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 $\Big(\text{E}(\sqrt{p}) + 1\Big)^2$ choix au total.

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

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 :

$$mn = (xt + yu)^2 + (|xu - yt|)^2$$

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 :

$p|x$ et $p|y$ ce qui implique $p^2|x^2$ et $p^2|y^2$ 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.

Théorème de Lagrange

La question 1 de cet exercice vise à démontrer le théorème de Lagrange. Joseph-Louis Lagrange est un mathématicien italien (comme Cesàro) du XVIIIème siècle, il a en fait démontré ce résultat dans un cas particulier de groupe, puisque la notion générale de groupe n'est apparue que postérieurement. Le point clé de cette preuve est l'utilisation d'une relation d'équivalence puis l'emploi du lien entre classe d'équivalence et partition.

A-Démonstration du théorème

1. Vérifions les trois propriétés qui caractérisent une relation d'équivalence.
   • **Réflexivité :** Soit $x \in G$, on a $x^{-1}x = e \in H$ puisque H est un sous-groupe de G, ceci montre que $x\mathcal{R}x$.
   • **Symétrie :** Soient $(x, y) \in G^2$, supposons que $x\mathcal{R}y$ et démontrons que $y\mathcal{R}x$. Comme $x\mathcal{R}y$, on a $x^{-1}y \in H$ et comme H est un sous-groupe de G, $(x^{-1}y)^{-1} = y^{-1}x$ est également dans H. Ce qui est la définition de $y\mathcal{R}x$.
   • **Transitivité :** Soient $(x, y, z) \in G^3$, on suppose que $x\mathcal{R}y$ et $y\mathcal{R}z$, montrons que $x\mathcal{R}z$. On a, par définition de la relation binaire $\mathcal{R}$, $x^{-1}y \in H$ et $y^{-1}z \in H$. Comme H est un sous-groupe, il est stable par produit et ainsi $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$. Ce qui est la définition de $x\mathcal{R}z$.
   On a démontré que :
   $$\boxed{\mathcal{R} \text{ est une relation d'équivalence}}$$

2. (a) Par définition la classe de a est l'ensemble des éléments de G qui sont en relation avec a. Pour tout $a \in G$, on a :
   $$\boxed{\mathrm{Cl}(a) = \{b \in G,\ a\mathcal{R}b\}}$$

   (b) Il est possible de démontrer l'égalité proposée par double inclusion, ici on propose un raisonnement par équivalence. Soit $a \in G$, on a :
   $$b \in \mathrm{Cl}(a) \Leftrightarrow a\mathcal{R}b \Leftrightarrow a^{-1}b \in H \Leftrightarrow \exists x \in H,\ a^{-1}b = x \Leftrightarrow \exists x \in H,\ b = ax \Leftrightarrow b \in \{ax,\ x \in H\}$$
   Ce qui démontre l'égalité proposée :
   $$\boxed{\forall a \in G,\ \mathrm{Cl}(a) = \{ax,\ x \in H\}}$$

3. (a) Il est clair que pour tout $a \in G$, l'application γ_a est bien définie puisque si $x \in H$, on a évidemment $ax \in \{ax,\ x \in H\}$.
   La surjectivité est aussi claire. En effet prenons $y \in \{ax,\ x \in H\}$, il existe $x \in H$ tel que $y = ax = \gamma_a(x)$, ce qui montre que y a un antécédent par γ_a.
   Enfin pour l'injectivité, prenons $(x, x') \in H^2$ tels que
   $$\gamma_a(x) = \gamma_a(x') \Leftrightarrow ax = ax' \Leftrightarrow x = x' \text{ en multipliant à droite par } a^{-1}$$
   On a démontré que pour tout $a \in G$:
   $$\boxed{\gamma_a \text{ est bijective}}$$

   (b) Deux ensembles finis qui sont en bijection ont le même cardinal, en utilisant la question 2.(b), on a ainsi pour tout $a \in G$:
   $$\boxed{\mathrm{Card}(\mathrm{Cl}(a)) = \mathrm{Card}(\{ax,\ x \in H\}) = \mathrm{Card}(H)}$$

4. Il faut se souvenir que les classes d'équivalence forment une partition de G. Comme l'ensemble G est fini, il y a un nombre fini de classes d'équivalence pour la relation $\mathcal{R}$, supposons qu'il y ait k classes d'équivalence où $k \in \mathbb{N}^*$. D'après l'étude menée à la question précédente, toutes ces classes d'équivalence ont le même nombre d'éléments le cardinal de H. Comme deux classes d'équivalence distinctes sont disjointes, on a alors $k \times \text{Card}(H) = \text{Card}(G)$.
   On a bien démontré le théorème de Lagrange puisque :

$$\boxed{\text{Card}(H) | \text{Card}(G)}$$

5. Notons $\text{Card}(G) = p$ où p est un nombre premier. Soit H un sous-groupe de G, d'après l'étude précédente le cardinal de H divise p. Cela implique que $\text{Card}(H) = 1$ ou $\text{Card}(H) = p$, distinguons les deux cas :
   - si $\text{Card}(H) = 1$ étant donné que H contient l'élément neutre du groupe, c'est que $H = \{e\}$.
   - si $\text{Card}(H) = p$, comme on a $H \subset G$ et $\text{Card}(G) = p$ cela implique que $H = G$.

$$\boxed{\text{Si Card}(G) \text{ est un nombre premier alors les seuls sous-groupes de } G \text{ sont } G \text{ et } \{e\}}$$

B-Une application du théorème

1. (a) Supposons que φ_a soit injective, étant donné que G est fini, on sait d'après le cours que $\mathbb{N}$ est fini et que $\text{Card}(\mathbb{N}) \leq \text{Card}(G)$. Ceci est clairement absurde, donc :

$$\boxed{\varphi_a \text{ n'est pas injective}}$$

   (b) Par définition de la non-injectivité, il existe $(n_1, n_2) \in \mathbb{N}^2$ avec $n_1 \neq n_2$ tels que $\varphi_a(n_1) = \varphi_a(n_2)$. Sans perte de généralité supposons que $n_1 > n_2$, on a :

$$\varphi_a(n_1) = \varphi_a(n_2) \Leftrightarrow a^{n_1} = a^{n_2} \Leftrightarrow a^{n_1}a^{-n_2} = a^{n_2}a^{-n_2} \Leftrightarrow a^{n_1-n_2} = e$$

   On pose $k = n_1 - n_2 \in \mathbb{N}^*$, ce qui montre que :

$$\boxed{\forall a \in G,\ \exists k \in \mathbb{N}^*,\ a^k = e}$$

   (c) Soit $a \in G$, l'ensemble $\{k \in \mathbb{N}^*,\ a^k = e\}$ est inclus dans $\mathbb{N}$ et il est non vide d'après la question précédente. Toute partie non vide de $\mathbb{N}$ admet un minimum donc :

$$\boxed{\text{Ord}(a) \text{ existe}}$$

2. (a) Par définition, on a bien pour tout $a \in G$, $H_a \subset G$. Vérifions les trois propriétés qui caractérisent un sous-groupe.
   - On a $a^0 = e \in H_a$.
   - Soient $(x, y) \in H_a^2$, montrons que $xy \in H_a$. On a :

$$x \in H_a \Leftrightarrow \exists r \in [\![0, \text{Ord}(a) - 1]\!],\ x = a^r$$

$$y \in H_a \Leftrightarrow \exists s \in [\![0, \text{Ord}(a) - 1]\!],\ x = a^s$$

   On a ainsi $xy = a^{r+s}$ avec $r + s \in [\![0, 2\text{Ord}(a) - 2]\!]$, deux cas sont à considérer :
   - Si $r + s \in [\![0, \text{Ord}(a) - 1]\!]$ alors, par définition de H_a, on a : $xy = a^{r+s} \in H_a$.

• Si $r+s \in [\![\text{Ord}(a), 2\text{Ord}(a)-2]\!]$ alors $r+s-\text{Ord}(a) \in [\![0, \text{Ord}(a)-2]\!]$, ceci implique que $a^{r+s-\text{Ord}(a)} \in H_a$.

En se souvenant que par définition de $\text{Ord}(a)$, on a $a^{\text{Ord}(a)} = e$, il vient :

$$xy = a^{r+s} = a^{r+s}e^{-1} = a^{r+s}\left[a^{\text{Ord}(a)}\right]-1 = a^{r+s}a^{-\text{Ord}(a)} = a^{r+s-\text{Ord}(a)} \in H_a$$

Ce qui démontre que H_a est stable par produit.

• Prenons $x \in H_a$ et démontrons que $x^{-1} \in H_a$. Si $x = e = a^0$ le résultat est clair, prenons $x \neq e$, on a :

$$x \in H_a \Leftrightarrow \exists r \in [\![1, \text{Ord}(a)-1]\!],\ x = a^r$$

L'élément $y = a^{\text{Ord}(a)-r}$ appartient à H_a puisque $\text{Ord}(a)-r \in [\![1, \text{Ord}(a)-1]\!]$, montrons que c'est l'inverse de x :

$$xy = a^r a^{\text{Ord}(a)-r} = a^{r+\text{Ord}(a)-r} = a^{\text{Ord}(a)} = e$$

et par un calcul tout à fait similaire, on a : $yx = e$. Ceci montre que $x^{-1} = y = a^{\text{Ord}(a)-r}$.

$$\boxed{H_a \text{ est un sous-groupe de } G}$$

(b) Montrons que le cardinal de H_a est égal à $\text{Ord}(a)$, il s'agit pour cela de montrer que pour $k \in [\![0, \text{Ord}(a)-1]\!]$, les éléments a^k sont distincts. En effet supposons que $a^{k_1} = a^{k_2}$ avec $(k_1, k_2) \in [\![0, \text{Ord}(a)-1]\!]^2$ et $k_1 > k_2$, on a $k_1 - k_2 \in [\![1, \text{Ord}(a)-1]\!]$ et

$$a^{k_1-k_2} = a^{k_1}[a^{k_2}]^{-1} = a^{k_1}[a^{k_1}]^{-1} = a^{k_1-k_1} = e$$

Ceci contredit la minimalité de $\text{Ord}(a)$.

En résumé H_a est un sous-groupe de G, il possède $\text{Ord}(a)$ éléments, d'après le théorème de Lagrange, on en déduit que

$$\boxed{\text{Ord}(a) \text{ divise } n}$$

3. D'après la question précédente, il existe $r \in \mathbb{N}^*$ tel que $\text{Ord}(a) \times r = n$. On a : $a^{\text{Ord}(a)} = e$, d'où

$$e = e^r = \left[a^{\text{Ord}(a)}\right]^r = a^{\text{Ord}(a)\times r} = a^n$$

$$\boxed{\forall a \in G,\ a^{\text{Card}(G)} = e}$$

Ce résultat généralise un exercice fait en cours qui démontrait cette formule dans le cas où le groupe est commutatif.

4. Soit G un groupe de cardinal p où p est un nombre premier. Comme $p \geq 2$, il existe un élément dans G distinct de l'élément neutre, notons-le a. D'après la question 2.(b), $\text{Ord}(a)$ est un diviseur de p, donc $\text{Ord}(a) = 1$ ou $\text{Ord}(a) = p$. Le cas $\text{Ord}(a) = 1$ est à exclure puisque $a \neq e$, donc $\text{Ord}(a) = p$.

En utilisant la question 2.(a), on a H_a qui est un sous-groupe de G de même cardinal que G, c'est donc que $H_a = G$, c'est-à-dire que tous les éléments de G sont des puissances de a. On a alors :

$$\forall (x, y) \in G^2,\ \exists (r, s) \in [\![0, p-1]\!],\ x = a^r \text{ et } y = a^s$$

Ceci donne $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$.

$$\boxed{\text{Un groupe de cardinal premier est commutatif}}$$

On peut montrer, en développant les outils étudiés ici, qu'un groupe de cardinal p^2 où p est un nombre premier est également nécessairement commutatif.