Simulation DS N°5

Structures-Arithmétique

11 Février 2019

Durée 1 heures

Problème 1

On dit que $(x, y, z) \in (\mathbb{N}^*)^3$ est un triplet pythagoricien si et seulement si $x^2 + y^2 = z^2$. L'objectif de cet exercice est de déterminer tous les triplets pythagoriciens. On note dans tout cet exercice $x \wedge y = \text{pgcd}(x, y)$. Les diviseurs considérés dans ce problème sont des entiers naturels. Enfin, on dira que $a \in \mathbb{N}$ est un carré si et seulement si il existe $b \in \mathbb{N}$ tel que $a = b^2$.

1. Soit $d \in \mathbb{N}^*$ un diviseur commun à x, y et z, en factorisant par d montrer qu'il suffit de déterminer les triplets pythagoriciens qui n'ont pas d'autres diviseurs communs que 1.

   On dit alors que x, y et z sont premiers entre eux et on parle dans ce cas de triplet pythagoricien primitif. Dans toute la suite, on s'intéresse à un triplet pythagoricien primitif (x, y, z).

2. Montrer que $x \wedge y = x \wedge z = y \wedge z = 1$. En déduire que x et y ne sont pas tous les deux pairs.
3. A l'aide de congruences modulo 4, montrer que x et y ne sont pas tous les deux impairs.

   Les entiers naturels x et y sont de parités distinctes, sans perte de généralité on suppose dans toute la suite que x est pair et y impair.

4. Justifier qu'il existe $(u, v, w) \in (\mathbb{N}^*)^3$ tels que $x = 2u$, $z + y = 2v$ et $z - y = 2w$.
5. Montrer que $v \wedge w = 1$.
6. Montrer que vw est un carré, en déduire que v et w sont des carrés. On pose $v = n^2$ et $w = m^2$ où $(n, m) \in \mathbb{N}^2$.
7. Montrer que $n > m$ et que $n \wedge m = 1$. Exprimer u en fonction de n et m.
8. En déduire que (x, y, z) est un triplet pythagoricien primitif si et seulement si il existe deux entiers n et m premiers entre eux et de parités distinctes avec $n > m > 0$ tels que $x = 2nm$, $y = n^2 - m^2$ et $z = n^2 + m^2$ ou $x = n^2 - m^2$, $y = 2nm$ et $z = n^2 + m^2$.

Problème Ouvert : Histoire vrai, question posé par un taupin français lors d'un DS en 2018

Les élèves de MPSI2 sont en train de finir l'AR18-7. Les grandes fenêtres de la salle permettent de contempler le beau ciel bleu d'aujourd'hui. Il y a même une nuée de vanneaux huppés qui volent en formation triangulaire parfaite. Soudain, les oiseaux se séparent en deux groupes de même effectif, eux-mêmes disposés en formation triangulaire parfaite. Interloqués, tous les étudiants posent leur stylo et se demandent alors combien il peut y avoir d'oiseaux, sachant qu'à première vue il y en a plus de 100 mais sûrement moins de 1000.

Il faut entendre par "formation triangulaire parfaite" qu'il y a un oiseau en tête de la nuée, suivi de deux oiseaux, suivis de trois oiseaux et ainsi de suite.

Problème 2 :

1. Dans toute la suite, on note $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2},\ (a,b) \in \mathbb{Z}^2\}$. Pour tout élément $x = a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on appelle norme de x l'entier relatif : $N(x) = a^2 - 2b^2$.
   (a) Montrer que si $x \in \mathbb{Z}[\sqrt{2}]$, il s'écrit de façon unique sous la forme $x = a + b\sqrt{2}$ où $(a,b) \in \mathbb{Z}^2$.
   (b) Montrer que $\mathbb{Z}[\sqrt{2}]$ muni de l'addition et de la multiplication usuelles est un anneau commutatif et intègre.
   (c) Démontrer que l'application suivante est un automorphisme d'anneau de $\mathbb{Z}[\sqrt{2}]$:
   $$\varphi \ : \ a + b\sqrt{2} \ \mapsto \ a - b\sqrt{2}$$
   (d) Montrer que N est multiplicative, c'est-à-dire que : $\forall (x,y) \in \mathbb{Z}[\sqrt{2}]^2,\ N(xy) = N(x)N(y)$.
   Dans la suite, on note $\mathbb{Z}[\sqrt{2}]^\times$ l'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ pour la multiplication.
   (e) Démontrer que pour tout $x \in \mathbb{Z}[\sqrt{2}]$, on a l'équivalence : $x \in \mathbb{Z}[\sqrt{2}]^\times \Leftrightarrow N(x) = \pm 1$.
   L'équivalence qui vient d'être démontrée pourra être utilisée avec profit dans toute la suite.
   (f) En déduire que pour tout $n \in \mathbb{N}$, $\pm(1 \pm \sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times$. Le but de la question 2 va être de démontrer que tous les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont de cette forme.
2. (a) Soient $(a,b) \in \mathbb{Z}^2$, justifier que si l'un des quatre éléments parmi : $a+b\sqrt{2}$, $a-b\sqrt{2}$, $-a+b\sqrt{2}$ et $-a-b\sqrt{2}$ est inversible alors les trois autres le sont aussi.
   (b) Soient $(a,b) \in \mathbb{N}^2$ tels que $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$.
      i. Justifier que $a \neq 0$.
      ii. Si $b = 0$, déterminer x.
      iii. Si $b \neq 0$, montrer que l'on a : $b \leq a < 2b$.
      iv. Si $b \neq 0$, simplifier $\dfrac{x}{1+\sqrt{2}}$.
      v. Montrer qu'il existe un entier naturel n tel que $x = (1+\sqrt{2})^n$. Pour cela, on pourra procéder par récurrence forte sur $a+b$ et utiliser la question précédente.
   (c) En déduire que : $\forall x \in \mathbb{Z}[\sqrt{2}]^\times,\ \exists n \in \mathbb{N},\ x = \pm(1 \pm \sqrt{2})^n$.
3. Revenons à notre problème d'oiseaux. On note N le nombre total de vanneaux huppés.
   (a) Justifier qu'il existe deux entiers naturels l et m tels que : $N = \dfrac{l(l+1)}{2} = m(m+1)$.
   (b) On pose $a = 2l+1$ et $b = 2m+1$. Démontrer que $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$.
   (c) En déduire qu'il existe $n \in \mathbb{N}$ tel que $a + b\sqrt{2} = (1+\sqrt{2})^n$. On note (a_n, b_n) l'unique couple d'entiers naturels tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$.
   (d) Démontrer que les suites (a_n) et (b_n) sont définies par les relations de récurrence :
   $$\begin{cases} a_0 = 1,\ b_0 = 0 \\ \forall n \in \mathbb{N},\ a_{n+1} = a_n + 2b_n \\ \forall n \in \mathbb{N},\ b_{n+1} = a_n + b_n \end{cases}$$
   (e) En développant $(1+\sqrt{2})^n$ pour les premières valeurs de n, trouver le nombre d'oiseaux.

CORRECTION

Problème 1

1. Soit $d \in \mathbb{N}^*$ un diviseur commun de x, y et z, il existe $(X, Y, Z) \in (\mathbb{N}^*)^3$ tels que $x = dX$, $y = dY$ et $z = dZ$. On a :
$$x^2 + y^2 = z^2 \Leftrightarrow (dX)^2 + (dY)^2 = (dZ)^2 \Leftrightarrow X^2 + Y^2 = Z^2$$
Il suffit de chercher les solutions sans diviseur commun, on obtiendra toutes les solutions en multipliant par un entier quelconque les trois coordonnées du triplet.
2. Soit $d \in \mathbb{N}^*$ un **nombre premier** tel que $d|x$ et $d|y$ alors $d|x^2 + y^2 = z^2$. Comme d divise z^2 alors d apparait dans la décomposition en facteurs premiers de z^2 donc il apparait dans la décomposition en facteurs premiers de z. En effet, les facteurs premiers de z et z^2 sont les mêmes, seules les valuations changent, ceci étant dû à l'unicité de la décomposition en facteurs premiers. Finalement d divise z. D'après l'hypothèse, un diviseur positif de x, y et z est égal à 1. On vient de démontrer que x et y n'ont pas de facteur premier en commun, d'après le cours cela implique qu'ils sont premiers entre eux.
On démontre de la même façon que $x \wedge z = y \wedge z = 1$.
$$\boxed{x \wedge y = x \wedge z = y \wedge z = 1}$$
Il est alors clair que x et y ne sont pas tous les deux pairs sinon ils auraient 2 comme facteur commun, ce qui est contradictoire avec le résultat précédent.
3. Par l'absurde, si x et y sont impairs alors il existe $(k, l) \in \mathbb{N}^2$ tels que $x = 2k + 1$ et $y = 2l + 1$. On a $x^2 = 4k^2 + 4k + 1$ et $y^2 = 4l^2 + 4l + 1$, ainsi $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$ donc $z^2 \equiv 2[4]$. C'est absurde car on vérifie immédiatement avec une table de congruence qu'un carré est congru à 0 ou 1 modulo 4.
$$\boxed{x \text{ et } y \text{ sont de parités distinctes}}$$
4. L'entier naturel x est pair et y est impair donc x^2 est pair et y^2 est impair, ce qui implique que z^2 est impair et par suite z est impair. On en déduit que $z + y$ et $z - y$ sont impairs. D'autre part, étant donné que x, y et z sont non nuls, on a : $x \geq 1$, $z + y \geq 1$ et $z - y \geq 1$ car $z^2 = y^2 + x^2 \geq y^2 + 1$. Finalement :
$$\boxed{\exists (u, v, w) \in (\mathbb{N}^*)^3,\ x = 2u,\ z + y = 2v \text{ et } z - y = 2w}$$
5. Soit $d \in \mathbb{N}^*$ tel que $d|v$ et $d|w$ alors $d|v + w = z$ et $d|v - w = y$. Or $y \wedge z = 1$ donc $d = 1$.
$$\boxed{v \wedge w = 1}$$
6. On a $4vw = (z + y)(z - y) = z^2 - y^2 = x^2 = 4u^2$.
$$\boxed{vw = u^2}$$
On reprend l'égalité précédente en utilisant la décomposition en facteurs premiers :
$$vw = \Big(\prod_{p \in \mathcal{P}} p^{\nu_p(u)}\Big)^2$$
Soit $p \in \mathcal{P}$ un nombre premier qui apparait dans la décomposition précédente alors $p|vw$. Comme v et w sont premiers entre eux alors p divise v et p ne divise pas w ou p ne divise pas v et p divise w. Dans la décomposition précédente en regroupant les facteurs premiers selon qu'ils divisent v ou w, on obtient :
$$v = \Big(\prod_{p \in \mathcal{P},\ p|v} p^{\nu_p(u)}\Big)^2 \text{ et } w = \Big(\prod_{p \in \mathcal{P},\ p|w} p^{\nu_p(u)}\Big)^2$$
$$\boxed{\exists (n, m) \in \mathbb{N}^2,\ v = n^2 \text{ et } w = m^2}$$

7. On a $2v - 2w = 2y > 0$ donc $v > w$ d'où $n^2 > m^2$ et par suite :

$$\boxed{n > m}$$

Si $d \in \mathbb{N}^*$ avec $d|n$ et $d|m$ alors $d|n^2 = v$ et $d|m^2 = w$, or $v \wedge w = 1$ d'où $d = 1$.

$$\boxed{n \wedge m = 1}$$

On a vu que $vw = u^2$ donc $n^2m^2 = u^2$ donc $u = nm$ puisque l'on travaille avec des entiers naturels.

$$\boxed{u = nm}$$

8. On vient de démontrer que les conditions données dans cette question sont des conditions nécessaires, l'autre triplet étant obtenu en supposant x impair et y pair. En effet, $x = 2u = 2nm$, $y = v - w = n^2 - m^2$ et $z = w + v = n^2 + m^2$ et m et n sont bien de parités distinctes car y est impair.
Réciproquement, on a bien :

$$x^2 + y^2 = (2nm)^2 + (n^2 - m^2)^2 = 4n^2m^2 + n^4 - 2n^2m^2 + m^4 = (n^2 + m^2)^2 = z^2$$

et (x, y, z) est un triplet Pythagoricien car si d est un nombre premier tel que $d|x$, $d|y$ et $d|z$ alors $d|2n^2 = y + z$ et $d|2m^2 = z - y$. Or d n'est pas pair car y (ou x) est impair puisque n et m sont de parités distinctes. Ainsi $d|m^2$ et $d|n^2$ donc $d|m$ et $d|n$, comme m et n sont premiers entre eux cela implique que $d = 1$. On a bien un triplet Pythagoricien primitif.

Problème 2 :

La grande majorité des résultats présentés dans ce problème sont également valables pour d'autres races d'oiseaux comme les oies rieuses, les cygnes chanteurs et presque tous les canards.

1. (a) L'existence de l'écriture est garantie par la définition de $\mathbb{Z}[\sqrt{2}]$. Il reste à démontrer l'unicité, pour cela supposons que $x \in \mathbb{Z}[\sqrt{2}]$ ait deux écritures : $x = a + b\sqrt{2} = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. Par soustraction, cela implique que $(a - c) + (b - d)\sqrt{2} = 0$, il y a deux cas à considérer :

   ▶ Si $b = d$, on obtient immédiatement $a = c$.

   ▶ Si $b \neq d$, on a $\sqrt{2} = \dfrac{c-a}{b-d}$. Ceci est absurde car $\sqrt{2}$ est irrationnel.

   On est toujours dans le premier cas et l'écriture est unique.

$$\boxed{\forall x \in \mathbb{Z}[\sqrt{2}],\ \exists!(a, b) \in \mathbb{Z}^2,\ x = a + b\sqrt{2}}$$

   (b) Nous allons démontrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de l'anneau $(\mathbb{R}, +, \times)$.

   ▶ Déjà $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ par définition.

   ▶ Montrons que $(\mathbb{Z}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbb{R}, +)$:

   - $0 = 0 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$
   - Soient $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$ avec $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. On a :

$$x + y = (a + c) + (b + d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ car } a + c \in \mathbb{Z} \text{ et } b + d \in \mathbb{Z}$$

   - Soit $x \in \mathbb{Z}[\sqrt{2}]$ avec $x = a + b\sqrt{2}$ où $(a, b) \in \mathbb{Z}^2$. On a :

$$-x = -a - b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ car } -a \in \mathbb{Z} \text{ et } -b \in \mathbb{Z}$$

   ▶ $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

   ▶ Soient $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$ avec $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. On a :

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ car } ac + 2bd \in \mathbb{Z} \text{ et } ad + bc \in \mathbb{Z}$$

$$\boxed{\mathbb{Z}[\sqrt{2}] \text{ est un sous-anneau de } \mathbb{R}}$$

   L'anneau $\mathbb{Z}[\sqrt{2}]$ est commutatif et intègre car c'est un sous-anneau de $\mathbb{R}$ qui est commutatif et intègre.

   (c) Vérifions les trois propriétés requises pour avoir un morphisme d'anneaux. Dans cette question, on se donne deux éléments de $\mathbb{Z}[\sqrt{2}]$ que l'on note $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ avec $(a, b, c, d) \in \mathbb{Z}^4$.

   ▶ On a :

$$\varphi(x + y) = \varphi((a + c) + (b + d)\sqrt{2}) = (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}) = \varphi(x) + \varphi(y)$$

   ▶ D'autre part :

$$\varphi(xy) = \varphi((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = \varphi(x)\varphi(y)$$

   ▶ Enfin, il est clair que $\varphi(1) = 1$.

   L'application φ est bijective car $\varphi \circ \varphi = \mathrm{id}_{\mathbb{Z}[\sqrt{2}]}$.

$$\boxed{\varphi \text{ est un automorphisme de } \mathbb{Z}[\sqrt{2}]}$$

(d) Soient $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$ avec $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. On a :

$$N(xy) = N((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd)^2 - 2(ad + bc)^2 = (ac)^2 + 4(bd)^2 - 2(ad)^2 - 2(bc)^2$$

D'autre part :

$$N(x)N(y) = (a^2 - 2b^2)(c^2 - 2d^2) = (ac)^2 - 2(ad)^2 - 2(bc)^2 + 4(bd)^2$$

Ce qui démontre le résultat voulu. $\boxed{N \text{ est multiplicative}}$

(e) Démontrons le résultat par double implication, on a :

($\Rightarrow$) Soit $x \in \mathbb{Z}[\sqrt{2}]^\times$, il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. En prenant la norme, il vient $N(xy) = N(1) = 1$, c'est-à-dire $N(x)N(y) = 1$. Or, par définition, $N(x)$ et $N(y)$ sont des entiers relatifs, on a nécessairement $N(x) = \pm 1$.

($\Leftarrow$) Réciproquement soit $x \in \mathbb{Z}[\sqrt{2}]$ avec $x = a + b\sqrt{2}$ où $(a, b) \in \mathbb{Z}^2$ tel que $N(x) = \pm 1$. On pose $y = (a - b\sqrt{2})N(x)$, on a :

$$xy = (a + b\sqrt{2})(a - b\sqrt{2})N(x) = (a^2 - 2b^2)N(x) = N(x)^2 = 1$$

Ainsi x est un élément inversible de $\mathbb{Z}[\sqrt{2}]$ et l'on a même trouvé l'expression de son inverse.
On vient de démontrer le critère qui va nous servir dans toute la suite de l'exercice :

$$\boxed{x \in \mathbb{Z}[\sqrt{2}]^\times \Leftrightarrow N(x) = \pm 1}$$

(f) Par une récurrence immédiate, on démontre que pour tout entier naturel n, $N(x^n) = N(x)^n$ en utilisant la propriété de multiplicativité de N. Ainsi pour tout entier naturel n, on a :

$$N(\pm(1 \pm \sqrt{2})^n) = N(\pm 1)N(1 \pm \sqrt{2})^n = 1 \times (-1)^n = (-1)^n$$

D'après le critère démontré à la question précédente, cela suffit pour affirmer que :

$$\boxed{\forall n \in \mathbb{N},\ \pm(1 \pm \sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times}$$

2. (a) Les quatre éléments en question ont la même norme : $a^2 - 2b^2$. Si l'un d'entre eux est inversible sa norme vaut ± 1 et par suite la norme des trois autres éléments vaut également ± 1 d'où leur inversibilité.

(b) i. Si $a = 0$ alors $N(x) = -2b^2$ ne peut être égal à ± 1 et par suite x ne peut pas être inversible. Ce qui est contraire à l'hypothèse de départ.

$$\boxed{\text{Si } a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times \text{ alors } a \neq 0}$$

ii. Si $b = 0$, on a $N(x) = a^2 = \pm 1$ puisque x est supposé inversible. Ainsi $a = 1$ puisque le cas $a = -1$ est à exclure comme l'on a supposé que $a \in \mathbb{N}$.

$$\boxed{\text{Si } b = 0 \text{ alors } x = 1}$$

iii. On suppose $b \neq 0$, comme x est inversible on a $N(x) = a^2 - 2b^2 = \pm 1$. D'une part :

$$a^2 \leq 2b^2 + 1 < 2b^2 + 2b^2 = 4b^2 \quad \text{en utilisant } 1 < 2b^2 \text{ puisque } b \text{ est un entier strictement positif}$$

Par croissance de la fonction racine carrée, étant donné que a et b sont positifs, l'inégalité précédente implique $a < 2b$.
D'autre part :

$$a^2 - 2b^2 = \pm 1 \geq -1 \text{ ce qui implique que } 2b^2 \leq a^2 + 1 \leq 2a^2 \text{ car } 1 \leq a^2$$

Ce qui démontre que $b \leq a$

$$\boxed{\text{Si } b \neq 0 \text{ alors } b \leq a < 2b}$$

iv. On a :

$$\frac{x}{1+\sqrt{2}} = \frac{x(1-\sqrt{2})}{(1+\sqrt{2})(1-\sqrt{2})} = -x(1-\sqrt{2}) = (2b-a) + (a-b)\sqrt{2}$$

$$\boxed{\frac{x}{1+\sqrt{2}} = (2b-a) + (a-b)\sqrt{2}}$$

v. Pour $r \in \mathbb{N}^*$, on considère l'hypothèse de récurrence :

$\mathcal{H}_r$: si $x = a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ avec $(a,b) \in \mathbb{N}^2$ et $a+b = r$ alors il existe $n \in \mathbb{N}$ tel que $x = (1+\sqrt{2})^n$

► Si $r = a+b = 1$ alors comme $(a,b) \in \mathbb{N}^2$ et $a \neq 0$ d'après la question 2.(b)i., on a nécessairement $a = 1$ et $b = 0$. Dans ce cas, on a $1 + 0\sqrt{2} = (1+\sqrt{2})^0$ ce qui montre que $n = 0$ convient.
► Soit $r \in \mathbb{N}^*$, on procède par récurrence forte en supposant que H_k est vraie pour tout $k \in [\![1, r]\!]$. Il s'agit de démontrer que $\mathcal{H}_{r+1}$ est vraie. Soit $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ avec $(a,b) \in \mathbb{N}^2$ et $a + b = r + 1$. Si $b = 0$ alors $x = 1$ d'après la question 2.(b)ii. et l'on peut choisir $n = 0$. Si $b \neq 0$, on considère :

$$\frac{x}{1+\sqrt{2}} = (2b-a) + (a-b)\sqrt{2} = a' + b'\sqrt{2}$$

On a $\dfrac{x}{1+\sqrt{2}}$ qui appartient à $\mathbb{Z}[\sqrt{2}]^\times$ comme quotient d'éléments inversibles. De plus $a' = 2b - a$ et $b' = a - b$ sont des entiers positifs d'après la question 2.(b)iii. et $a' + b' = b < a + b = r + 1$. Ce qui permet d'appliquer l'hypothèse de récurrence à $a' + b'\sqrt{2}$, il existe $n \in \mathbb{N}$ tel que $a' + b'\sqrt{2} = (1+\sqrt{2})^n$ et par suite $x = (1+\sqrt{2})^{n+1}$. Ce qui démontre que $\mathcal{H}_{r+1}$ est vraie et achève la récurrence.

$$\boxed{\text{Si } x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times \text{ avec } (a,b) \in \mathbb{N}^2 \text{ alors il existe } n \in \mathbb{N} \text{ tel que } x = (1+\sqrt{2})^n}$$

(c) Soit $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ avec $(a,b) \in \mathbb{Z}^2$. Il y a 4 cas à considérer :
► Si $a \geq 0$ et $b \geq 0$ alors d'après la question précédente, il existe $n \in \mathbb{N}$ tel que $\underline{a + b\sqrt{2} = (1+\sqrt{2})^n}$
► Si $a \leq 0$ et $b \leq 0$ alors d'après la question précédente, il existe $n \in \mathbb{N}$ tel que $-a - b\sqrt{2} = (1+\sqrt{2})^n$ d'où $\underline{a + b\sqrt{2} = -(1+\sqrt{2})^n}$.
► Si $a \geq 0$ et $b \leq 0$ alors d'après la question précédente, il existe $n \in \mathbb{N}$ tel que $a - b\sqrt{2} = (1+\sqrt{2})^n$, on applique φ à cette égalité et on utilise la propriété de morphisme de φ :

$$\varphi(a - b\sqrt{2}) = \varphi\Big((1+\sqrt{2})^n\Big) = \varphi(1+\sqrt{2})^n \Leftrightarrow \underline{a + b\sqrt{2} = (1-\sqrt{2})^n}$$

► Enfin si $a \leq 0$ et $b \geq 0$, on a d'après l'alinéa précédent, l'existence de $n \in \mathbb{N}$ tel que $-a-b\sqrt{2} = (1-\sqrt{2})^n$ d'où $\underline{a + b\sqrt{2} = -(1-\sqrt{2})^n}$
Dans les quatre cas, on a :

$$\boxed{\exists n \in \mathbb{N},\ x = \pm(1 \pm \sqrt{2})^n}$$

En résumé, cette question ainsi que la question 1.(f) permettent d'aboutir à la caractérisation des inversibles de l'anneau $\mathbb{Z}[\sqrt{2}]$:

$$\boxed{x \in \mathbb{Z}[\sqrt{2}]^\times \Leftrightarrow \exists n \in \mathbb{N},\ x = \pm(1 \pm \sqrt{2})^n}$$

3. (a) Les oiseaux volent en formation triangulaire, c'est-à-dire qu'il existe $l \in \mathbb{N}$ tel que :

$$N = 1 + 2 + 3 + ... + l = \frac{l(l+1)}{2}$$

D'autre part $\dfrac{N}{2}$ est également un entier qui peut s'écrire sous la forme $1 + 2 + 3 + ... + m$ puisque les deux groupes de $\dfrac{N}{2}$ oiseaux volent également en formation triangulaire.

$$\boxed{\exists (l, m) \in \mathbb{N}^2,\ N = \frac{l(l+1)}{2} = m(m+1)}$$

(b) Utilisons l'équivalence démontrée à la question 1.(e) en vérifiant que $N(a + b\sqrt{2}) = \pm 1$. On a :

$$\begin{aligned} N(a + b\sqrt{2}) &= a^2 - 2b^2 \\ &= (2l+1)^2 - 2(2m+1)^2 \\ &= 4l^2 + 4l + 1 - 8m^2 - 8m - 2 \\ &= 8\Big(\frac{l(l+1)}{2} - m(m+1)\Big) - 1 \\ &= -1 \end{aligned}$$

$$\boxed{\text{Si } a = 2l+1 \text{ et } b = 2m+1 \text{ alors } a + b\sqrt{2} \text{ est inversible}}$$

(c) Comme a et b sont positifs, on est dans le cadre de la question 2.(b), ainsi :

$$\boxed{\exists n \in \mathbb{N},\ a + b\sqrt{2} = (1+\sqrt{2})^n}$$

(d) Si $n = 0$, on a $(1+\sqrt{2})^0 = 1 = 1 + 0 \times \sqrt{2}$ ainsi $a_0 = 1$ et $b_0 = 0$. Soit $n \in \mathbb{N}$, on a :

$$a_{n+1} + b_{n+1}\sqrt{2} = (1+\sqrt{2})^{n+1} = (1+\sqrt{2})(1+\sqrt{2})^n = (1+\sqrt{2})(a_n + b_n\sqrt{2}) = (a_n + 2b_n) + (a_n + b_n)\sqrt{2}$$

Ce qui démontre que $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$, cette identification étant valable puisque tout élément de $\mathbb{Z}[\sqrt{2}]$ s'écrit de façon unique sous la forme $a + b\sqrt{2}$.

$$\boxed{\begin{cases} a_0 = 1,\ b_0 = 0 \\ \forall n \in \mathbb{N},\ a_{n+1} = a_n + 2b_n \\ \forall n \in \mathbb{N},\ b_{n+1} = a_n + b_n \end{cases}}$$

(e) Les formules précédentes permettent de calculer de proche en proche les coefficients du développement de $(1+\sqrt{2})^n$. Une fois que l'on connaît ces coefficients, on trouve $a = a_n$ puisque $a + b\sqrt{2} = (1+\sqrt{2})^n$ et on en déduit l car $l = \dfrac{a-1}{2}$. Si l'on connaît l, on trouve le nombre d'oiseaux N puisque $N = \dfrac{l(l+1)}{2}$.

n	a_n	b_n	a	l	N
0	1	0	1	0	0
1	1	1	1	0	0
2	3	2	3	1	1
3	7	5	7	3	6
4	17	12	17	8	36
5	41	29	41	20	210
6	99	70	99	49	1225

Le seul résultat étant compris entre 100 et 1000 est $N = 210$.

On remarque d'ailleurs que si n est pair alors b_n est pair ce qui ne peut pas convenir à notre problème où b est impair.

Ce jour-là il y avait 210 vanneaux huppés

Un autre problème assez similaire est celui de la pile d'oranges. On considère une pyramide à base carrée d'oranges, c'est-à-dire qu'il y n^2 oranges à la base (un carré de n par n), $(n-1)^2$ oranges au dessus ainsi de suite jusqu'à l'orange qui se trouve au sommet. Le nombre, N, d'oranges est de la forme :

$$N = 1 + 2 + ... + (n-1)^2 + n^2 \text{ pour un certain } n \in \mathbb{N}$$

La pile s'effrondre et l'on remarque que l'on peut réorganiser les oranges en un carré parfait. C'est-à-dire que $N = l^2$ où $l \in \mathbb{N}$. Hormis $N = 1$, la seule solution est $N = 4900$.