Devoir surveillé 6

▸ Exercice 1 : nombres de Mersenne et nombres parfaits

Pour $n \in \mathbf{N}^*$ on note $\mathcal{D}(n) = \{k \in \mathbf{N}^* \mid k \text{ divise } n\}$ l'ensemble des diviseurs **positifs** de n.
On note également $S(n)$ la somme des diviseurs **positifs** de n : $S(n) = \sum_{k \in \mathcal{D}(n)} k$.

Un entier $n \in \mathbf{N}^*$ est dit **parfait** si $S(n) = 2n$.
Par exemple, 6 est parfait puisque $S(6) = 1 + 2 + 3 + 6 = 12$.

Partie I. La fonction somme des diviseurs

1. Montrer qu'un entier $n \in \mathbf{N}^*$ est premier si et seulement si $S(n) = n + 1$.
2. Soit p un nombre premier et $k \in \mathbf{N}^*$. Calculer $S(p^k)$.
3. Soient $a, b \in \mathbf{N}^*$ deux entiers **premiers entre eux**. On note alors $f : \left| \begin{array}{ccc} \mathcal{D}(a) \times \mathcal{D}(b) & \longrightarrow & \mathbf{N} \\ (u, v) & \longmapsto & uv \end{array} \right.$.
   a. Montrer que f est à valeurs dans $\mathcal{D}(ab)$.
   b. Soit $d \in \mathcal{D}(ab)$. Montrer qu'il existe $(u, v) \in \mathcal{D}(a) \times \mathcal{D}(b)$ tels que $d = uv$. *Indication : on pourra s'intéresser à $u = d \wedge a$.*
   c. Soient $u_1, u_2 \in \mathcal{D}(a), v_1, v_2 \in \mathcal{D}(b)$ tels que $u_1 v_1 = u_2 v_2$.
   Justifier que $u_1 \wedge v_2 = 1$, puis en déduire que $(u_1, v_1) = (u_2, v_2)$.
   d. Justifier alors que f réalise une bijection de $\mathcal{D}(a) \times \mathcal{D}(b)$ dans $\mathcal{D}(ab)$.
   e. En déduire que $S(ab) = S(a)S(b)$ (on dit que f est multiplicative).

Partie II. Nombres premiers de Mersenne

4. Soient a, n deux entiers supérieurs ou égaux à 2 tels que $a^n - 1$ est premier.
   a. Montrer que $a = 2$.
   b. Prouver que n est premier.

Inversement, il n'est pas vrai que pour p premier, $2^p - 1$ soit premier, le plus petit contre-exemple étant $2^{11} - 1 = 23 \times 89$.
On appelle $n^{ème}$ nombre de Mersenne l'entier $2^{p_n} - 1$ où p_n est le $n^{ème}$ nombre premier.
On ne sait pas s'il existe une infinité de nombres de Mersenne premiers, et pour l'instant on n'en connaît que 52, le plus grand étant $2^{136\,279\,841} - 1$ (qui a 41 024 320 chiffres), dont la primalité a été prouvée il y a quelques mois.

Partie III. Nombres parfaits pairs

L'objectif de cette partie est de prouver qu'un entier pair n est parfait si et seulement si il existe $p \in \mathbf{N}^*$ tel que $2^p - 1$ soit premier et $n = 2^{p-1}(2^p - 1)$.

5. Soit $p \in \mathbf{N}^*$ tel que $2^p - 1$ soit un nombre premier. Montrer que $2^{p-1}(2^p - 1)$ est un nombre parfait, et qu'il est pair.
6. Soit n un nombre parfait pair.
   a. Prouver qu'il existe $a, k \in \mathbf{N}^*$, avec k impair supérieur ou égal à 3 tel que $n = 2^a k$.
   b. Montrer que $2^{a+1} - 1$ divise k. On note alors $d \in \mathbf{N}^*$ tel que $k = (2^{a+1} - 1)d$.
   c. Prouver que $S(k) = k + d$.
   d. En raisonnant par l'absurde, prouver que $d = 1$, puis que k est premier.
   e. En déduire qu'il existe un nombre premier p tel que $n = 2^{p-1}(2^p - 1)$ et que $2^p - 1$ soit premier.
7. Donner les quatre plus petits nombres parfaits pairs.

On sait très peu de choses au sujet des nombres parfaits impairs. Au point qu'on ne sait même pas s'il en existe ! En revanche, on sait que s'il en existe, ils sont supérieurs à 10^{1500}, et qu'ils doivent avoir au moins 10 facteurs premiers distincts.

▸ Exercice 2 : fonctions uniformément continues

Soit I un intervalle de $\mathbf{R}$, et soit $f : I \to \mathbf{R}$. On dit que f est uniformément continue sur I si :

$$\forall \varepsilon > 0,\ \exists \eta > 0, \forall x, y \in I, |x - y| < \eta \Rightarrow |f(x) - f(y)| < \varepsilon.$$

Partie I. Généralités et caractérisation séquentielle de la continuité uniforme

1. Soit f la fonction définie sur $[1, +\infty[$ par : $\forall x \in [1, +\infty[,\ f(x) = \sqrt{x}$.
   a. Montrer que $\forall x, y \in [1, +\infty[,\ |f(x) - f(y)| \leqslant \frac{1}{2}|x - y|$.
   b. En déduire que f est uniformément continue sur $[1, +\infty[$.
2. Prouver qu'une fonction f uniformément continue sur un intervalle I est continue sur I.
3. Soit $f : I \to \mathbf{R}$ uniformément continue sur I.
   a. Justifier que si (x_n), (y_n) sont deux suites à valeurs dans I telles que $x_n - y_n \underset{n\to+\infty}{\longrightarrow} 0$, alors $f(x_n) - f(y_n) \underset{n\to+\infty}{\longrightarrow} 0$.
   b. En déduire que si $(x_n) \in I^{\mathbf{N}}$ est convergente, alors $f(x_{n+1}) - f(x_n) \underset{n\to+\infty}{\longrightarrow} 0$.
   c. La fonction $f : \left| \begin{array}{ccc}]0,1] & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \frac{1}{x} \end{array} \right.$ est-elle uniformément continue sur $]0, 1]$?

Partie II. Fonctions uniformément continues sur un intervalle borné.

Dans cette partie, on considère deux réels $a < b$ et on note $I = [a, b[$.

4. Soit $f : I \to \mathbf{R}$ une fonction continue.
   a. Montrer que si f n'est pas majorée sur $[a, b[$, alors pour tout $c \in [a, b[$, f n'est pas majorée sur $[c, b[$.
   b. Prouver que si f n'est pas majorée sur I, alors il existe une suite croissante $(x_n) \in I^{\mathbf{N}}$ telle que pour tout $n \in \mathbf{N}$, $f(x_{n+1}) - f(x_n) \geqslant 1$. Montrer qu'une telle suite converge nécessairement vers b.
   c. En déduire que si f est uniformément continue sur I, alors elle est bornée.
5. On suppose à présent que f est uniformément continue sur I.
   a. Montrer qu'il existe une suite (y_n) convergeant vers b telle que la suite $(f(y_n))$ converge. On note $\ell = \lim\limits_{n\to+\infty} f(y_n)$.
   b. Prouver alors que pour toute suite (x_n) convergeant vers b, $f(x_n) \underset{n\to+\infty}{\longrightarrow} \ell$.
   c. Montrer que f est prolongeable en une fonction continue sur $[a, b]$. Ce prolongement est-il encore uniformément continu ?

▸ Exercice 3 : l'anneau $\mathbf{Z}\left[\sqrt{7}\right]$ et une équation de Pell-Fermat

On admettra dans la suite l'irrationnalité de $\sqrt{7}$.
On note $\mathbf{Z}[\sqrt{7}] = \left\{a + b\sqrt{7},\ (a,b) \in \mathbf{Z}^2\right\}$.

Partie I. L'anneau $\mathbf{Z}[\sqrt{7}]$.

1. Prouver que pour tout élément x de $\mathbf{Z}[\sqrt{7}]$, il existe un unique couple $(a,b) \in \mathbf{Z}^2$ tel que $x = a + b\sqrt{7}$.
2. Montrer que $\mathbf{Z}[\sqrt{7}]$, muni de l'addition et de la multiplication usuelles des réels est un sous-anneau de $\mathbf{R}$. Est-ce un corps ?
3. Soit $f : \left|\begin{array}{ccc} \mathbf{Z}[\sqrt{7}] & \longrightarrow & \mathcal{M}_2(\mathbf{R}) \\ a + b\sqrt{7} & \longmapsto & \begin{pmatrix} a & 7b \\ b & a \end{pmatrix} \end{array}\right.$.
   Montrer que f est un morphisme injectif d'anneaux de $(\mathbf{Z}[\sqrt{7}], +, \times)$ dans $\mathcal{M}_2(\mathbf{R})$ muni de sa structure usuelle d'anneau.
4. Pour $x \in \mathbf{Z}[\sqrt{7}]$, on note $N(x) = \det(f(x))$ (*la norme de x*).
   a. Prouver que $\forall (x,x') \in \mathbf{Z}[\sqrt{7}]^2,\ N(xx') = N(x)N(x')$.
   b. En déduire qu'un élément $x \in \mathbf{Z}[\sqrt{7}]$ est inversible dans $\mathbf{Z}[\sqrt{7}]$ si et seulement si $N(x) = 1$ ou $N(x) = -1$.

Partie II. Structure du groupe des unités de $\mathbf{Z}[\sqrt{7}]$ et équations de Pell-Fermat.
Dans la suite, on note G le groupe (multiplicatif) des unités de $\mathbf{Z}[\sqrt{7}]$, c'est-à-dire $G = \mathbf{Z}[\sqrt{7}]^\times$.
Il est évident que 1 et -1 sont dans G.

5. Vérifier que $8 + 3\sqrt{7} \in G$, et en déduire que $G \neq \{-1, 1\}$.
6. Soit $x = (a + b\sqrt{7}) \in G$. Montrer que $x \geqslant 1 \Rightarrow (a \geqslant 1$ **et** $b \geqslant 0)$. *Indication : comparer $\frac{1}{x}$ et x.*
7. Soit $M \in \mathbf{N}^*$. En utilisant la question précédente, prouver que $G \cap [1, M]$ est fini.
8. En déduire que $G \cap]1, +\infty[$ possède un plus petit élément u.
9. Soit $v \in G \cap]1, +\infty[$.
   a. Justifier qu'il existe un unique $k \in \mathbf{N}$ tel que $u^k \leqslant v < u^{k+1}$.
   b. Montrer que si k est comme dans la question précédente, alors $v = u^k$.
   c. En déduire que $G \cap \mathbf{R}_+^* = \langle u \rangle = \left\{u^k, k \in \mathbf{Z}\right\}$.
10. Montrer que $f : \left|\begin{array}{ccc} \{-1,1\} \times \mathbf{Z} & \longrightarrow & G \\ (\varepsilon, k) & \longmapsto & \varepsilon u^k \end{array}\right.$ est un isomorphisme de groupes où $\{-1,1\} \times \mathbf{Z}$ est muni de la structure de produit direct des deux groupes $(\{-1,1\}, \times)$ et $(\mathbf{Z}, +)$.
11. **Équations de Pell-Fermat**
    a. Montrer que l'équation $x^2 - 7y^2 = 1$, d'inconnue $(x,y) \in \mathbf{Z}^2$ possède une infinité de solutions. Donner deux telles solutions avec $x, y \in \mathbf{N}^*$.
    b. En admettant que $8 + 7\sqrt{3}$ est le plus petit élément de $G \cap]1, +\infty[$, déterminer le nombre de solutions de l'équation $x^2 - 7y^2 = -1$, d'inconnue $(x,y) \in \mathbf{Z}^2$.

CORRECTION DU DEVOIR SURVEILLÉ 6

▸ Exercice 1 : nombres de Mersenne et nombres parfaits

Partie I. La fonction somme des diviseurs.

1. Il est clair que $S(1) = 1 \neq 1+1$.
Un entier $n \geqslant 2$ est premier si et seulement si $\mathcal{D}(n) = \{1, n\}$, et si c'est le cas, $S(n) = n+1$.
Et en revanche, si n n'est pas premier, alors il existe $d \in \mathcal{D}(n) \setminus \{1, n\}$ et donc $S(n) \geqslant 1 + d + n > n+1$.
Donc $\boxed{n \text{ est premier si et seulement si } S(n) = n+1.}$

2. On a $\mathcal{D}(p^k) = \{1, p, p^2, \dots, p^k\} = \{p^\ell,\ \ell \in [\![0, k]\!]\}$.
Et donc

$$S\left(p^k\right) = \sum_{\ell=0}^{k} p^\ell = \frac{p^{k+1}-1}{p-1}.$$

Détails
Somme des termes d'une suite géométrique de raison $p \neq 1$.

3.a. Soit u un diviseur de a et v un diviseur de b. Alors il existe $d_1, d_2 \in \mathbf{N}$ tel que $a = ud_1$ et $b = vd_2$.
Et donc $ab = ud_1vd_2 = uvd_1d_2$, de sorte que $uv \in \mathcal{D}(ab)$.
Ainsi $\boxed{f \text{ est bien à valeurs dans } \mathcal{D}(ab).}$

3.b. Comme indiqué, notons $u = d \wedge a$, de sorte que $u \in \mathcal{D}(a)$.
Alors il existe $v \in \mathbf{N}$, premier à a tel que $d = uv$.
Puisque $v \mid d$ et que $d \mid ab$, $v \mid ab$. Puisque de plus $a \wedge v = 1$, alors par le lemme de Gauss, $v \mid b$.
Et donc $v \in \mathcal{D}(b)$, et on a $\boxed{d = uv.}$

3.c. Rappelons qu'un entier est premier à un produit si et seulement si il est premier à chacun des facteurs.
Donc ici, puisque $u_1 \mid a$ et que b est premier à a, alors b est premier avec u_1.
Et par le même argument, u_1 est donc premier avec tout diviseur de b, et en particulier avec v_2.

Détails
On a $a = ku_1$, et puisque b est premier avec a, il est premier avec u_1 et avec k (cette seconde information nous étant totalement inutile dans la suite).

Or $u_1v_1 = u_2v_2$, si bien que u_1 divise u_2v_2, et donc par le lemme de Gauss, u_1 divise u_2.
Puisque sur le même principe, $u_2 \mid u_1$, et que u_1, u_2 sont dans $\mathbf{N}$, alors $\boxed{u_1 = u_2.}$
Et donc nécessairement $\boxed{v_1 = v_2.}$

3.d. La question 3.b. prouve la surjectivité de f, la question 3.c. prouve sont injectivité.

3.e. On a donc

$$S(ab) = \sum_{w \in \mathcal{D}(ab)} w = \sum_{(u,v) \in \mathcal{D}(a) \times \mathcal{D}(b)} (uv) = \sum_{u \in \mathcal{D}(a)} \sum_{v \in \mathcal{D}(b)} uv = \left(\sum_{u \in \mathcal{D}(a)} u\right)\left(\sum_{v \in \mathcal{D}(b)} v\right) = \boxed{S(a)S(b).}$$

⚠ Attention !
Cette formule ne vaut que pour a, b premiers entre eux.

Partie II. Nombres premiers de Mersenne

4.a. On a $a^n - 1 = (a-1)\sum_{k=0}^{n-1} a^k$.

Or il est clair[1] que $\sum_{k=0}^{n-1} a^k \geqslant a \geqslant 2$.

Puisque $a^n - 1$ est premier, on a donc $a - 1 = 1$, si bien que $\boxed{a = 2.}$

[1] Car $n \geqslant 2$, et donc que le terme $k = 1$ figure bien dans la somme.

4.b. Prouvons que si n est composé, alors $2^n - 1$ n'est pas premier, ce qui par contraposée prouvera bien que si $2^n - 1$ est premier, alors n est premier.

Si n est composé, il existe alors $u, v \geqslant 2$ tels que $n = uv$.
Et alors

$$2^n - 1 = 2^{uv} - 1 = (2^u)^v - 1^v = (2^u - 1)\sum_{k=0}^{v-1} 2^{ku}.$$

Puisque $u \geqslant 2$, alors $2^u - 1 \geqslant 1$. Et puisque $v \geqslant 2$, $\sum_{k=0}^{v-1} 2^{ku} \geqslant 2^u \geqslant 2$.

Ainsi, $2^u - 1$ est un diviseur de $2^n - 1$ avec $1 < 2^n - 1 < 2^n - 1$, si bien que $2^n - 1$ n'est pas premier.

Et donc si $2^n - 1$ est premier, alors n est premier.

> **Remarque**
> Il est bon de préciser que $v \geqslant 2$, car pour $v = 1$, la somme ne comporterait qu'un unique terme, égal à 1.

Partie III. Nombres parfaits pairs

5. Puisque 2^{p-1} (qui a 2 comme seul facteur premier) et $2^p - 1$ (qui est impair) sont premiers entre eux, on a donc par la formule de la question 3,

$$S\left(2^{p-1}\left(2^p-1\right)\right) = S\left(2^{p-1}\right) S\left(2^p-1\right).$$

Mais $2^p - 1$ étant premier, $S(2^p-1) = 2^p - 1 + 1 = 2^p$ et par la question 2, $S\left(2^{p-1}\right) = 2^p - 1$.

Ainsi, $S\left(2^{p-1}(2^p-1)\right) = 2^p(2^p-1) = 2\times 2^{p-1}(2^p-1)$, si bien que $2^{p-1}\left(2^p-1\right)$ est parfait.

Il est pair car p étant premier, $p - 1 \geqslant 1$, et donc 2^{p-1} est pair.

6.a. Par la question 2, 2^k n'est jamais un nombre parfait car $S\left(2^k\right) = 2^{k+1} - 1 \neq 2 \times 2^k$.

Et donc n possède au moins un facteur premier impair, si bien que si on note $a = v_2(n)$ et $k = \prod_{\substack{p \text{ premier} \\ p \text{impair}}} p^{v_p(n)}$, alors k est impair supérieur ou égal à 3, et $n = 2^a k$.

6.b. On a donc $S(n) = 2n = 2^{a+1}k$, et puisque 2^a et k sont premiers entre eux[2], alors $S(n) = S\left(2^a\right) S(k)$.

Mais par la question 2, $S\left(2^a\right) = \dfrac{2^{a+1}-1}{2-1} = 2^{a+1} - 1$.

Et puisque $S(k)$ est entier, $2^{a+1} - 1$ divise $2^{a+1}k$.

Mais $2^{a+1} - 1$ et 2^{a+1} sont premiers entre eux[3], donc par le lemme de Gauss, $2^{a+1} - 1$ divise k.

[2] Toujours car 2^k a 2 pour unique facteur premier, et que 2 ne divise pas k.

[3] Deux entiers consécutifs sont toujours premiers entre eux, c'est une conséquence de Bézout.

6.c. On a donc $S(n) = (2^{a+1} - 1)S(k)$, et puisque n est parfait,

$$S(n) = 2n = 2^{a+1}k = 2^{a+1}(2^{a+1} - 1)d.$$

Et donc $S(k) = 2^{a+1}d = \left(2^{a+1} - 1\right) d + d = k + d.$

6.d. Si on avait $d > 1$, alors $1, d$ et k seraient trois diviseurs distincts de k, de sorte que

$$S(k) \geqslant 1 + d + k > k + d.$$

Donc nécessairement $d = 1$.

Et alors $S(k) = k + 1$, si bien que par la question 1, k est un nombre premier.

6.e. Puisque $d = 1$, on a donc prouvé que $n = 2^a\left(2^{a+1} - 1\right)$.

Mais de plus, $2^{a+1} - 1$ est premier si bien que par la partie II, $a + 1$ est un nombre premier p. Et alors $a = p - 1$, si bien que $n = 2^{p-1}\left(2^p - 1\right)$, où $2^p - 1$ est premier.

7. La question précédente nous dit donc qu'à chaque nombre de Mersenne premier correspond un et un seul nombre parfait pair.

Notons que l'application $p \mapsto 2^{p-1}(2^p - 1)$ est strictement croissante sur $\mathbf{N}$, de sorte qu'il s'agit de trouver les trois plus petits nombres premiers de Mersenne.

Les premiers nombres de Mersenne sont $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ et $2^7 - 1 = 127$ qui sont tous quatre premiers.

Les premiers nombres parfaits pairs sont donc

$$2^{2-1}(2^2 - 1) = 6, 2^{3-1}(2^3 - 1) = 28, 2^{5-1}(2^5 - 1) = 496 \text{ et } 2^6\left(2^7 - 1\right) = 64 \times 127 = 8\,128.$$

> **127 ∈ P ?**
> Pour vérifier si 127 est premier, il suffit de vérifier qu'il n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{127} < 12$, ce qui se vérifie aisément.

▸ Exercice 2 : fonctions uniformément continues

1.a. Soient $x, y \in [1, +\infty[$. Quitte à échanger x et y, on peut supposer que $x \leqslant y$, si bien que $|f(x) - f(y)| = \sqrt{y} - \sqrt{x}$ et $|x - y| = y - x$.

Il s'agit donc de prouver que $\sqrt{y}-\sqrt{x} \leqslant \frac{1}{2}(y-x)$, soit encore $2\sqrt{y}-y \leqslant 2\sqrt{x}-x$. Mais la fonction $\varphi : t \mapsto 2\sqrt{t}-t$ est dérivable sur $[1,+\infty[$, de dérivée $t \mapsto \frac{1}{\sqrt{t}}-1 \leqslant 0$.
Donc φ est décroissante, si bien que $\varphi(y) \leqslant \varphi(x)$, ce qui est bien l'inégalité souhaitée.
Ainsi, $\boxed{\text{pour tous } x,y \in [1,+\infty[,\ |f(x)-f(y)| \leqslant \frac{1}{2}|x-y|.}$

1.b. Soit $\varepsilon > 0$, et soit $\eta = 2\varepsilon > 0$. Alors pour tous $x,y \in [1,+\infty[$, si $|x-y| < \eta$, alors $|f(x)-f(y)| \leqslant \frac{1}{2}\eta = \varepsilon$.
Ainsi, $\boxed{f \text{ est uniformément continue sur } [1,+\infty[.}$

2. Pour avoir les idées claires, réécrivons la définition de la continuité de f.
f est continue si et seulement si elle continue en tout $a \in I$, c'est-à-dire si et seulement si

$$\forall a \in I,\ \forall \varepsilon > 0, \exists \eta > 0, \forall x \in I, |x-a| < \eta \Rightarrow |f(x)-f(a)| < \varepsilon.$$

Par ailleurs, la définition de la continuité uniforme est la suivante :

$$\forall \varepsilon > 0, \exists \eta > 0,\ \forall a,x \in I, |x-a| < \eta \Rightarrow |f(x)-f(a)| < \varepsilon.$$

Vous constaterez que ce sont les mêmes... si ce n'est que le $\forall a \in I$ a changé de place.

Fixons donc $a \in I$, et soit $\varepsilon > 0$.
Considérons alors un $\eta > 0$ tel que pour tout $x,y \in I$, $|x-y| < \eta \Rightarrow |f(x)-f(y)| < \varepsilon$.
Alors en particulier[4], pour tout $x \in I$, si $|x-a| < \eta$, alors $|f(x)-f(a)| < \varepsilon$.
Ainsi, f est continue en a, et ceci étant vrai pour tout $a \in I$, $\boxed{f \text{ est continue sur } I.}$

Intuition
S'il y a un η qui marche pour tous x, y, il marche en particulier pour $y = a$.

[4] En prenant $y = a$.

3.a. Soient donc $(x_n),(y_n) \in I^{\mathbf{N}}$ deux suites telles que $x_n - y_n \underset{n\to+\infty}{\longrightarrow} 0$.
Soit alors $\varepsilon > 0$, et considérons un $\eta > 0$ tel que $\forall x,y \in I, |x-y| < \eta \Rightarrow |f(x)-f(y)| < \varepsilon$.
Soit alors $n_0 \in \mathbf{N}$ tel que pour $n \geqslant n_0$, $|x_n - y_n| < \eta$. Notons qu'un tel n_0 existe puisque $x_n - y_n \underset{n\to+\infty}{\longrightarrow} 0$.
Alors pour $n \geqslant n_0$, puisque $x_n, y_n \in I$ et que $|x_n - y_n| < \eta$, alors $|f(x_n)-f(y_n)| < \varepsilon$.
Et donc nous venons de prouver que $\forall \varepsilon > 0,\ \exists n_0 \in \mathbf{N}, \forall n \geqslant n_0,\ |f(x_n)-f(y_n)| < \varepsilon$.
C'est la définition de $\boxed{f(x_n)-f(y_n) \underset{n\to+\infty}{\longrightarrow} 0.}$

Remarque
Un tel η existe par définition de l'uniforme continuité.

3.b. Si $(x_n) \in I^{\mathbf{N}}$ est convergente de limite ℓ, alors $x_{n+1} \underset{n\to+\infty}{\longrightarrow} \ell$ et donc $x_{n+1} - x_n \underset{n\to+\infty}{\longrightarrow} \ell - \ell = 0$.

Donc par la question précédente, appliquée avec $y_n = x_{n+1}$, $\boxed{f(x_{n+1})-f(x_n) \underset{n\to+\infty}{\longrightarrow} 0.}$

⚠ Attention !
Ce n'est pas une équivalence : on peut avoir

$$x_{n+1} - x_n \underset{n\to+\infty}{\longrightarrow} 0$$

sans que (x_n) converge.
C'est par exemple le cas pour $x_n = \ln(n)$.

3.c. Pour tout $n \in \mathbf{N}$, posons $x_n = \frac{1}{n+1}$. Alors (x_n) est à valeurs dans I, convergente (vers 0) et pourtant $f(x_{n+1}) - f(x_n) = n+1-n = 1$ ne tend pas vers 0.
Donc $\boxed{f \text{ n'est pas uniformément continue sur }]0,1].}$

Partie II. Fonctions uniformément continues sur un intervalle borné.

4.a. Soit $c \in [a,b]$. Puisque f est continue sur le segment $[a,c]$, par le théorème des bornes atteintes, elle y est bornée. Soit donc $M_1 \in \mathbf{R}$ tel que $\forall x \in [a,c]$, $|f(x)| \leqslant M_1$.

Si f est majorée sur $[c,b[$, soit M_2 tel que pour tout $x \in [c,b[$, $f(x) \leqslant M_2$, alors pour tout $x \in [a,b[$, on a $f(x) \leqslant \max(M_1,M_2)$, et donc f est majorée sur $[a,b[$.
Par contraposée, $\boxed{\text{si } f \text{ n'est pas majorée sur } [a,b[, \text{ alors elle n'est pas majorée sur } [c,b[.}$

4.b. Construisons une telle suite par récurrence, en posant $x_0 = a$.
Puisque f n'est pas majorée, $f(a)+1$ n'est pas un majorant de f, et donc il existe $x_1 \geqslant a$ tel que $f(x_1) \geqslant 1 + f(a)$, et donc $f(x_1) - f(x_0) \geqslant 1$.
Soit $n \in \mathbf{N}$ tel qu'on ait déjà construit $x_0 \leqslant x_1 \leqslant \ldots \leqslant x_n$ vérifiant : $\forall i \in [\![0,n-1]\!]$, $f(x_{i+1}) - f(x_i) \geqslant 1$.
Puisque f n'est pas majorée sur $[a,b[$, elle ne l'est pas non plus sur $[x_n,b[$, et donc $f(x_n)+1$ n'est pas un majorant de f sur $[x_n,b[$. Par conséquent, il existe un réel $t \in [x_n,b[$ tel que $f(t) \geqslant f(x_n)+1$.
Si on choisit pour x_{n+1} un tel réel t, on a alors $x_{n+1} \geqslant x_n$ et $f(x_{n+1}) - f(x_n) \geqslant 1$.

Par récurrence, on construit donc bien une suite (x_n) croissante, à valeurs dans I et telle que $\forall n \in \mathbf{N}, f(x_{n+1}) - f(x_n) \geqslant 1$.
Une telle suite (x_n) étant croissante et majorée par b, par le théorème de la limite monotone, elle converge vers un réel $\ell \in [a,b]$.
Supposons par l'absurde que $\ell \neq b$, de sorte que $\ell \in I$.
Alors par continuité de f en ℓ, $f(x_n) \underset{n\to+\infty}{\longrightarrow} f(\ell)$, si bien que

$$f(x_{n+1}) - f(x_n) \underset{n\to+\infty}{\longrightarrow} f(\ell) - f(\ell) = 0.$$

Mais pour tout $n \in \mathbf{N}$, $f(x_{n+1}) - f(x_n) \geqslant 1$, et donc par passage à la limite dans l'inégalité, $0 \geqslant 1$ ce qui est absurde.
On en déduit donc que $\boxed{x_n \underset{n\to+\infty}{\longrightarrow} b.}$

Détails
$\forall n \in \mathbf{N}, a \leqslant x_n < b$, et donc par passage à la limite $a \leqslant \ell \leqslant b$.

4.c. Si f n'était pas majorée, prenons une suite comme à la question précédente. Alors (x_n) converge, si bien que par la question 3, $f(x_{n+1}) - f(x_n) \underset{n\to+\infty}{\longrightarrow} 0$, ce qui n'est pas le cas comme expliqué ci-dessus. D'où une contradiction.
On en déduit donc que f est majorée sur I.

Et en changeant f en $-f$ (qui est encore uniformément continue car pour tout $x, y \in I$, $|(-f)(x) - (-f)(y)| = |f(x) - f(y)|$), on montre de même que $-f$ est majorée, et donc f est minorée.
Et par conséquent, $\boxed{f \text{ est bornée sur } I.}$

Alternative
En utilisant l'inégalité triangulaire renversée, on prouve que si f est uniformément continue, alors $|f|$ l'est aussi puisque

$$||f(x)| - |f(y)|| \leqslant |f(x) - f(y)|.$$

Et donc $|f|$ est majorée, si bien que f est bornée.

5.a. Prenons pour (x_n) une suite croissante convergeant vers b.
Par exemple on peut prendre $x_n = b - \frac{b-a}{n+1}$, qui est bien dans $[a,b]$.
Alors la suite $(f(x_n))$ étant bornée par la question précédente, on peut lui appliquer le théorème de Bolzano-Weierstrass : il existe une extractrice φ telle que $\left(f(x_{\varphi(n)})\right)_n$ converge.
Puisque (x_n) converge vers b, il en est de même de $(x_{\varphi(n)})$, et donc en posant $y_n = x_{\varphi(n)}$, on a bien $y_n \underset{n\to+\infty}{\longrightarrow} b$ et $(f(y_n))$ qui converge.

5.b. C'est la question 3.a, qui s'applique car f est uniformément continue : si $(x_n) \in I^{\mathbf{N}}$ converge vers b, alors $x_n - y_n \underset{n\to+\infty}{\longrightarrow} 0$, si bien que $f(x_n) - f(y_n) \underset{n\to+\infty}{\longrightarrow} 0$.
Et donc $f(x_n) = f(y_n) + f(x_n) - f(y_n) \underset{n\to+\infty}{\longrightarrow} \ell + 0 = \ell$.

5.c. Nous venons de prouver que pour toute suite $(x_n) \in I^{\mathbf{N}}$ de limite b, $f(x_n) \underset{n\to+\infty}{\longrightarrow} \ell$.
C'est la caractérisation séquentielle de $\lim_{x\to b} f(x) = \ell$.
Puisque $\ell \in \mathbf{R}$, on a donc bien prouvé que f possède une limite finie en b, et donc est $\boxed{\text{prolongeable par continuité en } b.}$

Notons donc $\tilde{f} : \left| \begin{array}{ccc} [a,b] & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \begin{cases} f(x) & \text{si } x < b \\ \ell & \text{si } x = b \end{cases} \end{array} \right.$ le prolongement par continuité de f à $[a,b]$.

Nous savons que f est continue, il s'agit de prouver qu'elle est uniformément continue.
Soit donc $\varepsilon > 0$ et soit $\eta_1 > 0$ tel que pour tout $x, y \in [a,b[$, $|x-y| < \eta_1 \Rightarrow |f(x)-f(y)| < \varepsilon$.
Soit également $\eta_2 > 0$ tel que pour tout $x \in [a,b[$, $|x-b| < \eta_2 \Rightarrow |f(x) - \ell| < \varepsilon$.
Posons alors $\eta = \min(\eta_1, \eta_2)$, et considérons deux réels $x, y \in [a,b]$.

- Si $x < b$ et $y < b$, alors $|x-y| < \eta \leqslant \eta_1$, et donc $|\tilde{f}(x) - \tilde{f}(y)| = |f(x) - f(y)| < \varepsilon$.
- Si $x = y = b$, alors $|\tilde{f}(x) - \tilde{f}(y)| = |\ell - \ell| = 0 < \varepsilon$.
- Si $x < b$ et $y = b$, alors $|x-b| < \eta \leqslant \eta_2$ et donc $|\tilde{f}(x) - \tilde{f}(y)| = |f(x) - \ell| < \varepsilon$.

Et donc nous venons bien de prouver que

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x, y \in [a,b]\ |x-y| < \eta \Rightarrow |\tilde{f}(x) - \tilde{f}(y)| < \varepsilon.$$

C'est donc que $\boxed{\tilde{f} \text{ est uniformément continue sur } [a,b].}$

▸ Exercice 3 : l'anneau $\mathbf{Z}[\sqrt{7}]$ et une équation de Pell-Fermat.

Partie I. L'anneau $\mathbf{Z}[\sqrt{7}]$

1. L'existence d'un tel couple relève directement de la définition de $\mathbf{Z}[\sqrt{7}]$, il s'agit donc surtout de prouver l'unicité.
Soient a_1, a_2, b_1, b_2 des entiers tels que $a_1 + b_1\sqrt{7} = a_2 + b_2\sqrt{7} \Leftrightarrow (b_1 - b_2)\sqrt{7} = a_2 - a_1$.
Si $b_1 \neq b_2$, alors $\sqrt{7} = \dfrac{a_2 - a_1}{b_1 - b_2} \in \mathbf{Q}$, ce qui est absurde.
Donc $b_1 = b_2$, et donc $a_1 = a_2$.
Ainsi, tout élément de $\mathbf{Z}[\sqrt{7}]$ s'écrit bien de manière unique sous la forme $a + b\sqrt{7}$, $(a, b) \in \mathbf{Z}^2$.

2. Le neutre multiplicatif de $\mathbf{R}$ est $1 = 1 + 0\sqrt{7} \in \mathbf{Z}[\sqrt{7}]$.
Soient $x, y \in \mathbf{Z}[\sqrt{7}]$, et soient $a_1, b_1, a_2, b_2 \in \mathbf{Z}$ tels que $x = a_1 + b_1\sqrt{7}$ et $y = a_2 + b_2\sqrt{7}$.
Alors $x - y = \underbrace{(a_1 - a_2)}_{\in\mathbf{Z}} + \underbrace{(b_1 - b_2)}_{\in\mathbf{Z}}\sqrt{7} \in \mathbf{Z}[\sqrt{7}]$.
Enfin, $xy = (a_1 + b_1\sqrt{7})(a_2 + b_2\sqrt{7}) = \underbrace{a_1a_2 + 7b_1b_2}_{\in\mathbf{Z}} + \underbrace{(a_1b_2 + a_2b_1)}_{\in\mathbf{Z}}\sqrt{7} \in \mathbf{Z}[\sqrt{7}]$.
Et donc $\mathbf{Z}[\sqrt{7}]$ est bien un sous-anneau de $\mathbf{R}$.

> **Remarque**
> À ce stade, $\mathbf{Z}[\sqrt{7}]$ est un sous-groupe de $(\mathbf{R}, +)$.

> **En particulier**
> Et donc on a notamment $\mathbf{Z}[\sqrt{7}]$ qui est un anneau commutatif.

Si $\mathbf{Z}[\sqrt{7}]$ était un corps, alors 2 serait inversible dans $\mathbf{Z}[\sqrt{7}]$, et donc il existerait $a, b \in \mathbf{Z}$ tels que $\frac{1}{2} = a + b\sqrt{7}$, soit encore $(2a - 1) + 2b\sqrt{7} = 0$.
Par la question 1, ceci implique que $b = 0$ et $2a - 1 = 0$, ce qui n'est pas possible dans $\mathbf{Z}$.
Donc 2 n'est pas inversible dans $\mathbf{Z}[\sqrt{7}]$, qui n'est donc pas un corps.

3. Notons que l'unicité de la question précédente garantit que f est bien définie, de manière non ambiguë.
On a alors $f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.
Soient $x, y \in \mathbf{Z}[\sqrt{7}]$, avec comme précédemment $x = a_1 + b_1\sqrt{7}$ et $y = a_2 + b_2\sqrt{7}$. Alors

$$f(x+y) = f\left((a_1 + a_2) + (b_1 + b_2)\sqrt{7}\right) = \begin{pmatrix} a_1 + a_2 & 7(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix} = \begin{pmatrix} a_1 & 7b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & 7b_2 \\ b_2 & a_2 \end{pmatrix} = f(x) + f(y).$$

$$f(x)f(y) = \begin{pmatrix} a_1 & 7b_1 \\ b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & 7b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + 7b_1b_2 & 7(a_1b_2 + a_2b_1) \\ a_1b_2 + a_2b_1 & a_1a_2 + 7b_1b_2 \end{pmatrix} = f\left((a_1a_2 + 7b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{7}\right) = f(xy).$$

Donc f est bien un morphisme d'anneaux.
Pour l'injectivité, on peut utiliser son noyau[5], mais tout simplement, avec les notations précédentes, on a, par unicité des coefficients d'une matrice

$$f(x) = f(y) \Leftrightarrow \begin{pmatrix} a_1 & 7b_1 \\ b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & 7b_2 \\ b_2 & a_2 \end{pmatrix} \Leftrightarrow \begin{cases} a_1 = a_2 \\ b_1 = b_2 \\ 7b_1 = 7b_2 \end{cases} \Leftrightarrow x = y.$$

Donc f est injectif.

[5] Rappelons qu'un morphisme d'anneaux est aussi un morphisme de groupes.

4. Notons que pour $x = a + b\sqrt{7} \in \mathbf{Z}[\sqrt{7}]$, on a donc $N(x) = \det\begin{pmatrix} a & 7b \\ b & a \end{pmatrix} = a^2 - 7b^2$. En particulier, $N(x) \in \mathbf{Z}$.

4.a. Soient $x, x' \in \mathbf{Z}[\sqrt{7}]$. Alors puisque f est un morphisme d'anneaux, et que le déterminant d'un produit de matrices 2×2 est le produit des déterminants, on a

$$N(xx') = \det(f(xx')) = \det(f(x)f(x')) = \det(f(x))\det(f(x')) = N(x)N(x').$$

4.b. Soit $x \in \mathbf{Z}[\sqrt{7}]$, inversible. Soit alors $x' \in \mathbf{Z}[\sqrt{7}]$ son inverse.
On a donc $N(1) = N(x)N(x')$. Mais $N(1) = \det I_2 = 1$, et $N(x)$ et $N(x')$ sont deux entiers, donc il s'agit d'inversibles de l'anneau $\mathbf{Z}$.

Or dans $\mathbf{Z}$, les seuls éléments inversibles sont 1 et -1, donc $N(x) = \pm 1$.

Inversement, si $x = a + b\sqrt{7}$ est tel que $|N(x)| = 1$. Alors $x \neq 0$ (car $N(0) = 0$), et donc x est inversible dans l'anneau $\mathbf{R}$.
Son inverse est

$$\frac{1}{x} = \frac{1}{a+b\sqrt{7}} = \frac{a-b\sqrt{7}}{(a+b\sqrt{7})(a-b\sqrt{7})} = \frac{a-b\sqrt{7}}{a^2-7b^2} = \frac{a}{N(x)} + \frac{b}{N(x)}\sqrt{7} \in \mathbf{Z}[\sqrt{7}].$$

Donc x est bien inversible dans l'anneau $\mathbf{Z}[\sqrt{7}]$.

Et donc $\boxed{\text{un élément } x \in \mathbf{Z}[\sqrt{7}] \text{ est inversible si et seulement si } N(x) = \pm 1.}$

⚠ Attention !
$\frac{1}{x}$ existe toujours dans $\mathbf{R}$ pour $x \neq 0$, la question ici est de savoir si cet inverse est encore dans $\mathbf{Z}[\sqrt{7}]$.

Partie II. Structure du groupe des unités de $\mathbf{Z}[\sqrt{7}]$ et équations de Pell-Fermat.

5. On a $N(8+3\sqrt{7}) = 8^2 - 7\times 3^2 = 1$. Donc $8+3\sqrt{7} \in G$.
Et donc G contient d'autres éléments que ± 1.

6. Supposons que $x \geqslant 1$. Alors $0 < \frac{1}{x} \leqslant 1$.

► **Si $N(x) = 1$.** Alors[6] $\frac{1}{x} = a - b\sqrt{7}$. Puisque $\frac{1}{x} \leqslant x$, on a donc $a - b\sqrt{7} \leqslant a + b\sqrt{7}$, et donc $b \geqslant 0$.
Et alors $a - b\sqrt{7} > 0$, donc $a > b\sqrt{7} \geqslant 0$. Puisque $a \in \mathbf{Z}$, $a \geqslant 1$.

► Si $N(x) = -1$, alors $\frac{1}{x} = -a + b\sqrt{7}$. Puisque $\frac{1}{x} \leqslant x$, $-a + b\sqrt{7} \leqslant a + b\sqrt{7}$ et donc $a \geqslant 0$.
Et donc $b\sqrt{7} > a$, si bien que $b > 0$.

[6] C'est le calcul de 4.b.

7. Soit $x = a + b\sqrt{7} \in G \cap [1, M]$.
Par la question précédente, $a \geqslant 1$ et $b \geqslant 0$.
O en déduit donc que $1 \leqslant a \leqslant a + b\sqrt{7} \leqslant M$ et que $0 \leqslant b \leqslant b\sqrt{7} \leqslant a + b\sqrt{7} \leqslant M$.
Autrement dit, $(a, b) \in [\![1, M]\!] \times [\![0, M]\!]$. Donc il y a au plus $M(M+1)$ couples (a, b) tels que $a + b\sqrt{7} \in G \cap [1, M]$, qui est donc $\boxed{\text{fini.}}$

Remarque
Notons que notre majoration du cardinal de $G \cap [1, M]$ est très grossière, mais nous suffit pour dire qu'il est fini.

8. Nous avons déjà dit que G contient $8 + 3\sqrt{7}$. Prenons donc M un entier supérieur ou égal à $8 + 3\sqrt{7}$. Alors $G \cap]1, M]$ est non vide et fini, il possède donc un plus petit élément u.
Et alors pour tout $x \in G \cap]1, +\infty[$, soit $x \leqslant M$, et alors $u \leqslant x$, soit $x > M$, et alors $u \leqslant M \leqslant x$.
Donc $\boxed{u \text{ est le plus petit élément de } G \cap]1, +\infty[.}$

9.a. Puisque $u > 1$, $u^n \underset{n\to+\infty}{\longrightarrow} +\infty$. Et en particulier, il existe $n_0 \in \mathbf{N}$ tel que $u^{n_0} > v$.
Soit alors $A_v = \{k \in \mathbf{N} \mid u^k \leqslant v\}$. C'est une partie non vide[7] de $\mathbf{N}$, majorée par n_0 (car si $k \geqslant n_0$, $u_k \geqslant u^{n_0} > v$).
Elle admet donc un plus grand élément k. Et puisque $k \in A_v$ et $k + 1 \notin A_v$, $u^k \leqslant v < u^{k+1}$.

[7] $0 \in A_v$.

9.b. On a donc $1 \leqslant \frac{v}{u^k} < u$. Et puisque v et u^k sont deux éléments de G, qui est un groupe, $\frac{v}{u^k} = v\left(u^k\right)^{-1} \in G$.
Puisque u est le plus petit élément de $G \cap]1, +\infty[$, et que $\frac{v}{u^k} < u$, on a donc $\frac{v}{u^k} \leqslant 1$, si bien que $1 = \frac{v}{u^k} \Leftrightarrow \boxed{v = u^k.}$

9.c. Puisque $u \in \mathbf{R}_+^*$ (car $u > 1$), on a donc pour tout $k \in \mathbf{Z}$, $u^k > 0$. Et donc $\langle u \rangle \subset G \cap \mathbf{R}_+^*$.
Inversement, soit $v \in G \cap \mathbf{R}_+^*$.
► Si $v > 1$, alors par la question précédente, $v \in \{u^k,\ k \in \mathbf{N}\} \subset \langle u \rangle$.
► Si $v = 1$, alors $v = u^0 \in \langle u \rangle$.
► Si $v < 1$, alors $\frac{1}{v} > 1$, et donc par la question précédente, il existe $k \in \mathbf{N}$ tel que $\frac{1}{v} = u^k$, et donc $v = u^{-k} \in \langle u \rangle$.
Donc $\boxed{G \cap \mathbf{R}_+^* = \langle u \rangle.}$

10. Soient donc $(\varepsilon_1, k_1), (\varepsilon_2, k_2)$ deux éléments de $\{-1, 1\} \times \mathbf{Z}$. Alors

$$f\left((\varepsilon_1, k_1) \cdot (\varepsilon_2, k_2)\right) = f\left(\varepsilon_1\varepsilon_2, k_1 + k_2\right) = \varepsilon_1\varepsilon_2 u^{k_1+k_2} = \varepsilon_1 u^{k_1}\varepsilon_2 u^{k_2} = f(\varepsilon_1, k_1) f(\varepsilon_2, k_2).$$

Donc f est bien un morphisme de groupes.

Soit $(\varepsilon, k) \in \mathrm{Ker}(f)$. Alors $f(\varepsilon, k) = \varepsilon u^k = 1$.
Puisque $u^k > 0$, $\varepsilon = 1$. Et alors[8] $u^k = 1 \Leftrightarrow k = 0$.
Donc $\mathrm{Ker}\, f = \{(1,0)\}$, où $(1,0)$ est le neutre si bien que f est injectif.
Enfin, si $x \in G$, alors soit $x > 0$, et donc par la question 9.c, il existe $k \in \mathbf{Z}$ tel que $x = u^k = f(1,k)$.
Soit $x < 0$, mais alors $-x > 0$, et donc il existe $k \in \mathbf{Z}$ tel que $x = -u^k = f(-1,k)$.
Dans tous les cas, x possède un antécédent par f, qui est donc surjectif.
Et donc f est bijectif : c'est un isomorphisme de groupes.

[8] $u > 1$, donc $u^k > 1$ pour $k \geqslant 1$ et $u^k < 1$ pour $k \leqslant -1$.

11. Équations de Pell-Fermat

11.a. Notons que $(x,y) \in \mathbf{Z}^2$ est une solution de $x^2 - 7y^2 = 1$ si et seulement si $\alpha = x + y\sqrt{7}$ est tel que $N(\alpha) = 1$.

Or nous savons déjà que $N(8 + 3\sqrt{7}) = 1$, et donc $(8,3)$ est solution de l'équation.
Mais pour tout $k \in \mathbf{N}^*$, $N\left((8+3\sqrt{7})^k\right) = N(8+3\sqrt{7})^k = 1$, si bien que si on note (a_k, b_k) les entiers tels que $(8+3\sqrt{7})^k = a_k + b_k\sqrt{7}$, alors $a_k^2 - 7b_k^2 = 1$.
Et donc (a_k, b_k) est solution.

Reste à remarquer que puisque $8 + 3\sqrt{7} > 1$, la suite $\left(\left(8+3\sqrt{7}\right)^k\right)_k$ est strictement croissante, et donc injective.
Ainsi, il y a une infinité de solutions à l'équation $x^2 - 7y^2 = 1$.

Nous avons déjà dit que $(8,3)$ est l'une d'entre elles.
Et puisque $(8+3\sqrt{7})^2 = 64 + 7\times 9 + 48\sqrt{7} = 127 + 48\sqrt{3}$, alors $(127, 48)$ est une deuxième solution.

11.b. Là encore, les couples (x,y) solutions de $x^2 - 7y^2 = -1$ correspondent aux élément $x + y\sqrt{7} \in \mathbf{Z}[\sqrt{7}]$ tels que $N(x + y\sqrt{7}) = -1$.
Notons que de tels éléments sont nécessairement dans G, et il s'agit donc de déterminer le nombre d'éléments de G dont la norme vaut -1.
Mais $N(u) = N(8+3\sqrt{7}) = 8^2 - 3^2\times 7 = 1$, si bien que pour tout $k \in \mathbf{Z}$, $N(u^k) = N(u)^k = 1$.
Ainsi, pour tout $g \in G \cap \mathbf{R}_+^*$, $N(x) \neq -1$.
Et pour tout $g \in G \cap \mathbf{R}_-^*$, on a $N(g) = \underbrace{N(-1)}_{=1} N(-g) = 1$.
Et donc il n'existe aucun élément de $\mathbf{Z}[\sqrt{7}]$ de norme -1, et donc aucune solution à l'équation $x^2 - 7y^2 = -1$.