

DEVOIR SURVEILLÉ N° 7 (4 HEURES)

Ce devoir est constitué de trois exercices et d'un problème. L'ordre des exercices ne correspond à aucun critère de difficulté ou de longueur : vous pouvez les traiter dans l'ordre que vous voulez. Veillez à soigner la copie tant pour l'écriture, la propreté que pour la rédaction, la rigueur et l'argumentation. Vous numéroterez vos copies et ferez apparaître clairement sur la première page le nombre de copies.

La calculatrice n'est pas autorisée.

EXERCICE I : Racines n -ièmes primitives de l'unité

Soit $n \in \mathbb{N}^*$. On note U_n l'ensemble des racines n -ièmes de l'unité : $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

1. Montrer que si U_n est un sous-groupe de (\mathbb{C}^*, \times)

Le but de la suite de l'exercice sera de déterminer les racines n -ièmes primitives de l'unité, c'est-à-dire les nombres γ de U_n vérifiant : $\forall z \in U_n, \exists k \in \mathbb{Z} \mid z = \gamma^k$.

2. Soit $p \in \mathbb{Z} \cap [1, n]$ tel que $p \wedge n = 1$. On pose $\omega_p = e^{\frac{2ip\pi}{n}}$

(a) Montrer que : $\exists u \in \mathbb{Z} \mid \omega_1 = \omega_p^u$.

(b) En déduire que ω_p est une racine n -ième primitive de l'unité.

3. Soit $p \in \mathbb{Z} \cap [1, n]$ tel que $p \wedge n = d \neq 1$. On pose $\omega_p = e^{\frac{2ip\pi}{n}}$ et q le quotient de la division euclidienne de n par d .

(a) Montrer que : $\forall k \in \mathbb{Z}, \omega_p^k \in U_q$.

(b) En déduire que ω_p n'est pas une racine n -ième primitive de l'unité.

4. Conclure.

EXERCICE II : Equation de Pythagore

On considère l'équation suivante, d'inconnue $(x, y, z) \in (\mathbb{N}^*)^3$: (E) : $x^2 + y^2 = z^2$

1. (a) Montrer que si (x, y, z) est un triplet solution de (E) et si p est un nombre premier divisant deux de ces éléments, alors p divise le troisième.
- (b) En déduire que pour trouver tous les triplets solutions de (E), il suffit de trouver les triplets solutions (x, y, z) avec x, y et z premiers deux à deux.

Dans la suite on considère (x, y, z) une solution de (E) avec $x \wedge y = 1$, $x \wedge z = 1$ et $y \wedge z = 1$.

2. Montrer que z est impair et que x et y sont de parité contraire.

3. On suppose que x est pair.

(a) Montrer que : $(z - y) \wedge (z + y) = 2$, puis qu'il existe $(\alpha, \beta, \gamma) \in (\mathbb{N}^*)^3$ tels que :

$$z - y = 2\alpha \quad , \quad z + y = 2\beta \quad \text{et} \quad x = 2\gamma \quad \text{avec} \quad \gamma^2 = \alpha\beta \quad \text{et} \quad \alpha \wedge \beta = 1$$

(b) En déduire qu'il existe $(u, v) \in (\mathbb{N}^*)^2$ tels que : $\alpha = u^2 \quad , \quad \beta = v^2 \quad \text{et} \quad u \wedge v = 1$.

4. Déterminer l'ensemble des solutions de (E)

EXERCICE III : Exercice pour la Chandeleur

Le BDE décide d'organiser une soirée Crêpes / Gaufres à l'occasion de la Chandeleur. Il a en sa possession un stock de 2 kg de confitures et autre pâte à tartiner (au chocolat et noisette par exemple...). Pour garnir une gaufre il faut exactement 18 g de confiture ou pâte à tartiner. Pour une crêpe il en faut 13 g. Pour satisfaire les élèves, il faut qu'il y ait "beaucoup plus" de crêpes que de gaufres, mais moins de crêpes que du double de gaufres. Le but du problème est de retrouver la quantité de crêpes et de gaufres confectionnées lors de la soirée, sachant que toute la confiture (et la pâte à tartiner) a été utilisée. Nous allons formaliser le problème.

1. Résoudre l'équation d'inconnues $(x, y) \in \mathbb{Z}^2$: $13x + 18y = 1$
2. Résoudre l'équation d'inconnues $(x, y) \in \mathbb{Z}^2$: $13x + 18y = 2000$
3. Résoudre l'équation d'inconnues $(x, y) \in \mathbb{N}^2$: $13x + 18y = 2000$
4. Répondre au problème posé (on montrera que parmi les solutions de la question précédente, seulement deux vérifient les conditions encadrant la quantité de crêpes par rapport aux gaufres ... et une des deux plus que l'autre...).

PROBLEME I : Equation de Pell Fermat

L'entreprise Carréchoch fabrique des carrés de chocolat réputés. Elle vend ces chocolats sous forme de grandes plaques carrées. Ces plaques contiennent donc exactement m^2 carrés de chocolat.

A l'occasion de son troisième centenaire, elle souhaite mettre en vente des plaques de chocolat ayant la même forme carrée mais possédant une quantité triple de chocolat.

Un ingénieur de la firme à qui l'on a soumis le problème s'avise rapidement que le problème est impossible car, affirme-t-il à ses dirigeants et commerciaux ébahis, $\sqrt{3}$ n'est pas rationnel.

Par contre, il poursuit qu'à un petit carré près, ce problème devient résoluble.

Considérant que le nombre de petits carrés dans une plaque habituelle est compris entre 100 et 1000, les dirigeants de la firme conviennent que l'on ne s'apercevra pas vraiment que l'on n'a pas exactement le triple de carrés, donc acceptent de créer les plaques de n^2 petits carrés avec $n^2 = 3m^2 \pm 1$.

Nous allons retrouver le nombre de petits carrés dans chaque plaque.

Préliminaires

1. Montrer, comme l'ingénieur l'a annoncé, que $\sqrt{3}$ n'est pas rationnel.
2. En effectuant par exemple un travail modulo 4, montrer que si (n, m) est solution du problème posé, on a nécessairement : $n^2 = 3m^2 + 1$

On va donc étudier l'équation de Pell-Fermat : (i) : $x^2 - 3y^2 = 1$ avec $(x, y) \in \mathbb{N}^2$

PARTIE I : Etude de $\mathbb{Z}[\sqrt{3}]$

On rappelle que $\sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}$ et $\sqrt{3} \in]1, 2[$.

On considère l'ensemble $\mathbb{Z}[\sqrt{3}] = \{x \in \mathbb{R} \mid \exists (a, b) \in \mathbb{Z}^2; x = a + b\sqrt{3}\}$.

1. Montrer que $\mathbb{Z}[\sqrt{3}]$ est un anneau commutatif, sous-anneau du corps \mathbb{R}
2. Montrer que si $x \in \mathbb{Z}[\sqrt{3}]$, le couple $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{3}$ est unique.
3. Si $x = a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Z}^2$, on pose $\bar{x} = a - b\sqrt{3}$ et $N(x) = x\bar{x}$
 - (a) Montrer que, si $x \in \mathbb{Z}[\sqrt{3}]$ alors $N(x) \in \mathbb{Z}$.
 - (b) Montrer que : $\forall (x, x') \in \left(\mathbb{Z}[\sqrt{3}]\right)^2, \overline{xx'} = \bar{x}\bar{x}'$

(c) Montrer que : $\forall (x, x') \in \left(\mathbb{Z} \left[\sqrt{3}\right]\right)^2$, $N(x x') = N(x) N(x')$

Soit U le groupe des éléments inversibles de $\mathbb{Z} \left[\sqrt{3}\right]$ pour la loi \times

4. Soit $x \in \mathbb{Z} \left[\sqrt{3}\right]$. Montrer que :

$$x \in U \iff N(x) = 1 \text{ ou } N(x) = -1 \iff N(x) = 1$$

5. Soit $x = a + b\sqrt{3} \in U$.

(a) Montrer que $a \neq 0$

(b) Si $a > 0$. Montrer que : $b > 0 \implies x > 1$, $b = 0 \implies x = 1$ et $b < 0 \implies x \in]-1, 1[$

(c) Si $a < 0$. Montrer que : $b < 0 \implies x < -1$, $b = 0 \implies x = -1$ et $b > 0 \implies x \in]-1, 1[$

6. On pose $x_0 = 2 + \sqrt{3}$. Montrer que x_0 est le plus petit élément de l'ensemble $H = U \cap]1, +\infty[$.

7. (a) Montrer que : $\forall u \in H$, $\exists p \in \mathbb{N} \mid x_0^p \leq u < x_0^{p+1}$. En considérant $\frac{u}{x_0^p}$, montrer que $u = x_0^p$

(b) Montrer que : $H = \{x_0^p \mid p \in \mathbb{N}^*\}$

PARTIE II : Equation de Pell-Fermat

On considère l'équation (i) : $x^2 - 3y^2 = 1$ avec $(x, y) \in (\mathbb{N}^*)^2$.

1. Soit $(a, b) \in (\mathbb{N}^*)^2$. Montrer que : (a, b) est solution de (i) $\iff a + b\sqrt{3} \in H$

2. Dédurre de la forme des éléments de H que : (a, b) solution de (i) $\iff \exists p \in \mathbb{N}^* \mid a + b\sqrt{3} \in x_0^p$.

$$\text{Montrer qu'alors on a : } a = \frac{x_0^p + \overline{x_0^p}}{2} \text{ et } b = \frac{x_0^p - \overline{x_0^p}}{2\sqrt{3}}$$

3. En remarquant : $-1 < \overline{x_0} < 1$, déterminer toutes les solutions de (i) : $x^2 - 3y^2 = 1$ telles que $y \leq 100$.

4. Trouver le nombre de petits carrés dans les grandes plaques

EXERCICE I : Racines n -ièmes primitives de l'unité

Soit $n \in \mathbb{N}^*$. Soit $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

1. U_n est une partie de \mathbb{C}^* car $\forall z \in U_n, z \in \mathbb{C}$ et $z \neq 0$ car $0^n \neq 1$.

Soit $(z, z') \in U_n^2$. On a $\left(\frac{z}{z'}\right)^n = \frac{z^n}{z'^n} = \frac{1}{1} = 1$. Ainsi $\forall (z, z') \in U_n^2, \frac{z}{z'} \in U_n$.

Donc, par caractérisation des sous-groupes, **U_n est un sous-groupe de (\mathbb{C}^*, \times)**

2. Soit $p \in \mathbb{Z} \cap [1, n]$ tel que $p \wedge n = 1$. On pose $\omega_p = e^{\frac{2ip\pi}{n}}$. Remarquons que l'on a : $\omega_p = \omega_1^p$.

(a) D'après la relation de Bezout, on a : $\exists (u, v) \in \mathbb{Z}^2 \mid up + vn = 1$. Ainsi : $\omega_1 = \omega_1^{up} \times \omega_1^{nv} = (\omega_1^p)^u \times (\omega_1^n)^v = \omega_p^u \times 1^v$. Ainsi : **$\exists u \in \mathbb{Z} \mid \omega_1 = \omega_p^u$** .

(b) Soit $z \in U_n$. On sait qu'il existe $q \in \mathbb{Z}$ tel que : $z = \omega_q = e^{\frac{2iq\pi}{n}} = \omega_p^q = \omega_p^{qu}$ avec u l'entier trouvé à la question précédente. Ainsi tout élément de U_n est une puissance de ω_p :

ω_p est une racine n -ième primitive de l'unité.

3. Soit $p \in \mathbb{Z} \cap [1, n]$ tel que $p \wedge n = d \neq 1$. On pose $\omega_p = e^{\frac{2ip\pi}{n}}$ et q le quotient de la division euclidienne de n par d .

(a) Soit $k \in \mathbb{Z}$. $(\omega_p^k)^q = \omega_1^{kpq}$. Or pq est un multiple de dq donc de n , ainsi : $\omega_1^{kpq} = 1$. Ainsi

$\forall k \in \mathbb{Z}, \omega_p^k \in U_q$.

(b) $\omega_1^q = e^{\frac{2iq\pi}{n}} \neq 1$ car q n'est pas un multiple de n . Donc ω_1 n'est pas une puissance de ω_p et donc

ω_p n'est pas une racine n -ième primitive de l'unité.

4. En regroupant les résultats obtenus dans les différents cas, on a

les racines n -ièmes primitives de l'unité sont les $e^{\frac{2ip\pi}{n}}$ avec $p \wedge n = 1$

EXERCICE II : Equation de Pythagore

On considère l'équation suivante, d'inconnue $(x, y, z) \in (\mathbb{N}^*)^3$: (E) : $x^2 + y^2 = z^2$

1. (a) Soit p un nombre premier. On rappelle que si p divise le produit de deux entiers ab alors p divise a ou p divise b . En particulier si p divise le carré a^2 d'un entier, p divise a .

Soit alors (x, y, z) est un triplet d'entiers solution de (E) et p un nombre premier.

☞ Si p divise x et y , alors p divise x^2 et y^2 donc aussi $x^2 + y^2$ donc z^2 et donc p divise z

☞ Si p divise x et z , alors p divise x^2 et z^2 donc aussi $z^2 - x^2$ donc y^2 et donc p divise y

☞ Si p divise z et y , alors p divise z^2 et y^2 donc aussi $z^2 - y^2$ donc x^2 et donc p divise x

Ainsi **si p divise deux éléments parmi x, y et z , alors p divise le troisième**.

- (b) Si (x, y, z) est un triplet d'entiers, on appelle d le pgcd de ces trois nombres, c'est-à-dire le pgcd de z et de $x \wedge y$. En appelant x', y' et z' les quotients respectifs de x, y et z par d , on vérifie que (x, y, z) est un triplet pythagoricien ssi (x', y', z') est un triplet pythagoricien. Ainsi il suffit de trouver les triplets pythagoriciens avec des entiers (x', y', z') premiers entre eux dans leur ensemble.

Mais grâce à la question précédente, on sait que si un triplet pythagoricien est formé de nombres premiers entre eux dans leur ensemble, alors ils sont premiers entre eux deux à deux. Ainsi pour trouver tous les triples solutions de (E),

il suffit de trouver les triplets solutions (x, y, z) avec x, y et z premiers deux à deux

Dans la suite on considère (x, y, z) une solution de (E) avec $x \wedge y = 1, x \wedge z = 1$ et $y \wedge z = 1$.

2. On travaille modulo 4. Les carrés modulo 4 sont 0 et 1. Les entiers somme de deux carrés sont donc congrus à 0, 1 ou 2 modulo 4. Comme z^2 est à la fois un carré et une somme de carrés, z^2 est congru soit à 0 soit à 1 modulo 4. Or cela ne peut pas être 0 sinon on aurait eu x et y (et z) pairs ce qui est interdit car x et y sont premiers entre eux. Ainsi $z^2 \equiv 1[4]$ et donc **z est impair**.

De plus, parmi x^2 et y^2 , un d'entre eux est congru à 0 modulo 4 et l'autre à 1 modulo 4. Ainsi **parmi x et y , l'un est pair et l'autre est impair**

3. On suppose que x est pair.

(a) ☞ On a z et y impairs donc $z+y$ et $z-y$ sont pairs et donc 2 divise le pgcd de $z-y$ et $z+y$

☞ Si p est un nombre premier impair, alors p ne peut diviser à la fois $z-y$ et $z+y$ sinon il diviserait la somme et la différence de ces deux nombres à savoir $2z$ et $2y$. Or comme p est premier avec 2, p divise z et y ce qui est impossible.

Ainsi le pgcd de $z-y$ et $z+y$ est une puissance de 2.

☞ Enfin 4 ne divise pas $(z-y) \wedge (z+y)$. Sinon 4 diviserait $2z$ et $2y$ et donc z et y serait pair ce qui est faux.

Ainsi **$(z-y) \wedge (z+y) = 2$** .

Comme on sait que x , $z-y$ et $z+y$ sont pairs, on peut poser γ , α et β leurs quotients respectifs par 2 :

$z-y = 2\alpha$, $z+y = 2\beta$ et $x = 2\gamma$ et ces entiers sont positifs car x , y et z le sont et $y \leq z$. Comme $(z-y) \wedge (z+y) = 2$, on en déduit que $\alpha \wedge \beta = 1$. Enfin on a $2\alpha \times 2\beta = (z-y)(z+y) = z^2 - y^2 = x^2 = 4\gamma^2$. Ainsi :

$$\exists(\alpha, \beta, \gamma) \in (\mathbb{N}^*)^3 \mid z-y = 2\alpha, \quad z+y = 2\beta \quad \text{et} \quad x = 2\gamma \quad \text{avec} \quad \gamma^2 = \alpha\beta \quad \text{et} \quad \alpha \wedge \beta = 1$$

(b) α et β sont des entiers premiers entre eux dont le produit est un carré parfait donc ce sont des carrés parfaits. **$\exists(u, v) \in (\mathbb{N}^*)^2$ tels que : $\alpha = u^2$, $\beta = v^2$** .

De plus, comme α et β sont deux premiers entre eux, c'est aussi le cas pour u et v i.e. **$u \wedge v = 1$** .

4. En regroupant les résultats des questions précédentes, on obtient que l'ensemble des solutions de l'équation est

$$E = \left\{ (x, y, z) \in (\mathbb{N}^*)^3 \mid \exists(u, v, w) \in (\mathbb{N}^*)^2 \begin{cases} x = 2uvw \\ y = w(v^2 - u^2) \\ y = w(v^2 + u^2) \end{cases} \text{ avec } u < v \text{ et } u \wedge v = 1 \right\}$$

EXERCICE III : Exercice pour la Chandeleur

Le BDE décide d'organiser une soirée Crêpes / Gaufres à l'occasion de la Chandeleur. Il a en sa possession un stock de 2 kg de confitures et autre pâte à tartiner (au chocolat et noisette par exemple...). Pour garnir une gaufre il faut exactement 18 g de confiture ou pâte à tartiner. Pour une crêpe il en faut 13 g. Pour satisfaire les élèves, il faut qu'il y ait "beaucoup plus" de crêpes que de gaufres, mais moins de crêpes que du double de gaufres. Le but du problème est de retrouver la quantité de crêpes et de gaufres confectionnées lors de la soirée, sachant que toute la confiture (et la pâte à tartiner) a été utilisée
Nous allons formaliser le problème.

1. On effectue l'algorithme d'Euclide. On obtient : $18 = 13 \times 1 + 5$ puis $13 = 5 \times 2 + 3$ puis $5 = 3 \times 1 + 2$ et enfin $3 = 2 \times 1 + 1$. D'où 13 et 18 sont premiers entre eux et en remontant les calculs, on a : $1 = 7 \times 13 - 5 \times 18$. **le couple $(7, -5)$ est solution particulière de l'équation diophantienne $13x + 18y = 1$**

☛ Soit $(x, y) \in \mathbb{Z}^2$ tel que $13x + 18y = 1$. On a : $13x + 18y = 7 \times 13 - 5 \times 18$ i.e $13(x-7) = -18(y+5)$ (E). Or 13 et 18 sont premiers entre eux donc d'après le théorème de Gauss, 13 divise $(y+5)$ i.e. il existe $k \in \mathbb{Z} \mid y = -5 + 13k$. En remplaçant dans la relation (E), on a alors : $x = 7 - 18k$

☛ Réciproquement. Soit $k \in \mathbb{Z}$ et soit $(x, y) = (7 - 18k, 13k - 5)$. On vérifie aisément $(x, y) \in \mathbb{Z}^2$ et $13x + 18y = 1$

Ainsi les solutions dans \mathbb{Z}^2 de l'équation $13x + 18y = 1$ forment l'ensemble

$$E_1 = \{(7 - 18k, 13k - 5) \mid k \in \mathbb{Z}\}$$

2. En constatant qu'en multipliant par 2000 une solution particulière de l'équation précédente on obtient une solution particulière de notre équation, puis en effectuant le même raisonnement pour obtenir toutes les solutions, on trouve :

$$E_2 = \{(x, y) \in \mathbb{Z}^2 \mid 13x + 18y = 2000\} = \{(14000 - 18k, 13k - 10000) \mid k \in \mathbb{Z}\}$$

3. On cherche les couples $(x, y) \in E_2$ avec x et y positifs soit les couples $(14000 - 18k, 13k - 10000)$ avec k entier tel que $14000 - 18k \geq 0$ et $13k - 10000 \geq 0$ i.e.

$18k \leq 14000 = 18 \times 777 + 14$ et $13k \geq 10000 = 13 \times 769 + 3$ donc, puisque k est entier, on a $770 \leq k \leq 777$. Ainsi les solutions dans \mathbb{N}^2 de l'équation $13x + 18y = 2000$ sont les couples

$$(140, 10), (122, 23), (104, 36), (86, 49), (68, 62), (50, 75), (32, 88) \text{ et } (14, 101)$$

4. On cherche $(x, y) \in \mathbb{N}^2$ avec $13x + 18y = 2000$ et $y < x < 2y$. On trouve donc $(86, 49)$ et $(68, 62)$ et parmi celles-ci, c'est $(86, 49)$ qui vérifie la condition "il y a *beaucoup plus* de crêpes que de gaufres"

PROBLEME I : Equation de Pell Fermat

L'entreprise Carréchoc fabrique des carrés de chocolat réputés. Elle vend ces chocolats sous forme de grandes plaques carrées. Ces plaques contiennent donc exactement m^2 carrés de chocolat.

A l'occasion de son troisième centenaire, elle souhaite mettre en vente des plaques de chocolat ayant la même forme carrée mais possédant une quantité triple de chocolat.

Un ingénieur de la firme à qui l'on a soumis le problème s'avise rapidement que le problème est impossible car, affirme-t-il à ses dirigeants et commerciaux ébahis, $\sqrt{3}$ n'est pas rationnel.

Par contre, il poursuit qu'à un petit carré près, ce problème devient résoluble.

Considérant que le nombre de petits carrés dans une plaque habituelle est compris entre 100 et 1000, les dirigeants de la firme conviennent que l'on ne s'apercevra pas vraiment que l'on n'a pas exactement le triple de carrés, donc acceptent de créer les plaques de n^2 petits carrés avec $n^2 = 3m^2 \pm 1$.

Nous allons retrouver le nombre de petits carrés dans chaque plaque.

Préliminaires

1. Par l'absurde, supposons que $\sqrt{3}$ soit rationnel. Il existe deux entiers premiers entre eux p et q tels que : $\sqrt{3} = \frac{p}{q}$. Ainsi : $p^2 = 3q^2$. Donc $3 \mid p^2$ et comme 3 est un nombre premier $3 \mid p$. Il existe donc un entier r tel que $p = 3r$ et on a alors $q^2 = 3r^2$. Mais alors $3 \mid q$ donc $3 \mid p \wedge q$ et ainsi p et q ne sont pas premiers entre eux : Contradiction.

Ainsi $\sqrt{3}$ est irrationnel

2. Les carrés parfaits sont congrus à 0 ou 1 modulo 4. Ainsi, pour tout couple d'entiers (n, m) , $n^2 - 3m^2 \equiv n^2 + 3m^2 [4]$ est congru soit à 0, à 1 ou à 2 modulo 4... mais jamais à -1 : on ne peut pas avoir $n^2 - 3m^2 = -1$. Mais puisque l'on a $n^2 - 3m^2 = \pm 1$, on a donc :

$$\text{si } (n, m) \text{ est solution du problème, on a } n^2 - 3m^2 = 1$$

On va donc étudier l'équation de Pell-Fermat : (i) : $x^2 - 3y^2 = 1$ avec $(x, y) \in \mathbb{N}^2$

PARTIE I : Etude de $\mathbb{Z}[\sqrt{3}]$

On rappelle que $\sqrt{3} \in \mathbb{R} \setminus \mathbb{Q}$ et $\sqrt{3} \in]1, 2[$. Soit $\mathbb{Z}[\sqrt{3}] = \{x \in \mathbb{R} \mid \exists(a, b) \in \mathbb{Z}^2; x = a + b\sqrt{3}\}$.

1. $\mathbb{Z}[\sqrt{3}]$ étant une partie du corps \mathbb{R} , pour montrer qu'il s'agit d'un anneau il suffit de montrer qu'il est stable par soustraction et multiplication et qu'il possède l'élément neutre de la multiplication (car le fait qu'il soit non vide et stable par soustraction montrera que c'est un sous-groupe de $(\mathbb{R}, +)$, et les autres propriétés des opérations $+$ et \times seront obtenues par restriction des propriétés qu'elles ont sur \mathbb{R} tout entier).

Or : $1 = 1 + 0\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ et les stabilités de $\mathbb{Z}[\sqrt{3}]$ par soustraction et multiplication se vérifient aisément. Ainsi $\mathbb{Z}[\sqrt{3}]$ est un anneau, sous -anneau de $(\mathbb{R}, +, \times)$.

2. soit $x \in \mathbb{Z}[\sqrt{3}]$. Supposons que les deux couples d'entiers (a, b) et (c, d) sont tels que $x = a + b\sqrt{3}$ et $x = c + d\sqrt{3}$. On a alors : $(a - c) = (d - b)\sqrt{3}$ et donc, comme le produit d'un irrationnel par un rationnel n'est rationnel que si le rationnel est nul, on en déduit que : $a - c = 0 = d - b$ i.e. $(a, b) = (c, d)$. Ainsi

si $x \in \mathbb{Z}[\sqrt{3}]$, le couple $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{3}$ est unique.

3. Si $x = a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Z}^2$, on pose $\bar{x} = a - b\sqrt{3}$ et $N(x) = x\bar{x}$

(a) Soit $x \in \mathbb{Z}[\sqrt{3}]$. On note $x = a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Z}^2$. On a $N(x) = x\bar{x} = a^2 - 3b^2 \in \mathbb{Z}$

(b) Soit $(x, x') \in (\mathbb{Z}[\sqrt{3}])^2$. On écrit x et x' sous la forme : $x = a + b\sqrt{3}$ et $x' = c + d\sqrt{3}$ avec $(a, b, c, d) \in \mathbb{Z}^4$. On a alors :

$$\blacktriangleright \overline{xx'} = \overline{(a + b\sqrt{3})(c + d\sqrt{3})} = \overline{(ac + 3bd) + (ad + bc)\sqrt{3}} = (ac + 3bd) - (ad + bc)\sqrt{3}$$

$$\blacktriangleright \overline{\bar{x}\bar{x}'} = \overline{(a - b\sqrt{3})(c - d\sqrt{3})} = (ac + 3bd) - (ad + bc)\sqrt{3}$$

Ainsi $\forall (x, x') \in (\mathbb{Z}[\sqrt{3}])^2, \overline{xx'} = \overline{\bar{x}\bar{x}'}$

(c) Soit $(x, x') \in (\mathbb{Z}[\sqrt{3}])^2$. On a : $N(xx') = xx' \times \overline{xx'} = xx' \times \overline{\bar{x}\bar{x}'} = (x\bar{x})(x'\bar{x}')$.

Ainsi $\forall (x, x') \in (\mathbb{Z}[\sqrt{3}])^2, N(xx') = N(x)N(x')$

Soit U le groupe des éléments inversibles de $\mathbb{Z}[\sqrt{3}]$ pour la loi \times

4. Soit $x \in \mathbb{Z}[\sqrt{3}]$.

\blacktriangleright Si $x \in U$. Alors il existe $x' \in \mathbb{Z}[\sqrt{3}]$ tel que $xx' = 1$. On a alors $N(x)N(x') = N(1) = 1$ avec $N(x)$ et $N(x')$ entiers donc $N(x)$ est inversible dans \mathbb{Z} i.e. $N(x) = 1$ ou -1

\blacktriangleright Si $N(x) = 1$ ou -1 . Alors il existe $(a, b) \in \mathbb{Z}^2$ tels que $x = a + b\sqrt{3}$ et on a alors $N(x) = a^2 - 3b^2 = \pm 1$. Or on a vu que l'équation $n^2 - 3m^2 = -1$ n'avait pas de solutions entières donc $a^2 - 3b^2 = 1$ i.e. $N(x) = 1$

\blacktriangleright Si $N(x) = 1$. Alors $x\bar{x} = 1$ avec $\bar{x} \in \mathbb{Z}[\sqrt{3}]$ donc x est inversible.

Ainsi $x \in U \iff N(x) = 1 \text{ ou } N(x) = -1 \iff N(x) = 1$

5. Soit $x = a + b\sqrt{3} \in U$.

(a) $x \in U$ donc $a^2 = 1 + 3b^2 \geq 1$ Ainsi $a \neq 0$

(b) Si $a > 0$.

\blacktriangleright Si $b > 0$. Alors $x = a + b\sqrt{3} \geq 1 + \sqrt{3} > 1$: $x > 1$

\blacktriangleright Si $b = 0$. Alors $x = a$ et $N(x) = a^2 = 1$ Donc $x = 1$

\blacktriangleright Si $b < 0$. Alors $\bar{x} = a - b\sqrt{3} \geq 1 + \sqrt{3} > 1$ et $\bar{x} \in U$. Ainsi $\bar{x} > 1$. Donc, comme $x = \frac{1}{\bar{x}}$: $x \in]0, 1[$

(c) Si $a < 0$. En remarquant qu'alors $-x \in U$ est de la forme $-x = a' + b'\sqrt{3}$ avec $a' > 0$, la discussion précédente permet d'obtenir :

$$b < 0 \implies x < -1, \quad b = 0 \implies x = -1 \quad \text{et} \quad b > 0 \implies x \in]-1, 0[$$

6. On pose $x_0 = 2 + \sqrt{3}$. Soit $H = U \cap]1, +\infty[$.

On constate d'abord que $N(x_0) = (2 + \sqrt{3})(2 - \sqrt{3}) = 1$ et $x_0 > 1$ donc $x_0 \in H$.

Soit $x \in H$. On écrit $x = a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Z}^2$.

Puisque $x \in U$ et $x > 1$, la discussion précédente permet d'affirmer $a > 0$ et $b > 0$. Mais comme a et b sont des entiers, $a \geq 1$ et $b \geq 1$. Mais alors $a^2 = 3b^2 + 1 \geq 4$ et donc $a \geq 2$. Ainsi $x \geq 2 + \sqrt{3} = x_0$.

Ainsi x_0 est un élément de H et un minorant de H :

x_0 est le plus petit élément de l'ensemble $H = U \cap]1, +\infty[$

7. (a) Soit $u \in H$. Soit $p = \left\lfloor \frac{\ln(u)}{\ln(x_0)} \right\rfloor$. On a $p \in \mathbb{N}^*$ car $u \geq x_0 > 1$. De plus : $p \ln(x_0) \geq \ln(u) <$

$(p+1) \ln(x_0)$. Ainsi $\forall u \in H, \exists p \in \mathbb{N} \mid x_0^p \leq u < x_0^{p+1}$.

De plus, U étant un groupe pour la loi \times et u et x_0^p étant deux éléments de U , on a : $u x_0^{-p} \in U$.

Mais : $1 \geq u x_0^{-p} < x_0$ Donc comme x_0 est le plus petit élément de U strictement supérieur à 1, on a $u x_0^{-p} = 1$ et donc $u = x_0^p$.

(b) On vient de voir : $\forall u \in H, \exists p \in \mathbb{N}^* \mid u = x_0^p$. Ainsi $H \subset \{x_0^p \mid p \in \mathbb{N}^*\}$.

D'autre part, si $p \in \mathbb{N}^*$, $x_0^p \in U$ et de plus $x_0^p \geq x_0 > 1$. Donc $x_0^p \in H$. $\{x_0^p \mid p \in \mathbb{N}^*\} \subset H$.

Ainsi par double inclusion on a établi, $H = \{x_0^p \mid p \in \mathbb{N}^*\}$

PARTIE II : Equation de Pell-Fermat

On considère l'équation (i) : $x^2 - 3y^2 = 1$ avec $(x, y) \in (\mathbb{N}^*)^2$.

1. Soit $(a, b) \in (\mathbb{N}^*)^2$.

(a, b) solution de (i) $\iff N(a + b\sqrt{3}) = 1 \iff a + b\sqrt{3} \in U \iff a + b\sqrt{3} \in H$ car $a > 0$ et $b > 0$.

Donc (a, b) est solution de (i) $\iff a + b\sqrt{3} \in H$

2. (a, b) est solution de (i) $\iff a + b\sqrt{3} \in H \iff \exists p \in \mathbb{N}^* \mid a + b\sqrt{3} = x_0^p$ et alors $a - b\sqrt{3} = \overline{x_0^p}$

Donc (a, b) solution de (i) $\iff \exists p \in \mathbb{N}^* \mid a = \frac{x_0^p + \overline{x_0^p}}{2}$ et $b = \frac{x_0^p - \overline{x_0^p}}{2\sqrt{3}}$

3. Comme $x_0 > 1$ et $\overline{x_0} = \frac{1}{x_0}$, on a $x_0 \in]0, 1[$. Ainsi pour tout $p \in \mathbb{N}^*$, $x_0^p \in]0, 1[$. Ainsi on aura

$y \leq 100$ tant que $x_0^p \geq 200\sqrt{3} + 1$. Or :

$x_0^1 = 2 + \sqrt{3}$, $x_0^2 = 7 + 4\sqrt{3}$, $x_0^3 = 26 + 15\sqrt{3}$, $x_0^4 = 97 + 56\sqrt{3}$. Enfin si $p \geq 5$, $x_0^p \geq x_0^5 = 362 + 209\sqrt{3} > 200\sqrt{3} + 1$. Ainsi les solutions avec $y \leq 100$ sont $(2, 1), (7, 4), (26, 15), (97, 56)$

4. On cherche un couple $(n, m) \in \mathbb{N}^2$ solution de (i) avec $m^2 \in [100, 1000]$ donc avec $m \in [10, 32]$: on trouve $(n, m) = (26, 15)$. Ainsi le nombre total de petits carrés dans les plaques habituelles est

$m^2 = 225$

et dans les grandes plaques $n^2 = 3m^2 + 1 = 676$