Devoir Surveillé N°5

Fonctions Réelles Structures & Arithmétique

Documents & Calculatrices Interdites

Durée : 4 heures

Vendredi 12 Février 2021

EXERCICE 1 : Un anneau d'extension quadratique

Soit α l'une des deux racines complexes[1] du polynôme $P(z) = z^2 + z + 2$.
On désigne par $\mathbf{Z}[\alpha]$ l'ensemble des nombres complexes défini par

$$\boxed{\mathbf{Z}[\alpha] = \left\{p + \alpha q\,;\ (p,q) \in \mathbf{Z}^2\right\}}$$

1. Montrez que $\mathbf{Z}[\alpha]$ est un sous-anneau de $\mathbf{C}$.

2.a. Montrez [2] que $\alpha + \bar{\alpha} = -1$ et $\alpha\,\bar{\alpha} = 2$.

b. Montrez que pour tout $z \in \mathbf{Z}[\alpha]$, $\bar{z} \in \mathbf{Z}[\alpha]$.

c. Montrez que pour tout $z \in \mathbf{Z}[\alpha]$, $z\,\bar{z} \in \mathbf{N}$.

3.a. Soit $z = p + \alpha q$ un élément de $\mathbf{Z}[\alpha]$. Montrez que z est inversible dans $\mathbf{Z}[\alpha]$ *si et seulement si* (p,q) vérifie :

$$p^2 + 2q^2 - pq = 1 \qquad (1)$$

b. Montrez que l'équation (2) est impossible lorsque $pq < 0$.

c. Montrez que l'équation (2) est impossible lorsque $pq > 0$.

d. Déduisez des questions précédentes l'ensemble des éléments inversibles de $\mathbf{Z}[\alpha]$.

EXERCICE 2 : Nombres de Fibonacci

On considère la suite $(F_n)_{n\in\mathbf{N}}$ définie par les relations

$$F_0 = 0,\ F_1 = 1,\ \text{et } \forall n \in \mathbf{N}^\star,\ F_{n+1} = F_n + F_{n-1}$$

Les F_n sont des nombres entiers naturels appelés **nombres de Fibonacci**.

1. Montrez que pour tout entier naturel $n \in \mathbf{N}^\star$, $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. Déduisez-en que F_n et F_{n+1} sont premiers entre eux.

2. Montrez que pour tout couple $(n,p) \in \mathbf{N}\times\mathbf{N}^\star$, $F_{n+p} = F_pF_{n+1} + F_{p-1}F_n$. Déduisez-en que

$$PGCD(F_n, F_p) = PGCD(F_{n+p}, F_p)$$

3. Démontrez finalement,

$$\forall (n,p) \in \mathbf{N}^2,\quad PGCD(F_n, F_p) = F_{PGCD(n,p)}$$

1. il n'est pas nécessaire d'expliciter α

Exercice 3

Question 1

1. Etudier la convexité de $x \mapsto x^p$ sur $\mathbb{R}^+$, lorsque p est un entier supérieur ou égal à 2.
2. En déduire que pour tout $(a,b) \in (\mathbb{R}^+)^2$, $(a+b)^p \leq 2^{p-1}(a^p+b^p)$.

Question 2

On considère la fonction f définie par $f(x) = \ln(\ln x)$.

1. Déterminer l'ensemble de définition de f et montrer que f y est concave.
2. En déduire :

$$\forall (x,y) \in]1,+\infty[^2, \quad \ln\left(\frac{x+y}{2}\right) \geq \sqrt{\ln x \ln y}.$$

Question 3

1. Vérifier que la fonction $f : x \mapsto \ln(1+e^x)$ est convexe sur $\mathbb{R}$.
2. Soient $x_1, x_2, \ldots, x_n$, des réels strictement positifs. Montrer que $\left(\prod_{k=1}^{n}(1+x_k)\right)^{\frac{1}{n}} \geq 1 + \left(\prod_{k=1}^{n} x_k\right)^{\frac{1}{n}}$.

   indication : pour $k \in [\![1,n]\!]$, on pourra poser $y_k = \ln(x_k)$ et montrer l'inégalité correspondante sur les y_k
3. Soient $a_1, a_2, \ldots, a_n$, $b_1, b_2 \ldots, b_n$ des réels strictement positifs. Prouver l'inégalité $\left(\prod_{k=1}^{n}(a_k+b_k)\right)^{\frac{1}{n}} \geq \left(\prod_{k=1}^{n} a_k\right)^{\frac{1}{n}} + \left(\prod_{k=1}^{n} b_k\right)^{\frac{1}{n}}$.

Question 4

1. Montrer que pour tout réel x, les intégrales $S(x) = \int_0^1 \sin(xt)e^{-t^2}dt$ et $C(x) = \int_0^1 t\cos(xt)e^{-t^2}dt$ existent.
2. A l'aide de l'inégalité de T-L, montrer : $\forall a \in \mathbb{R}, \forall y \in \mathbb{R} : \left|\sin(a+y) - \sin a - y\cos a\right| \leq \frac{y^2}{2}$.
3. Montrer que $\forall x \in \mathbb{R}, \forall h \in \mathbb{R}^*, \forall t \in [0,1] : \left|\frac{\sin((x+h)t)e^{-t^2} - \sin(xt)e^{-t^2}}{h} - t\cos(xt)e^{-t^2}\right| \leq \frac{|h|}{2}t^2e^{-t^2}$
4. En déduire que pour tout $x \in \mathbb{R}$, pour tout $h \in \mathbb{R}^* : \left|\frac{S(x+h)-S(x)}{h} - C(x)\right| \leq \frac{|h|}{2}\int_0^1 t^2e^{-t^2}dt$.
5. Montrer alors que S est une fonction dérivable sur $\mathbb{R}$ et expliciter sa dérivée S'.

Problème 1

Equation de Pell-Fermat

On admet l'irrationalité de $\sqrt{2}$ et on introduit l'ensemble

$$\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2},\ (a,b) \in \mathbb{Z}^2\right\}$$

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

$(\mathbb{Z}[\sqrt{2}], +, \times)$ est donc un anneau.

2. **a.** Montrer que pour tout $x \in \mathbb{Z}[\sqrt{2}]$, il existe un *unique* couple $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$.

On peut alors définir le *conjugué* de x par $\overline{x} = a - b\sqrt{2}$.

b. Montrer que pour $(x,y) \in \mathbb{Z}[\sqrt{2}]^2$, $\overline{x \times y} = \overline{x} \times \overline{y}$.

3. Pour $x \in \mathbb{Z}[\sqrt{2}]$, on pose $\mathrm{N}(x) = x\overline{x}$.

a. Justifier que pour tout $x \in \mathbb{Z}[\sqrt{2}]$, $\mathrm{N}(x) \in \mathbb{Z}$.

b. Montrer que pour tout $(x,y) \in \left(\mathbb{Z}[\sqrt{2}]\right)^2$, $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$.

c. Montrer que $x \in \mathbb{Z}[\sqrt{2}]$ est inversible dans l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$ si et seulement si $|\mathrm{N}(x)| = 1$.

On note H l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{2}]$. On rappelle qu'alors $(\mathrm{H}, \times)$ est un groupe. H est notamment stable par produit et par inversion. De plus, d'après la question précédente,

$$\mathrm{H} = \left\{x \in \mathbb{Z}[\sqrt{2}], |\mathrm{N}(x)| = 1\right\}$$

4. Soient $x \in \mathrm{H}$ et $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$.

a. Montrer que si $a \geq 0$ et $b \geq 0$, alors $x \geq 1$.

b. Montrer que si $a \leq 0$ et $b \leq 0$, alors $x \leq -1$.

c. Montrer que si $ab \leq 0$, alors $|x| \leq 1$.

5. On note $\mathrm{H}^+ = \mathrm{H} \cap]1, +\infty[$.

a. Soient $x \in \mathrm{H}^+$ et $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Montrer que $a > 0$ et $b > 0$.

b. En déduire que $u = 1 + \sqrt{2}$ est le minimum de H^+.

6. Soit $x \in \mathrm{H}^+$.

a. Montrer qu'il existe $n \in \mathbb{Z}$ tel que $u^n \leq x < u^{n+1}$.

b. Montrer que $x = u^n$.

7. En déduire que $\mathrm{H} = \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$.

Problème 2 Théorème de Fermat de Noël

Le but de ce problème est d'étudier la question posée et résolue par Pierre de Fermat : "quels sont les nombres entiers pouvant s'écrire comme somme de deux carrés d'entiers naturels ?"

Dans tout ce problème dire que l'entier naturel n est somme de deux carrés d'entiers naturels signifie :

$$\exists (x,y) \in \mathbb{N}^2,\ n = x^2 + y^2$$

A-Préliminaires

1. Donner une décomposition de chaque entier entre 0 et 18 comme somme de deux carrés d'entiers naturels lorsque cela vous semble possible.
2. À l'aide d'un tableau de congruences, montrer qu'aucun entier congru à 3 modulo 4 n'est somme de deux carrés d'entiers naturels.
3. On note $\mathcal{P}_{3,4}$ l'ensemble des nombres premiers congrus à 3 modulo 4. Le but de cette question est de montrer que $\mathcal{P}_{3,4}$ est infini. On raisonne par l'absurde en supposant que $\mathcal{P}_{3,4}$ est fini et s'écrit $\mathcal{P}_{3,4} = \{p_i,\ i \in [\![1,n]\!]\}$ où $n \in \mathbb{N}^*$.
   (a) Justifier qu'un produit d'un nombre quelconque d'entiers naturels congrus à 1 modulo 4 est congru à 1 modulo 4.
   (b) On pose $M = \left(4\prod_{i=1}^{n} p_i\right) - 1$.
      i. Montrer que M n'est pas premier.
      ii. Montrer que M possède au moins un diviseur premier congru à 3 modulo 4.
      iii. Conclure.

Remarque : *Plus généralement, si a et b sont deux entiers naturels non nuls et si on note $\mathcal{P}_{a,b}$ l'ensemble des nombres premiers congrus à a modulo b alors le théorème de la progression arithmétique de Dirichlet affirme que :*

$\mathcal{P}_{a,b}$ est infini si et seulement si a et b sont premiers entre eux

Ce théorème est très difficile à démontrer car la méthode vue pour $\mathcal{P}_{3,4}$ ne se généralise pas. Ce résultat n'intervient pas dans la suite du problème.

4. Soit p un nombre premier et $a \in [\![1,p-1]\!]$, montrer qu'il existe un unique $u \in [\![1,p-1]\!]$ tel que $au \equiv 1\ [p]$.
   On notera dans toute la suite cet inverse $\mathbf{a^{-1}}$.
5. En reprenant les notations de la question précédente, montrer qu'il existe un unique $t \in [\![1,p-1]\!]$ tel que $a + t \equiv 0\ [p]$.
   On notera dans toute la suite cet opposé $\mathbf{-a}$.

Remarque : *Les deux questions précédentes permettent de justifier que l'ensemble $[\![0,p-1]\!]$ muni de l'addition et de la multiplication modulo p est un corps. On le note usuellement $\mathbb{Z}/p\mathbb{Z}$.*

B-Une équation modulaire

Le but de ce paragraphe est de démontrer le lemme suivant :

Lemme 1 : L'équation $s^2 \equiv -1\ [p]$ d'inconnue s possède :
- Deux solutions appartenant à $[\![1, p-1]\!]$ lorsque p est premier congru à 1 modulo 4.
- Aucune solution si p est premier congru à 3 modulo 4.
- Une unique solution appartenant à $[\![1, p-1]\!]$ si $p = 2$.

1. Démontrer le cas $p = 2$.
2. Soit p un nombre premier impair. On considère la relation binaire définie pour tous $(x, y) \in [\![1, p-1]\!]^2$ par :

$$x \mathcal{R} y \Leftrightarrow x = y \text{ ou } x = -y \text{ ou } x = y^{-1} \text{ ou } x = -y^{-1}$$

Les notations $-x$ et x^{-1} sont celles introduites dans la partie A.

   (a) Montrer que $\mathcal{R}$ est une relation d'équivalence.

   (b) Soit $x \in [\![1, p-1]\!]$. Justifier que la classe de x est $\text{Cl}(x) = \{x, -x, x^{-1}, -x^{-1}\}$.

   (c) Donner les classes d'équivalence dans le cas où $p = 11$ puis dans le cas où $p = 13$.

3. Dans cette question, on cherche à préciser les cas où certains éléments de la classe de x sont égaux :

   (a) Montrer que $x = -x$ est impossible.

   (b) Montrer que $x = x^{-1}$ équivaut à $x = 1$ ou $x = p-1$.

   (c) Montrer que $x = -x^{-1}$ possède 0 ou 2 solutions.

   (d) En déduire que l'ensemble $[\![1, p-1]\!]$ est partitionné par les classes d'équivalence de la relation $\mathcal{R}$ en sous-ensembles ayant 4 éléments et un ou deux sous-ensembles ayant 2 éléments.

4. En déduire le lemme annoncé.

C-Nombres premiers somme de deux carrés

Le but de ce paragraphe est de démontrer le lemme suivant :

Lemme 2 : Tout nombre premier congru à 1 modulo 4 est somme de deux carrés d'entiers naturels.

Soit p un nombre premier congru à 1 modulo 4. On note dans ce paragraphe $\Gamma = [\![0, E(\sqrt{p})]\!]$ où E désigne la partie entière.

1. On pose $\gamma =$Card (Γ^2). Donner γ et montrer que $\gamma > p$.
2. Soit $s \in \mathbb{Z}$ fixé.

   (a) Montrer qu'il existe deux couples disctincts (x, y) et (x', y') de Γ^2 tels que $x - sy \equiv x' - sy'\ [p]$.

   (b) On pose $\widehat{x} = |x - x'|$ et $\widehat{y} = |y - y'|$. Montrer que $(\widehat{x}, \widehat{y}) \in \Gamma^2$ et que $\widehat{x} \equiv \varepsilon s \widehat{y}\ [p]$ avec $\varepsilon \in \{-1, 1\}$.

3. En choisissant s de façon à utiliser le lemme 1, montrer que $\widehat{x}^2 + \widehat{y}^2 = p$.
4. En déduire les nombres premiers qui sont somme de deux carrés d'entiers naturels.

D-Entiers somme de deux carrés

Nous allons dans cette partie démontrer le théorème suivant qui apporte la réponse au problème initial.

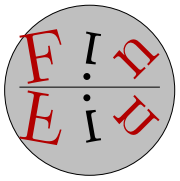
Théorème : Un entier naturel $n \geq 2$ peut s'écrire comme somme de deux carrés d'entiers naturels si et seulement si tous les facteurs premiers congrus à 3 modulo 4 dans la décomposition de n en facteurs premiers apparaissent à une puissance paire.

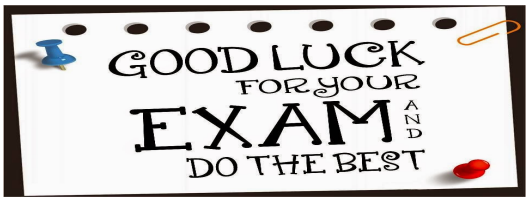
1. Montrer que si $m = x^2 + y^2$ et $n = t^2 + u^2$ avec m, n, x, y, t et u des entiers naturels, alors mn est également somme de deux carrés. On trouvera cette écriture explicitement grâce à une factorisation astucieuse.
2. Montrer que si $n \in \mathbb{N}$ est somme de deux carrés alors nz^2 où $z \in \mathbb{N}$ est également somme de deux carrés.
3. Montrer que si tous les facteurs premiers congrus à 3 modulo 4 dans la décomposition de n en facteurs premiers apparaissent à une puissance paire alors n s'écrit comme somme de deux carrés d'entiers naturels.
4. Montrons à présent la réciproque du théorème. Soit $n = x^2 + y^2$ avec $n \geq 2$ et $(x, y) \in \mathbb{N}^2$. Notons p un diviseur premier de n congru à 3 modulo 4.
   (a) Montrer que l'hypothèse $x \not\equiv 0\ [p]$ est contradictoire avec le lemme 1, on pourra utiliser x^{-1}.
   (b) En déduire que p^2 divise n.
   (c) Montrer que $\dfrac{n}{p^2}$ est également somme de deux carrés d'entiers naturels.
   (d) Conclure quant à la réciproque du théorème annoncé.
5. Voici une application du théorème : on note $(p_k)_{k\geq 1}$ la liste des nombres premiers impairs donnés dans l'ordre croissant. En considérant $M_k = \left(\prod_{i=1}^{k} p_i\right)^2 + 2^2$, montrer qu'il y a une infinité de nombres premiers congrus à 1 modulo 4.
6. Montrer qu'un entier congru à 7 modulo 8 ne peut être la somme de trois carrés d'entiers naturels.

Remarque : *Un théorème dû à Lagrange assure que tout entier naturel est somme de 4 carrés d'entiers naturels.*

E-Une dernière surprise

■ À l'aide de Python, déterminer le nombre moyen de décompositions d'un entier naturel n comme somme de deux carrés d'entiers **relatifs** pour n allant de 0 à 100000. Que peut-on conjecturer ? On transmettra par mail les programmes ayant servis à répondre à cette question.





Corrigé

EXERCICE 1

Soit α l'une des deux racines complexes du polynôme $P(z) = z^2 + z + 2$.
On désigne par $\mathbf{Z}[\alpha]$ l'ensemble des nombres complexes défini par

$$\boxed{\mathbf{Z}[\alpha] = \left\{p + \alpha q\,;\ (p,q) \in \mathbf{Z}^2\right\}}$$

0. **remarque préliminaire** P est un polynôme à coefficients réels de discriminant strictement négatif. Il admet deux racines complexes conjuguées qui vérifient

$$\left\|\begin{array}{lcr} \alpha + \bar{\alpha} & = & -1 \\ \alpha \times \bar{\alpha} & = & 2 \\ \alpha^2 + \alpha + 2 & = & 0 \end{array}\right.$$

1. Pour montrer que $\mathbf{Z}[\alpha]$ est un sous-anneau de $\mathbf{C}$, utilisons la **caractérisation des sous-anneaux** :

- $1 = 1 + 0\ \alpha \in \mathbf{Z}[\alpha]$
- soit $(z_1, z_2) \in \mathbf{Z}[\alpha]^2$. Par construction, il existe des couples (p_1, q_1) et (p_2, q_2) d'entiers relatifs tels que $z_1 = p_1 + \alpha q_1$ et $z_2 = p_2 + \alpha q_2$. On a alors

$$\begin{aligned} z_1 - z_2 &= \left(p_1 + \alpha q_1\right) - \left(p_2 + \alpha q_2\right) \\ &= \underbrace{(p_1 - p_2)}_{\in \mathbf{Z}} + \alpha \underbrace{(q_1 - q_2)}_{\in \mathbf{Z}} \end{aligned}$$

- soit $(z_1, z_2) \in \mathbf{Z}[\alpha]^2$. Avec les notations précédentes,

$$\begin{aligned} z_1 \times z_2 &= \left(p_1 + \alpha q_1\right) \times \left(p_2 + \alpha q_2\right) \\ &= p_1 p_2 + \alpha^2 q_1 q_2 + \alpha(p_1 q_2 + p_2 q_1) \\ &= p_1 p_2 - (\alpha + 2) q_1 q_2 + \alpha(p_1 q_2 + p_2 q_1) \\ &= \underbrace{(p_1 p_2 - 2 q_1 q_2)}_{\in \mathbf{Z}} + \alpha \underbrace{(p_1 q_2 + p_2 q_1 - q_1 q_2)}_{\in \mathbf{Z}} \end{aligned}$$

D'après la **caractérisation des sous-anneaux**, $\mathbf{Z}[\alpha]$ est uun sous-anneau de $(\mathbf{C}, +, \times)$. ▲

2.a. D'après la remarque préliminaire (somme et produit des racines) $\alpha + \bar{\alpha} = -1$ et $\alpha\,\bar{\alpha} = 2$. ▲

b. Soit $z \in \mathbf{Z}[\alpha]$. Par construction, il existe $(p, q) \in \mathbf{Z}^2$ tel que $z = p + \alpha q$. En utilisant la remarque préliminaire (ou la question précédente), il vient

$$\begin{aligned} \bar{z} &= \overline{p + \alpha q} = p + \bar{\alpha} q \\ &= p - (\alpha + 1) q = \underbrace{(p - q)}_{\in \mathbf{Z}} - \alpha \underbrace{q}_{\in \mathbf{Z}} \end{aligned}$$

▲

c. Soit $z \in \mathbf{Z}[\alpha]$. Avec les notations précédentes, on a

$$\begin{aligned} z\,\bar{z} &= (p+\alpha q)(p+\bar{\alpha} q) \\ &= p^2 + |\alpha|^2 q^2 + pq(\alpha + \bar{\alpha}) \\ &= p^2 + 2q^2 - pq \end{aligned}$$

Sous cette forme il apparait clairement que $z\,\bar{z}$ est un entier relatif. Comme de plus $z\,\bar{z} = |z]|^2$, ce produit est positif. Ainsi $z\,\bar{z} \in \mathbf{N}$. ▲

3.a. Soit $z = p + \alpha q$ un élément de $\mathbf{Z}[\alpha]$.

- Supposons que $z \in \mathbf{Z}[\alpha]^\times$ soit inversible. Notons $w = z^{-1}$. Comme $z\,w = 1$ il vient
$$|z|^2\,|w|^2 = 1$$
D'après la question précédente, $|z|^2$ et $|w|^2$ sont des entiers naturels, qui divisent 1. Ceci entraîne que $|z|^2 = |w|^2 = 1$. En utilisant l'expression obtenue à la question précédente pour le produit $z\,\bar{z}$, il s'ensuit :
$$p^2 + 2q^2 - pq = 1$$
- Réciproquement, supposons que $p^2 + 2q^2 - pq = 1$. Compte-tenu de l'expression obtenue à la question précédente pour le produit $z\,\bar{z}$, l'hypothèse se traduit par $z\,\bar{z} = 1$. Par conséquent, z est inversible et son inverse est son conjugué $\bar{z}$.

Par double-implication on a prouvé que z est inversible dans $\mathbf{Z}[\alpha]$ *si et seulement si* (p, q) vérifie :

$$p^2 + 2q^2 - pq = 1 \qquad (2)$$

▲

b. Soit $(p, q) \in \mathbf{Z}^2$ tel que $pq < 0$. Montrons par l'absurde que (p, q) ne peut être solution de (2).
Supposons *au contraire* que (p, q) vérifie (2). En ce cas, $0 \leqslant p^2 + 2q^2 = 1 + pq$. Comme pq est strictement négatif, il en résulte successivement que $0 \leqslant p^2 + 2q^2 < 1$, puis que $p = q = 0$. Substituons dans (2) pour obtenir $0 = 1$. *Absurde !*
Ainsi, l'équation (2) est impossible lorsque $pq < 0$. ▲

c. Soit $(p, q) \in \mathbf{Z}^2$ tel que $pq > 0$. Montrons par l'absurde que (p, q) ne peut être solution de (2).
Supposons *au contraire* que (p, q) vérifie (2).

$$\begin{aligned} p^2 + 2q^2 - pq = 1 &\iff p^2 - 2pq + q^2 + q^2 + pq = 1 \\ &\iff (p-q)^2 + q^2 = 1 - pq. \end{aligned}$$

Comme précédemment, l'encadrement $0 \leqslant (p-q)^2 + q^2 < 1$ entraîne que $q = 0$ et $p = q$, soit $p = 0$ et $q = 0$. Substituons dans (2) pour obtenir $0 = 1$. *Absurde !*
Ainsi, l'équation (2) est impossible lorsque $pq > 0$. ▲

d. D'après les questions précédentes, $\mathbf{Z}[\alpha]^\times \subset \{p+\alpha q \mid pq = 0\}$. Réciproquement,

- si $p = 0$, l'équation (2) s'écrit $2q^2 = 1$ qui est impossible dans $\mathbf{Z}$.

- si $q=0$, l'équation (2) est équivalent à $p^2=1$ qui admet pour solutions $+1$ et -1.

Finalement

$$\boxed{\mathbf{Z}[\alpha]^\times=\{-1,+1\}}$$

▲

EXERCICE 2

Soit $(F_n)_{n\in\mathbf{N}}$ la suite définie par les relations $F_0=0$, $F_1=1$, et $\forall n\in\mathbf{N}^\star$, $F_{n+1}=F_n+F_{n-1}$.

1. Montrons par récurrence sur $n\in\mathbf{N}^\star$ que $F_{n+1}F_{n-1}-F_n^2=(-1)^n$.

- **Initialisation :** pour $n=1$, on a $F_2\times F_0-F_1^2=0-1=-1$.
- **Hérédité :** soit $n\in\mathbf{N}^\star$ tel que $F_{n+1}F_{n-1}-F_n^2=(-1)^n$. Utilisons les relations $F_{n+1}=F_n+F_{n-1}$ et $F_{n+2}=F_{n+1}+F_n$. Il vient

$$\begin{aligned}F_{n+2}F_n-F_{n+1}^2&=[F_{n+1}+F_n]\times F_n-[F_n+F_{n-1}]\times F_{n+1}\\&=F_n^2-F_{n+1}F_{n-1}\\&=-\big[F_{n+1}F_{n-1}-F_n^2\big]\end{aligned}$$

  Par hypothèse de récurrence, il en résulte que $F_{n+2}F_n-F_{n+1}^2=(-1)^{n+1}$.
- **Conclusion :** par récurrence, on a montré que

$$\forall n\in\mathbf{N}^\star,\ F_{n+1}F_{n-1}-F_n^2=(-1)^n.$$

  En particulier, en posant pour tout entier $n\in\mathbf{N}^\star$, $U_n=(-1)^nF_{n-1}$, on a obtenu les relations

$$\forall n\in\mathbf{N}^\star,\quad U_{n+1}F_n+U_nF_{n+1}=1.$$

  Le **Théorème de Bezout** permet alors de conclure que pour tout entier naturel $n\in\mathbf{N}^\star$, les nombres de Fibonacci F_n et F_{n+1} sont premiers entre eux.

2. Notons pour $n\in\mathbf{N}$,

$$\mathcal{P}(n)\qquad\forall p\in\mathbf{N}^\star,\qquad F_{n+p}=F_pF_{n+1}+F_{p-1}F_n$$

On montre par récurrence sur n que $\forall n\in\mathbf{N},\mathcal{P}(n)$.

- **Initialisation :** lorsque $n=0$, on a bien pour tout entier $p\in\mathbf{N}^\star$ $F_p=F_p\times F_1+F_0F_{p-1}$ puisque $F_0=0$ et $F_1=1$.
- **Hérédité :** soit $n\in\mathbf{N}$ tel que $\mathcal{P}(n)$. Considérons un entier $p\in\mathbf{N}^\star$. *A fortiori* $p+1$ est un entier naturel non nul et l'hypothèse de récurrence – qui est en l'occurrence une hypothèse de type universel – appliquée à $p+1$, donne :

$$\begin{aligned}F_{(n+1)+p}&=F_{n+(p+1)}=F_{p+1}F_{n+1}+F_pF_n\\&=[F_p+F_{p-1}]F_{n+1}+F_pF_n\\&=F_p\times[F_n+F_{n+1}]+F_{p-1}\times F_{n+1}\\&=F_pF_{n+2}+F_{p-1}F_{n+1}\end{aligned}$$

- **Conclusion :**par récurrence sur n, on a montré que

$$\forall (n,p) \in \mathbf{N} \times \mathbf{N}^\star, \qquad F_{n+p} = F_p F_{n+1} + F_{p-1} F_n$$

Soit $(n,p) \in \mathbf{N} \times \mathbf{N}^\star$. On sait que $F_{n+p} = F_p F_{n+1} + F_{p-1} F_n$ et on montre que $PGCD(F_n, F_p) = PGCD(F_{n+p}, F_p)$. Pour ce faire, on vérifie, par double-inclusion que $\mathcal{D}(F_n, F_p) = \mathcal{D}(F_{n+p}, F_p)$.

$\boxed{\subset}$ si d divise à la fois F_n et F_p, d'après la relation précédente il divise aussi $F_{n+p} = F_p F_{n+1} + F_{p-1} F_n$. D'où l'on tire que $d \in \mathcal{D}(F_{n+p}, F_p)$.

$\boxed{\supset}$ si d divise F_p et F_{n+p}. Alors, d'une part d divise aussi $F_{p-1} F_n = F_{n+p} - F_p F_{n+1}$. D'autre part, d divise F_p tandis que F_p et F_{p-1} sont premiers entre eux (d'après la première question), donc d et F_{p-1} sont aussi premiers entre eux. Finalement, d'après le **théorème de Gauss** on peut conclure que d doit diviser F_n. Il s'agit donc bien d'un diviseur commun à F_p et F_n.

Par double-inclusion, on a bien établi que $\mathcal{D}(F_n, F_p) = \mathcal{D}(F_{n+p}, F_p)$. En particulier, ces ensembles ont donc même plus grand élément : $PGCD(F_n, F_p) = PGCD(F_{n+p}, F_p)$

3. Soit $(m,n) \in \mathbf{N}^2$ un couple d'entiers non tous les deux nuls. On suppose sans perte de généralité que $n \neq 0$. Effectuons la division euclidienne de m par n. On a

$$m = nq + r, \text{ où } 0 \leqslant r \leqslant n-1$$

En itérant le résultat de la question précédente, on a

$$\begin{aligned} PGCD(F_n, F_r) &= PGCD(F_n, F_{r+n}) = \cdots = PGCD(F_n, F_{r+nq}) \\ &= PGCD(F_n, F_m) \end{aligned}$$

Ainsi, pour tout couple d'entiers naturels non nuls, on a

$$PGCD(F_m, F_n) = PGCD(F_n, F_r),$$

où r est le reste de la division euclidienne de m par n.

Finalement, on conclut à l'aide de l'algorithme d'Euclide pour le calcul de $d = PGCD(m,n)$: si $a_0 \geqslant a_1 > \cdots > a_m = d > 0$ est la suite des restes non nuls successivement apparus, on a d'après ce qui précède

$$\begin{aligned} PGCD(F_m, F_n) &= PGCD(F_{a_0}, F_{a_1}) \\ &= PGCD(F_{a_1}, F_{a_2}) \\ &\vdots \\ &= PGCD(F_{a_m}, 0) = F_{PGCD(m,n)} \end{aligned}$$

▲

Problème 1

1. Clairement $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$.
$1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$. Il existe donc $(a, b, c, d) \in \mathbb{Z}^4$ tel que $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$.
Alors $x - y = (a - c) + (b - d)\sqrt{2}$ et $(a - c, b - d) \in \mathbb{Z}^2$ donc $x - y \in \mathbb{Z}[\sqrt{2}]$.
Également, $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$ et $(ac + 2bd, ad + bc) \in \mathbb{Z}^2$ donc $xy \in \mathbb{Z}[\sqrt{2}]$.
Ainsi $\mathbb{Z}[\sqrt{2}]$ est donc un sous-anneau de $(\mathbb{R}, +, \times)$.

2. **a.** Soit $x \in \mathbb{Z}[\sqrt{2}]$. L'existence d'un couple $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$ découle simplement de la définition de $\mathbb{Z}[\sqrt{2}]$. Soit maintenant $(c, d) \in \mathbb{Z}^2$ tel que

$$x = a + b\sqrt{2} = c + d\sqrt{2}$$

On a donc $(a - c) = (d - b)\sqrt{2}$. Si $d \neq b$, $\sqrt{2}$ serait rationnel. Ainsi $b = d$ et par suite $a = c$. D'où l'unicité du couple (a, b).

b. Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]$. Il existe donc $(a, b, c, d) \in \mathbb{Z}^4$ tel que $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$. Alors

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

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

On a donc bien $\overline{x \cdot y} = \overline{x} \cdot \overline{y}$.

3. **a.** Soient $x \in \mathbb{Z}[\sqrt{2}]$ et $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Alors $\mathrm{N}(x) = a^2 - 2b^2 \in \mathbb{Z}$.

b. Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$. Alors, en utilisant la question précédente

$$\mathrm{N}(xy) = xy\overline{x \cdot y} = xy\overline{x} \cdot \overline{y} = x\overline{x}y\overline{y} = \mathrm{N}(x)\mathrm{N}(y)$$

c. Soit $x \in \mathbb{Z}[\sqrt{2}]$.
Supposons x inversible. Il existe donc $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. Ainsi $\mathrm{N}(xy) = \mathrm{N}(1) = 1$. D'après la question précédente, $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ d'où $\mathrm{N}(x)\mathrm{N}(y) = 1$. Puisque $\mathrm{N}(x)$ et $\mathrm{N}(y)$ sont entiers, on a donc $\mathrm{N}(x) = \pm 1$ i.e. $|\mathrm{N}(x)| = 1$.
Réciproquement soit $x \in \mathbb{Z}[\sqrt{2}]$ tel que $|\mathrm{N}(x)| = 1$. Si $\mathrm{N}(x) = 1$, alors $x\overline{x} = 1$ donc x est inversible (d'inverse $\overline{x}$). Si $\mathrm{N}(x) = -1$, alors $x(-\overline{x}) = 1$ donc x est inversible (d'inverse $-\overline{x}$).

4. **a.** Supposons $a \geq 0$ et $b \geq 0$. On ne peut avoir $(a, b) = (0, 0)$ car $0 \notin \mathrm{H}$. Un des deux entiers naturels a et b est donc non nul. Ainsi $a \geq 1$ ou $b \geq 1$ et, dans les deux cas, $x \geq 1$.

b. Supposons $a \leq 0$ et $b \leq 0$. On ne peut avoir $(a, b) = (0, 0)$ car $0 \notin \mathrm{H}$. Un des deux entiers a et b est donc non nul. Ainsi $a \leq -1$ ou $b \leq -1$ et, dans les deux cas, $x \leq -1$.

c. Supposons $ab \leq 0$. Alors $a(-b) \geq 0$. Les deux questions précédentes montrent que $|\overline{x}| \geq 1$. Puisque $|\mathrm{N}(x)| = |x||\overline{x}| = 1$, $|x| \leq 1$.

5. **a.** Puisque $x > 1$, la question précédente montre qu'on ne peut avoir $a \leq 0$ et $b \leq 0$ ni $ab \leq 0$. C'est donc que nécessairement $a > 0$ et $b > 0$.

b. $u \in \mathrm{H}^+$ car $u > 1$ et $\mathrm{N}(u) = -1$.
Soient $x \in \mathrm{H}^+$ et $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. D'après la question précédente, $a \geq 1$ et $b \geq 1$ donc $x \geq u$. Ainsi u est un minorant de H^+.
u est donc le minimum de H^+.

6. **a.** Il suffit de poser $n = \left\lfloor \frac{\ln x}{\ln u} \right\rfloor$. On a alors

$$n \leq \frac{\ln x}{\ln u} < n + 1$$

ou encore

$$n \ln(u) \leq \ln(x) < (n + 1) \ln u$$

car $\ln u > 0$. Puis par stricte croissance de l'exponentielle

$$u^n \leq x < u^{n+1}$$

b. Supposons $x \neq u^n$. Alors

$$u^n < x < u^{n+1}$$

puis

$$1 < \frac{x}{u^n} < u$$

car $u > 0$. Or H et $u \in H$ donc $u^n \in H$. On sait également que $x \in H$ donc $\frac{x}{u^n} \in H$ car H est un groupe. Or $\frac{x}{u^n} > 1$ donc $\frac{x}{u^n} \in H^+$. Or $\frac{x}{u^n} < u$, ce qui contredit la minimalité de u.
On a donc prouvé que $x = u^n$.

7. On sait que $u \in H$ donc $u^n \in H$ pour tout $n \in \mathbb{Z}$ car H est un groupe. Puisque $-1 \in H$, on a également $-u^n \in H$ pour tout $n \in \mathbb{Z}$. Ainsi

$$\{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\} \subset H$$

Soit maintenant $x \in H$. On sait que $0 \notin H$ donc $x \neq 0$.

- Si $x > 1$, alors $x \in H^+$ et il existe donc $n \in \mathbb{Z}$ tel que $x = u^n$ d'après la question précédente.
- Si $x = 1$, alors $x = u^0$.
- Si $0 < x < 1$, alors $\frac{1}{x} \in H^+$ donc il existe $n \in \mathbb{Z}$ tel que $\frac{1}{x} = u^n$ i.e. $x = u^{-n}$.
- Si $x < 0$, alors $-x \in H$ et $-x > 0$, et les cas précédents montrent l'existence d'un $n \in \mathbb{Z}$ tel que $-x = u^n$ i.e. $x = -u^n$.

On a donc prouvé que

$$H \subset \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$$

Par double inclusion

$$H = \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$$

Problème 2

Pierre de Fermat est un magistrat français du XVII ième siècle, il est surnommé "le prince des amateurs". On lui doit de nombreux résultats mathématiques, notamment en arithmétique. Il s'est également intéressé aux sciences physiques avec le principe de Fermat en optique.

A-Préliminaires

1. On a les décompositions suivantes :

$$\begin{array}{l|l|l} 0=0^2+0^2 & 5=1^2+2^2 & 13=2^2+3^2 \\ 1=0^2+1^2 & 8=2^2+2^2 & 16=0^2+4^2 \\ 2=1^2+1^2 & 9=0^2+3^2 & 17=1^2+4^2 \\ 4=0^2+2^2 & 10=1^2+3^2 & 18=3^2+3^2 \end{array}$$

Par contre 3, 6, 7, 11, 12, 14 et 15 ne semblent pas s'écrire comme somme de deux carrés d'entiers naturels.

Il semble difficile, même avec ces quelques exemples, de trouver une règle générale pour savoir quels sont les entiers qui s'écrivent comme somme de deux carrés d'entiers naturels.

2. Soit $x \in \mathbb{N}$, examinons les valeurs possibles de x et x^2 modulo 4. On a :

x modulo 4	x^2 modulo 4
0	0
1	1
2	0
3	1

Ainsi si $(x,y) \in \mathbb{N}^2$, on a x^2+y^2 qui peut être congru à 0, 1 ou 2 modulo 4. Ceci démontre que :

> un entier congru à 3 modulo 4 ne peut pas s'écrire comme somme de deux carrés d'entiers naturels

Ce premier résultat permet d'expliquer que 3, 7, 11 et 15 ne sont pas somme de deux carrés d'entiers naturels.

3. (a) Démontrons le résultat par récurrence sur le nombre de facteurs dans le produit en question. Pour $r \in \mathbb{N}^*$, on considère :

$$\mathcal{H}_r \ : \text{ Si } (t_i)_{1\leq i\leq r} \text{ est une famille d'entiers congrus à 1 modulo 4 alors } \prod_{i=1}^{r} t_i \text{ est congru à 1 modulo 4}$$

► Si $r=1$, le résultat est évident.

► On suppose que $\mathcal{H}_r$ est vraie pour $r \in \mathbb{N}^*$ fixé. Soit $(t_i)_{1\leq i\leq r+1}$ une famille de $r+1$ entiers naturels congrus à 1 modulo 4. En utilisant l'hypothèse de récurrence, on a :

$$\prod_{i=1}^{r} t_i \equiv 1\ [4] \quad \text{et } t_{r+1} \equiv 1\ [4]$$

Par produit de ces deux congruences, il vient :

$$\prod_{i=1}^{r+1} t_i = \Big(\prod_{i=1}^{r} t_i\Big) t_{r+1} \equiv 1\times 1\ [4]$$

Ce qui démontre que $\mathcal{H}_{r+1}$ est vraie et achève la récurrence.

> Un produit d'entiers naturels congrus à 1 modulo 4 est congru à 1 modulo 4

(b) i. Remarquons que M est congru à 3 modulo 4 puisque :

$$M = \left(4\prod_{i=1}^{n} p_i\right) - 1 \equiv 0 - 1 \equiv 3\ [4]$$

Par l'absurde supposons que M soit un nombre premier. Comme il est congru à 3 modulo 4, c'est l'un des p_i pour un certain $i \in [\![1, n]\!]$. Ceci est absurde puisque M est clairement strictement supérieur à chacun des p_i où $i \in [\![1, n]\!]$.

M n'est pas premier

ii. Le nombre M est impair, il se décompose comme un produit de facteurs premiers impairs. Si tous les diviseurs premiers qui interviennent dans la décomposition de M sont congrus à 1 modulo 4 alors, d'après la question (a), M est également congru à 1 modulo 4, ce qui n'est pas le cas.

M possède un diviseur premier congru à 3 modulo 4

iii. Le diviseur premier de M congru à 3 modulo 4 trouvé à la question précédente est l'un des $(p_i)_{1\leq i\leq n}$, notons le p_{i_0} où $i_0 \in [\![1, n]\!]$.
On a :

$$p_{i_0} \Big| 4\prod_{i=1}^{n} p_i, \text{ c'est-à-dire } p_{i_0}|M+1 \text{ et } p_{i_0}|M$$

Ainsi : $p_{i_0}|(M+1-M)$ ce qui est absurde. L'hypothèse selon laquelle $\mathcal{P}_{3,4}$ contient un nombre fini d'éléments est fausse et par suite :

$\mathcal{P}_{3,4}$ est infini

4. ► **Existence.** Soit p un nombre premier et $a \in [\![1, p-1]\!]$. Les entiers a et p sont premiers entre eux, ce qui nous permet d'appliquer le théorème de Bézout :

$$\exists(\widehat{u}, \widehat{v}) \in \mathbb{Z}^2, \text{ tels que } a\widehat{u} + p\widehat{v} = 1$$

En prenant cette relation modulo p cela donne $a\widehat{u} \equiv 1\ [p]$. Cependant rien ne garantit que $\widehat{u}$ convienne puisque l'on ne sait pas si $\widehat{u} \in [\![1, p-1]\!]$. Pour contourner ce problème, on considère le reste de la division euclidienne de $\widehat{u}$ par p que l'on note u. On a $\widehat{u} \equiv u\ [p]$, ainsi $au \equiv 1\ [p]$. D'après le théorème de la division euclidienne, on sait que $u \in [\![0, p-1]\!]$, mais $u \neq 0$ sinon $au \equiv 0\ [p]$. Finalement $u \in [\![1, p-1]\!]$ et $au \equiv 1\ [p]$.
► **Unicité.** Soient $(u, u') \in [\![1, p-1]\!]^2$ tels que $au \equiv 1\ [p]$ et $au' \equiv 1\ [p]$. On a : $au \equiv au'\ [p]$, c'est-à-dire $a(u-u') \equiv 0\ [p]$. Ainsi $p|a(u-u')$ mais p est premier avec a, ce qui implique via le théorème de Gauss que $p|u-u'$. Cependant :

$$1 \leq u \leq p-1 \text{ et } 1 \leq u' \leq p-1 \text{ implique que } -(p-2) \leq u-u' \leq p-2$$

En résumé $u-u'$ est un multiple de p et $u-u' \in [\![-(p-2), p-2]\!]$, nécessairement $u-u'=0$, c'est-à-dire $u=u'$. Ce qui démontre l'unicité.

Si p est premier : pour tout $a \in [\![1, p-1]\!]$, a possède un unique inverse modulo p

5. ► **Existence.** Soit p un nombre premier et $a \in [\![1, p-1]\!]$. On va voir que $t = p - a$ répond à la question, en effet :

$$t + a = p - a + a = p \equiv 0\ [p]$$

et $t \in [\![1, p-1]\!]$ puisque :

$$1 \leq a \leq p-1 \Leftrightarrow 1 \leq p-a \leq p-1$$

► **Unicité.** Soient $(t, t') \in [\![1, p-1]\!]^2$ tels que $a+t \equiv 0\ [p]$ et $a+t' \equiv 0\ [p]$. On a $t+a \equiv t'+a\ [p]$ ce qui implique que $t \equiv t'\ [p]$. Or t et t' sont deux éléments de $[\![1, p-1]\!]$ donc $t = t'$. Ce qui démontre l'unicité.

Si p est premier : pour tout $a \in [\![1, p-1]\!]$, a possède un unique opposé modulo p

B-Une équation modulaire

1. Si $p = 2$, on a : $[\![1, p-1]\!] = \{1\}$ et $1^2 = 1 \equiv -1\ [2]$. Ce qui démontre le lemme 1 dans le cas où $p = 2$.
2. (a) Observons d'abord que si $y \in [\![1, p-1]\!]$ alors $-y$, y^{-1} et $-y^{-1}$ sont définis de façon unique et appartiennent à $[\![1, p-1]\!]$ d'après les questions 4. et 5. de la partie précédente. Vérifions les propriétés requises pour avoir une relation d'équivalence.

► **Réflexivité**. Soit $x \in [\![1, p-1]\!]$, on a $x\mathcal{R}x$ puisque $x = x$. La relation binaire $\mathcal{R}$ est réflexive.

► **Symétrie**. Soient $(x, y) \in [\![1, p-1]\!]^2$, tels que $x\mathcal{R}y$. Il y a 4 cas qui peuvent se présenter :

• Si $x = y$ alors $y = x$ et par suite $y\mathcal{R}x$.

• Si $x = -y$, en revenant à la définition de l'opposé donnée dans la question 5. de la partie précédente, on a $x + y \equiv 0\ [p]$, c'est-à-dire $y + x \equiv 0\ [p]$. Ce qui démontre que $y = -x$ et par suite $y\mathcal{R}x$.

• Si $x = y^{-1}$, en revenant à la définition de l'inverse donnée dans la question 4. de la partie précédente, on a $xy \equiv 1\ [p]$, c'est-à-dire $yx \equiv 1\ [p]$. Ce qui démontre que $y = x^{-1}$ et par suite $y\mathcal{R}x$.

• Si $x = -y^{-1}$, on a $x + y^{-1} \equiv 0\ [p]$ donc $y^{-1} = -x$. Ceci implique que $y \times (-x) \equiv 1\ [p]$ ou encore $y = (-x)^{-1} = -x^{-1}$. Ce qui démontre que $y\mathcal{R}x$.

► **Transitivité.** Soient $(x, y, z) \in [\![1, p-1]\!]^3$, on suppose que $x\mathcal{R}y$ et $y\mathcal{R}z$. Il y a 16 cas à considérer qui peuvent être résumés dans le tableau suivant.

	$y = z$	$y = -z$	$y = z^{-1}$	$y = -z^{-1}$
$x = y$	$x = z$	$x = -z$	$x = z^{-1}$	$x = -z^{-1}$
$x = -y$	$x = -z$	$x = z$	$x = -z^{1}$	$x = z^{-1}$
$x = y^{-1}$	$x = z^{-1}$	$x = -z^{-1}$	$x = z$	$x = -z$
$x = -y^{1}$	$x = -z^{-1}$	$x = z^{-1}$	$x = -z$	$x = z$

Dans tous les cas, on a $x\mathcal{R}z$.

$\mathcal{R}$ est une relation d'équivalence

(b) Soit $x \in [\![1, p-1]\!]$, par définition de la classe d'équivalence de x, on a : $\mathrm{Cl}(x) = \{y \in [\![1, p-1]\!],\ x\mathcal{R}y\}$. On a :

$$x\mathcal{R}y \Leftrightarrow x = y \text{ ou } x = -y \text{ ou } x = y^{-1} \text{ ou } x = -y^{-1}$$

Ce qui démontre que :

$$\boxed{\mathrm{Cl}(x) = \{x, -x, x^{-1}, -x^{-1}\}}$$

(c) ► Pour $p = 11$, on a :

- $\mathrm{Cl}(1) = \{1, -1, 1^{-1}, -1^{-1}\} = \{1, 10\}$ car :

$$1 + 10 \equiv 0\ [11] \text{ donc } -1 = 10$$

$$1 \times 1 \equiv 1\ [11] \text{ donc } 1^{-1} = 1$$

$$-1^{-1} \equiv -1 \equiv 10\ [11] \text{ donc } -1^{-1} = 10$$

- $\mathrm{Cl}(2) = \{2, 9, 6, 5\}$ car :

$$2 + 9 \equiv 0\ [11]$$

$$2 \times 6 \equiv 1\ [11]$$

$$9 \times 5 \equiv 1\ [11]$$

- $\mathrm{Cl}(3) = \{3, 8, 4, 7\}$ car :

$$3 + 8 \equiv 0\ [11]$$

$$3 \times 4 \equiv 1\ [11]$$

$$8 \times 7 \equiv 1\ [11]$$

$$\boxed{\text{Il y a trois classes d'équivalence : } \{1, 10\},\ \{2, 9, 6, 5\} \text{ et } \{3, 8, 4, 7\}}$$

► Pour $p = 13$, avec le même type de calculs, on trouve :

$$\boxed{\text{qu'il y a quatre classes d'équivalence : } \{1, 12\},\ \{2, 11, 7, 6\},\ \{3, 10, 9, 4\} \text{ et } \{5, 8\}}$$

3. (a) Soit $x \in [\![1, p-1]\!]$, on suppose que $x = -x$. Par définition de $-x$ cela signifie que $x + x \equiv 0\ [p]$. C'est-à-dire que $p|2x$, or p est impair donc il est premier avec 2, en vertu du théorème de Gauss ceci entraîne que $p|x$. Ceci est absurde puisque $x \in [\![1, p-1]\!]$.

$$\boxed{\forall x \in [\![1, p-1]\!],\ x \neq -x}$$

(b) Soit $x \in [\![1, p-1]\!]$, on suppose que $x = x^{-1}$. Par définition de x^{-1} cela signifie que $x^2 \equiv 1\ [p]$. C'est-à-dire que $p|x^2 - 1 = (x+1)(x-1)$, comme p est premier ceci entraîne que $p|x+1$ ou $p|x-1$.

► On a $x + 1 \in [\![2, p]\!]$ puisque $x \in [\![1, p-1]\!]$. Ce qui démontre que si $p|x+1$ alors $x + 1 = p$, c'est-à-dire $x = p - 1$.

►On a $x - 1 \in [\![0, p-2]\!]$ puisque $x \in [\![1, p-1]\!]$. Ce qui démontre que si $p|x-1$ alors $x - 1 = 0$, c'est-à-dire $x = 1$.

Réciproquement, on a $1 \times 1 \equiv 1\ [p]$ et $(p-1) \times (p-1) = p^2 - 2p + 1 \equiv 1\ [p]$, ce qui démontre que si $x = 1$ ou $x = p - 1$ alors $x = x^{-1}$.

$$\boxed{\forall x \in [\![1, p-1]\!],\ x = x^{-1} \Leftrightarrow x = 1 \text{ ou } x = p - 1}$$

(c) Soit $x \in [\![1, p-1]\!]$, on suppose que $x = -x^{-1}$. Par définition de $-x^{-1}$ cela signifie que $-x^2 \equiv 1\ [p]$. Deux cas se présentent :

► Soit l'équation n'admet aucune solution appartenant à $[\![1, p-1]\!]$.

► Soit l'équation admet une solution $x_0 \in [\![1, p-1]\!]$, c'est-à-dire que $-x_0^2 \equiv 1\ [p]$. Considérons une solution $x \in [\![1, p-1]\!]$ de $-x^2 \equiv 1\ [p]$. On a alors :

$$x^2 \equiv x_0^2\ [p] \Leftrightarrow x^2 - x_0^2 \equiv 0\ [p] \Leftrightarrow (x+x_0)(x-x_0) \equiv 0\ [p] \Leftrightarrow p|(x+x_0)(x-x_0)$$

Comme p est premier, ceci implique que $p|x+x_0$ ou $p|x-x_0$. Or $x+x_0 \in [\![2, 2p-2]\!]$, donc si $p|x+x_0$ alors $x+x_0 = p$ et par suite $x = p - x_0$. D'autre part, $x - x_0 \in [\![-(p-2), p-2]\!]$, donc si $p|x-x_0$ alors $x - x_0 = 0$ et par suite $x = x_0$.

Les deux solutions trouvées dans ce cas : x_0 et $p - x_0 \equiv -x_0\ [p]$ sont bien distinctes car d'après la question (a), il n'est pas possible que $x_0 = -x_0$.

En résumé :

si $x \in [\![1, p-1]\!]$, alors l'équation $x = -x^{-1}$ admet 0 ou 2 solutions

(d) On sait que l'ensemble des classes d'équivalence pour la relation $\mathcal{R}$ forme une partition de l'ensemble $[\![1, p-1]\!]$. Chacune de ces classes d'équivalence possède 4 éléments x, $-x$, x^{-1} et $-x^{-1}$ sauf si certains de ces éléments sont égaux :

► $x = -x$ est impossible d'après la question (a).

► $x = x^{-1} \Leftrightarrow x = 1$ ou $x = p-1$, d'après la question (b). Ce qui donne la classe $\{1, p-1\}$ qui est réduite à deux éléments. Les éléments 1 et $p-1$ forment bien une classe puisque $1 + (p-1) \equiv 0\ [p]$.

► $x = -x^{-1}$ possède 0 ou 2 solutions d'après la question (c). Dans le cas où il y a deux solutions, nous obtenons une classe à deux éléments : $\{x_0, p - x_0\}$, en reprenant les notations de la question (c). C'est bien une classe d'équivalence car $-x_0 = x_0^{-1}$ puisque $x_0 = -x_0^{-1}$.

► Les autres cas d'égalité entre éléments de la classe de x se ramènent à ces quatre cas-là puisque :

$$-x = x^{-1} \Leftrightarrow x = -x^{-1},\ -x = -x^{-1} \Leftrightarrow x = x^{-1} \text{ et } x^{-1} = -x^{-1} \Leftrightarrow x = -x$$

Cette étude démontre bien le résultat annoncé.

4. D'après le résultat de la question 3.(d), l'ensemble $[\![1, p-1]\!]$ est l'union des classes d'équivalence pour la relation $\mathcal{R}$. Comme les classes sont disjointes, on a en gardant les mêmes notations que précédemment :

$$p - 1 = 4 \times \underbrace{k}_{\text{nombre de classes à 4 éléments}} + \underbrace{2}_{\text{la classe } \{1, p-1\}} + \text{ éventuellement la classe } \{x_0, p - x_0\}$$

► Si p est congru à 1 modulo 4, alors l'écriture précédente montre que la classe optionnelle $\{x_0, p - x_0\}$ doit apparaître sinon $p = 4k + 3$. Or x_0 vérifie $x_0^2 \equiv -1\ [p]$ et nous avons vu que cette équation a alors exactement 2 solutions, l'autre étant $p - x_0$. Ce qui démontre le lemme dans le cas où $p \equiv 1\ [4]$.

► Si p est congru à 3 modulo 4, alors la classe $\{x_0, p - x_0\}$ n'apparaît pas sinon $p = 4k + 5 \equiv 1\ [4]$. D'après la question 3.(c), cela signifie que l'équation $x = -x^{-1}$ n'a pas de solution. Cette équation étant équivalente à $x^2 \equiv -1\ [p]$ cela démontre le lemme dans le cas où $p \equiv 3\ [4]$.

Comme le cas $p = 2$ du lemme a été démontré à la question 1., on a achevé la démonstration de ce lemme 1.

C-Nombres premiers somme de deux carrés

1. On a $\text{Card}(\Gamma) = \text{E}(\sqrt{p}) + 1$. On rappelle que Γ^2 est l'ensemble des couples dont les deux coordonnées sont dans Γ. Nous avons $\text{E}(\sqrt{p}) + 1$ choix pour la première coordonnée et $\text{E}(\sqrt{p}) + 1$ choix pour la seconde coordonnée, ce qui nous donne $\left(\text{E}(\sqrt{p}) + 1\right)^2$ choix au total.

$$\boxed{\gamma = \text{Card}(\Gamma^2) = \left(\text{E}(\sqrt{p}) + 1\right)^2}$$

D'autre part, d'après les propriétés usuelles de la partie entière, on a : $\sqrt{p} < \text{E}(\sqrt{p}) + 1$. Ce qui démontre que :

$$\boxed{\gamma > p}$$

2. (a) Soit $s \in \mathbb{Z}$. L'idée de la question est qu'il y a strictement plus de p couples dans Γ^2 mais qu'il y a p classes de congruence modulo p, ce qui explique l'égalité proposée. Pour le démontrer, on considère l'application :

$$\begin{array}{rccc} \varphi & : & \Gamma^2 & \to & [\![0, p-1]\!] \\ & & (x, y) & \mapsto & x - sy \ [p] \end{array}$$

L'application φ n'est pas injective puisque le nombre d'éléments de l'ensemble de départ est strictement plus grand que le nombre d'éléments de l'ensemble d'arrivée, ce qui implique que deux éléments ont la même image. Il existe $(x, y) \in \Gamma^2$ et $(x', y') \in \Gamma^2$ avec $(x, y) \neq (x', y')$ tels que :

$$\boxed{x - sy \equiv x' - sy' \ [p]}$$

(b) On sait que x et x' appartiennent à $[\![0, \text{E}(\sqrt{p})]\!]$, on a :

$$0 \leq x \leq \text{E}(\sqrt{p}) \text{ et } -\text{E}(\sqrt{p}) \leq -x' \leq 0$$

En sommant ces deux inégalités, on obtient :

$$-\text{E}(\sqrt{p}) \leq x - x' \leq \text{E}(\sqrt{p})$$

Ce qui implique que $\widehat{x} = |x - x'| \leq \text{E}(\sqrt{p})$ et par suite $\widehat{x} \in [\![0, \text{E}(\sqrt{p})]\!]$. De même $\widehat{y} \in [\![0, \text{E}(\sqrt{p})]\!]$. Ce qui démontre que $(\widehat{x}, \widehat{y}) \in \Gamma^2$.
Enfin d'après la question précédente, nous avons $x - sy \equiv x' - sy' \ [p]$ ce qui équivaut à $x - x' \equiv s(y - y') \ [p]$. On prend la valeur absolue :

$$|x - x'| \equiv \pm s|y - y'| \ [p] \Leftrightarrow \widehat{x} \equiv \varepsilon s \widehat{y} \ [p] \text{ avec } \varepsilon \in \{-1, 1\}$$

$$\boxed{\exists (\widehat{x}, \widehat{y}) \in \Gamma^2, \ \widehat{x} \equiv \varepsilon s \widehat{y} \ [p] \text{ avec } \varepsilon \in \{-1, 1\}}$$

3. Dans cette partie, on a supposé que p est un nombre premier congru à 1 modulo 4. D'après le lemme 1, il est possible de choisir $s \in [\![1, p-1]\!]$ tel que $s^2 \equiv -1 \ [p]$. Ainsi en élevant la relation de la question précédente au carré, il vient :

$$\widehat{x}^2 \equiv s^2 \widehat{y}^2 \ [p] \Leftrightarrow \widehat{x}^2 + \widehat{y}^2 \equiv 0 \ [p] \Leftrightarrow p | \widehat{x}^2 + \widehat{y}^2$$

Or $\widehat{x} \in \Gamma$, c'est-à-dire que : $0 \leq \widehat{x} \leq \text{E}(\sqrt{p})$ et par suite $0 \leq \widehat{x}^2 \leq \text{E}(\sqrt{p})^2$. D'autre part $\text{E}(\sqrt{p}) < \sqrt{p}$ puisque p est un nombre premier donc il ne peut être égal à un carré. Finalement :

$$0 \leq \widehat{x}^2 < p$$

De même $0 \leq \widehat{y}^2 < p$ et en sommant les deux inégalités précédentes, il vient : $0 \leq \widehat{x}^2 + \widehat{y}^2 < 2p$. Enfin $\widehat{x}^2$ et $\widehat{y}^2$ ne sont pas tous les deux nuls puisque $(x, y) \neq (x', y')$, ce qui nous donne :

$$0 < \widehat{x}^2 + \widehat{y}^2 < 2p$$

Comme $p|\widehat{x}^2 + \widehat{y}^2$, on a nécessairement $p = \widehat{x}^2 + \widehat{y}^2$.

Si p est un nombre premier congru à 1 modulo 4 alors p est la somme de deux carrés

4. C'est un simple bilan des questions précédentes :
   ▶ On a : $2 = 1^2 + 1^2$, donc 2 est la somme de deux carrés d'entiers naturels.
   ▶ Si p est un nombre premier congru à 1 modulo 4 alors p est la somme de deux carrés d'entiers naturels d'après la question précédente.
   ▶ Si p est un nombre premier congru à 3 modulo 4 alors p n'est pas la somme de deux carrés d'entiers naturels d'après la question 2. de la partie A.

Un nombre premier p est somme de deux carrés d'entiers naturels si et seulement si $p = 2$ ou $p \equiv 1$ [4]

D-Entiers somme de deux carrés

1. On vérifie que :

$$mn = (x^2 + y^2)(t^2 + u^2) = x^2t^2 + x^2u^2 + y^2t^2 + y^2u^2 = (xt + yu)^2 + (xu - yt)^2$$

Il est clair que $xt + yu \in \mathbb{N}$ par contre $xu - yt$ est un entier relatif mais quitte à remplacer $xu - yt$ par son opposé on se ramène à la décomposition souhaitée. Finalement :

$$\boxed{mn = (xt + yu)^2 + (|xu - yt|)^2}$$

2. Soit n un entier naturel qui est somme de deux carrés d'entiers naturels, c'est-à-dire qu'il existe $(x, y) \in \mathbb{N}^2$ tels que $n = x^2 + y^2$. On a :

$$nz^2 = (x^2 + y^2)z^2 = (xz)^2 + (yz)^2$$

nz^2 est la somme de deux carrés d'entiers naturels

3. On a vu que 0 et 1 sont sommes de deux carrés. Soit $n \geq 2$, on peut décomposer n en facteurs premiers en distinguant ceux congrus à 1 modulo 4 et ceux congrus à 3 modulo 4 :

$$n = 2^k \times \underbrace{\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right)}_{\text{nombres premiers congrus à 1 modulo 4}} \times \underbrace{\left(\prod_{j=1}^{s} q_j^{\beta_j}\right)}_{\text{nombres premiers congrus à 3 modulo 4}}$$

avec $(k, r, s) \in \mathbb{N}^3$, $(\alpha_i)_{1 \leq i \leq r} \in \mathbb{N}^r$ et $(\beta)_{1 \leq j \leq s} \in \mathbb{N}^s$ sont des entiers pairs d'après l'hypothèse faite dans la question.
On sait que 2 est somme de deux carrés et que pour tout $i \in [\![1, r]\!]$, p_i est somme de deux carrés. Or d'après la question 1., un produit d'entiers qui sont sommes de deux carrés est une somme de deux carrés, par une

récurrence immédiate, on démontre qu'un produit quelconque d'entiers qui sont sommes de deux carrés est une somme de deux carrés. Ainsi $2^k \times \left(\prod_{i=1}^{r} p_i^{\alpha_i}\right)$ est une somme de deux carrés. D'autre part, on a :

$$\left(\prod_{j=1}^{s} q_j^{\beta_j}\right) = \left(\prod_{j=1}^{s} q_j^{\beta_j/2}\right)^2$$

D'après la question précédente, comme n est le produit d'un entier qui est somme de deux carrés et d'un carré alors n est une somme de deux carrés.

Si pour tout nombre premier p congru à 3 modulo 4, $\nu_p(n)$ est pair alors n est somme de deux carrés

4. (a) Comme $p|n$, on a $x^2 + y^2 \equiv 0\ [p]$. Si l'on suppose que $x \not\equiv 0\ [p]$, on sait que x possède un inverse modulo p, d'après la question 4. de la partie A, notons cet inverse u. En multipliant la relation $x^2 + y^2 \equiv 0\ [p]$ par u^2, il vient :

$$u^2x^2 + u^2y^2 \equiv 0\ [p] \Leftrightarrow 1 + u^2y^2 \equiv 0\ [p] \Leftrightarrow (uy)^2 \equiv -1\ [p]$$

Cette dernière relation est absurde, d'après le lemme 1, puisque $p \equiv 3\ [4]$ par hypothèse.

$$x \equiv 0\ [p]$$

(b) Par le même raisonnement qu'à la question précédente, on a également $y \equiv 0\ [p]$. On a donc :

$$p|x \text{ et } p|y \text{ ce qui implique } p^2|x^2 \text{ et } p^2|y^2 \text{ et par suite } p^2|x^2 + y^2$$

$$p^2|n$$

(c) On a $n = x^2 + y^2$ donc $\dfrac{n}{p^2} = \left(\dfrac{x}{p}\right)^2 + \left(\dfrac{y}{p}\right)^2$. Nous avons vu dans la question 4.(a) que p divise x et p divise y, c'est-à-dire que $\dfrac{x}{p}$ et $\dfrac{y}{p}$ sont des entiers naturels.

$\dfrac{n}{p^2}$ est une somme de deux carrés d'entiers naturels

(d) On vient de démontrer que si p est un diviseur premier de n congru à 3 modulo 4 alors p^2 divise n. Il y a deux cas à considérer :

► Si p ne divise pas $\dfrac{n}{p^2}$ alors p apparaît à la puissance 2 dans la décomposition en facteurs premiers de n.

► Si p divise n, on peut appliquer à nouveau le raisonnement précédent à $\dfrac{n}{p^2}$ qui est également une somme de deux carrés d'entiers naturels d'après la question 4.(c). Ainsi $p^2|\dfrac{n}{p^2}$ donc $p^4|n$.

On poursuit le raisonnement précédent ce qui démontre que p apparaît à une puissance paire dans la décomposition en facteurs premiers de n.

Si $p \equiv 3\ [4]$ et $p|n$ alors $\nu_p(n)$ est pair

5. On a $\prod_{i=1}^{k} p_i$ qui est un nombre impair donc il est congru à 1 ou 3 modulo 4. Dans les deux cas $\left(\prod_{i=1}^{k} p_i\right)^2 \equiv 1\ [4]$ et par suite $M_k \equiv 1\ [4]$. L'entier M_k est impair et supérieur à 2 donc il possède un facteur premier impair p. Le nombre premier p n'est pas l'un des p_i où $i \in [\![1, k]\!]$ car sinon $p|M_k$ et $p|\left(\prod_{i=1}^{k} p_i\right)^2$, ce qui implique en faisant la différence que $p|4$. Ceci est absurde car p est impair.
On en déduit que tous les facteurs premiers de M_k sont supérieurs à p_k. D'autre part M_k ne possède pas de facteur premier congru à 3 modulo 4, en effet si tel était le cas d'après la question 4.(a), on aurait ce facteur premier qui diviserait 2 ; ce qui est absurde.
Finalement, pour tout entier naturel k, M_k possède un facteur premier congru à 1 modulo 4 supérieur à p_k. Nous savons qu'il y a une infinité de nombres premiers donc $\lim_{k\to+\infty} p_k = +\infty$. Cette étude démontre qu'il y a des nombres premiers congrus à 1 modulo 4 aussi grands que l'on veut.

Il y a une infinité de nombres premiers congrus à 3 modulo 4

6. Soit x un entier naturel, on examine les différents cas modulo 8 :

x modulo 8	x^2 modulo 8
0	0
1	1
2	4
3	1
4	0
5	1
6	4
7	1

Si x, y et z sont trois entiers naturels, en examinant les différentes possibilités, on voit que l'on ne peut pas avoir $x^2 + y^2 + z^2 \equiv 7\ [8]$.

Un entier congru à 7 modulo 8 ne peut pas être une somme de trois carrés d'entiers naturels

E-Une dernière surprise

```
from math import *

def estcarre(n):
    """renvoie 1 si n est un carré d'entier, 0 sinon"""
    val = 0
    for i in range(int(sqrt(n)) + 2):
        if i ** 2 == n:
            val = 1
    return(val)



def nbdecomp(n):
    """calcul le nombre de décomposition de n"""
    nb = 0
    for i in range(int(sqrt(n)) + 2):
        if n - i ** 2 >= 0:
            nb = nb + estcarre(n - i ** 2)
    return(nb)


def total(N):
    return(1 / ( N + 1 ) * sum(nbdecomp(i) for i in range( N + 1)))


#On lance 4*total(100000) pour trouver :

#3.1546084539154613
```

Dans ce programme, on a cherché les décompositions en tant que somme de deux carrés d'entiers naturels et on a multiplié par 4 pour avoir le nombre total, en négligeant les cas où 0 intervient dans la décomposition.

On peut démontrer que ce nombre moyen de décompositions tend vers π.