble $\{|N(z)|, z \in I - \{0\}\}$ est un ss-ens. non vide de

$\mathbb{N}$, donc admet un plus petit élément. Il existe donc $a \in I - \{0\}$ tel que :

$$\forall z \in I - \{0\}, \quad |N(a)| \leq |N(z)|$$

Soit alors $z' \in I$. D'après la question précédente, il existe $(q, r) \in \mathbb{Z}[\sqrt{d}]^2$ tels que : $\begin{cases} z' = qa + r \\ |N(r)| < |N(a)| \end{cases}$. Or $a \in I$ idéal $\Rightarrow qa \in I \Rightarrow z - qa \in I$.

Donc $r \in I$ et $|N(r)| < |N(a)|$, d'où $\underline{r = 0}$ par déf. de a. On a donc :

$$\forall z' \in I, \exists q \in \mathbb{Z}[\sqrt{d}] \text{ tq } z' = qa, \text{ soit } I \subset a.\mathbb{Z}[\sqrt{d}].$$

L'inclusion réciproque est facile (car I idéal). D'où $\underline{I = a.\mathbb{Z}[\sqrt{d}]}$: cqfd

---

PARTIE D :

1) Soit $x \in \mathbb{Z}[\sqrt{d}]$, premier. S'il existe $y, z \in \mathbb{Z}[\sqrt{d}]$ tq $x = yz$, alors

$x | yz$ donc $x | y$ ou $x | z$.

- si $x | y$: $\exists a \in \mathbb{Z}[\sqrt{d}]$ tq $y = ax$, d'où $x = axz$ d'où $az = 1$

(car $x \neq 0$ et $\mathbb{Z}[\sqrt{d}]$ intègre). Ainsi, z est inversible.

- de même, si $x | z$, on trouve : y inversible.

On a donc montré : $x | yz \Rightarrow y$ inversible ou z inversible. i.e. $\underline{x \text{ irréductible}}$.

---

2) Supposons ici $\mathbb{Z}[\sqrt{d}]$ principal. Soit x irréductible, et $(y, z) \in \mathbb{Z}[\sqrt{d}]^2$ tq $x | yz$.

Supposons que x ne divise pas y. Soit I l'idéal engendré par x et y. $\mathbb{Z}[\sqrt{d}]$ étant principal, il existe u tq I soit l'idéal engendré par u. $(I = u.\mathbb{Z}[\sqrt{d}])$

Alors : $x \in I \Rightarrow \exists a \in \mathbb{Z}[\sqrt{d}]$ tq $x = au$

$y \in I \Rightarrow \exists b \in \mathbb{Z}[\sqrt{d}]$ tq $y = bu$

x étant irréductible, $x = au \Rightarrow a$ inversible ou u inversible.

Si a était inversible, on aurait $u = a^{-1}x$ d'où $y = ba^{-1}x$ serait multiple de x, ce qui contredit l'hypothèse. On a donc forcément u inversible. Mais, dans ce cas, $1 \in id(\{u\})$ (car $1 = u^{-1}u$), donc $1 \in I$ i.e. $\exists (a,b) \in \mathbb{Z}[\sqrt{d}]^2$ tq $1 = ax + by$.

On a alors : $z = axz + byz$. Puisque $x | xz$ et $x | yz$, on a donc $x | z$.

Finalement, on a montré que : si $x | yz$ et $x \nmid y$ alors $x | z$, donc x est premier.

---

3) • Si $d \equiv 1\ [4]$, $|a^2 - db^2| \equiv |a^2 - b^2|\ [4]$. Or, si $x \in \mathbb{Z}$, on a nécessairement $x^2 \equiv 0\ [4]$ ou $x^2 \equiv 1\ [4]$ (envisager les quatre cas possibles !). On ne peut donc jamais avoir $|a^2 - b^2| \equiv 2\ [4]$, et l'équation $a^2 - db^2 = 2$ n'a pas de solution dans $\mathbb{Z}^2$.

• Si $d \leq -3$: si l'équation avait une solution (a,b) tq $b \neq 0$, on aurait :

$$2 = |a^2 - db^2| = a^2 + |d| b^2 \geq 3b^2 \geq 3 \quad !!$$

Les seules solutions possibles sont donc les couples $(a,0)$. Mais l'équation $a^2 = 2$ n'a pas de solution dans $\mathbb{Z}$. Donc, finalement, l'éq. n'a pas de solution.

---

4) - Notons d'abord que 2 n'est pas inversible dans $\mathbb{Z}[\sqrt{d}]$ (car $N(2) = 4$)

- Si $2 = yz$, avec $(y,z) \in (\mathbb{Z}[\sqrt{d}])^2$, alors $N(y)N(z) = N(2) = 4$.
  - si $N(y) = \pm 1$ ou $N(z) = \pm 1$, on a y inversible ou z inversible
  - sinon, on a néc^t $|N(y)| = |N(z)| = 2$, ce qui est impossible d'après la question précédente.

Final^t, $2 = yz \Rightarrow y$ inversible ou z inversible, i.e. 2 irréductible dans $\mathbb{Z}[\sqrt{d}]$.

---

5) ~~Erreur d'énoncé : il fallait montrer « 2 n'est pas premier dans $\mathbb{Z}[\sqrt{d}]$ »~~

• $(d + \sqrt{d})(d - \sqrt{d}) = d^2 - d = d(d-1)$. Or $d(d-1)$ est pair, donc 2 divise $d^2 - d$ (dans $\mathbb{Z}$, donc a fortiori ds $\mathbb{Z}[\sqrt{d}]$). Si 2 était premier, on aurait $2 | d + \sqrt{d}$ ou $2 | d - \sqrt{d}$.
Si, par exemple, $2 | d + \sqrt{d}$, il existerait $(a,b) \in \mathbb{Z}^2$ tq $d + \sqrt{d} = 2(a + b\sqrt{d})$
Soit $2a = d$ et $2b = 1$!!

Cela est impossible, donc 2 n'est pas premier dans $\mathbb{Z}[\sqrt{d}]$.

• Donc : pour $d \leq -3$ ou $d \equiv 1\ [4]$, l'anneau $\mathbb{Z}[\sqrt{d}]$ n'est pas principal
(sinon, 2 irréductible $\Rightarrow$ 2 premier ...)

---

6) • Formons la table des congruences des carrés modulo 10 :

$a \equiv$	0	1	2	3	4	5	6	7	8	9
$a^2 \equiv$	0	1	4	9	6	5	6	9	4	1

Or : $|a^2 - 10b^2| = 2 \Rightarrow a^2 - 10b^2 = \pm 2 \Rightarrow a^2 \equiv \pm 2\ [10]$: l'équation $|a^2 - 10b^2| = 2$ n'a donc pas de solution dans $\mathbb{Z}^2$.

• On en déduit, comme en D.4, que 2 est irréductible ds $\mathbb{Z}[\sqrt{10}]$

• $(2 + \sqrt{10})(2 - \sqrt{10}) = -6$ donc $2 | (2 + \sqrt{10})(2 - \sqrt{10})$ puis raisonnement similaire à D.5 ...

1) _ Notons d'abord que $i\sqrt{2}$ n'est pas inversible dans $\mathbb{Z}[\sqrt{-2}]$ car $N(i\sqrt{2})=2$.
- Si $i\sqrt{2}=yz$ avec $y,z\in\mathbb{Z}[\sqrt{-2}]$, alors $N(y)\,N(z)=2$ d'où, nécess^t, $N(y)=\pm1$ ou $N(z)=\pm1$ d'où y inversible ou z inversible : $i\sqrt{2}$ est donc premier.

---

2) Si $x\in\mathbb{N}^*$ est divisible par $i\sqrt{2}$ dans $\mathbb{Z}[\sqrt{-2}]$, il existe $(a,b)\in\mathbb{Z}^2$ tel que
$x=i\sqrt{2}\,(a+ib\sqrt{2})=-2b+ia\sqrt{2}$. $x\in\mathbb{N}^* \Rightarrow a=0$ et $-2b=x$ donc x est pa

---

3) Soit x un entier impair, et soit $d\in A$ tel que $d\,|\,x+i\sqrt{2}$ et $d\,|\,x-i\sqrt{2}$, d irréductible. On a alors $d\,|\,(x+i\sqrt{2})-(x-i\sqrt{2})$ soit $d\,|\,2i\sqrt{2}$. d étant irréductible, (ou premier...)
on a $d\,|\,2$ ou $d\,|\,i\sqrt{2}$. Mais $d|2 \Rightarrow d|-2 \Rightarrow d\,|\,(i\sqrt{2})^2 \Rightarrow d\,|\,i\sqrt{2}$.
On a donc dans tous les cas $d\,|\,i\sqrt{2}$; or $i\sqrt{2}$ est premier dans A, d'où $d=\pm1$ (±1 sont les él^{ts} inversibles de $\mathbb{Z}[\sqrt{-2}]$), ou $d=\pm i\sqrt{2}$. Si on avait $d=\pm i\sqrt{2}$, puisque $d\,|\,x+i\sqrt{2}$, on aurait $i\sqrt{2}\,|\,x$, ce qui est impossible d'après la question précédente car x est impair.
Final^t, le seul diviseur commun (irréductible) à $x+i\sqrt{2}$ et $x-i\sqrt{2}$ est ±1, donc $x+i\sqrt{2}$ et $x-i\sqrt{2}$ sont premiers entre eux.

---

4) _ A étant principal, on sait que tout élément de A admet une déc. en facteurs premiers.
- Soit $w\in A$, $w=\pm p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ sa déc. en facteurs premiers. [cf. cours: ±1 sont ici les seuls él^{ts} inversibles de A]
Alors $uv=w^n=\pm\, p_1^{n\alpha_1}\cdots p_k^{n\alpha_k}$. u et v étant premiers entre eux n'ont pas de facteurs premiers communs. On peut donc partitionner $\{p_1,\dots p_k\}$ en deux ss-ens disjoints, le premier formé des facteurs premiers de u, le second formé de ceux de v.
On aura alors $uv=\pm\underbrace{p_1^{n\alpha_1}\cdots p_\ell^{n\alpha_\ell}}_{\text{facteurs 1ers de } u}\ \underbrace{p_{\ell+1}^{n\alpha_{\ell+1}}\cdots p_k^{n\alpha_k}}_{\text{fact. 1ers de } v}$ et, à l'aide des théorèmes usuels (en particulier le th. de Gauss)
on en tire : $u=\pm\,p_1^{n\alpha_1}\cdots p_\ell^{n\alpha_\ell}$ et $v=\pm\,p_{\ell+1}^{n\alpha_{\ell+1}}\cdots p_k^{n\alpha_k}$ soit $u=\pm w_1^n$, $v=\pm w_2^n$

---

5) • En étudiant les huit cas possibles, on remarque que si $x\in\mathbb{Z}$, on a $x^3\equiv 0,1,3,5,$ ou 7 modulo 8. D'où, si $y^2=x^3-2$, $y^2\equiv 6,7,1,3$ ou 5 modulo 8
En étudiant les congruences des carrés, on observe que la seule possibilité est $y^2\equiv1\ [8]$, donc y impair.
• D'après E.3., $y\pm i\sqrt{2}$ sont premiers entre eux. Puisque $x^3=(y+i\sqrt{2})(y-i\sqrt{2})$ la question E.4 donne : $\exists\, w_1,w_2\in\mathbb{Z}[\sqrt{-2}]$ tq $y+i\sqrt{2}=w_1^3$ et $y-i\sqrt{2}=w_2^3$
- Si $w_1=a+ib\sqrt{2}$ avec $(a,b)\in\mathbb{Z}^2$, $y+i\sqrt{2}=(a+ib\sqrt{2})^3$ donne $\begin{cases} a^3-6ab^2=y & (1)\\ 3a^2b-2b^3=1 & (2)\end{cases}$
(2) implique $b\,|\,1$ d'où $b=\pm1$. $b=1$ donne $3a^2=3$ d'où $a=\pm1$. Puisque $y>0$, on a forcément $a=-1$ et $y=5$, puis $x=3$. $b=-1$ donne $3a^2=1$: impossible. Finalement $x=3$, $y=5$ est bien la seule solution [FIN]