Problème 1

① h est continue sur $[a,b]$ et dérivable sur $]a,b[$ comme combinaison de f et g qui le sont.

• $h(b) = 0$ et $h(a) = (f(b)-f(a))(g(a)-g(b)) - (f(a)-f(b))(g(b)-g(a))$

Donc $h(b) = h(a) = 0$

D'après le théorème de Rolle, $\exists c \in]a,b[$, $h'(c) = 0$

② Or $\forall t \in]a,b[$, $h'(t) = (f(b)-f(a))\,g'(t) - (g(b)-g(a))\,f'(t)$

Donc $\boxed{\exists\, c \in]a,b[,\ (f(b)-f(a))\,g'(c) = (g(b)-g(a))\,f'(c).}$

③ $\lim\limits_{a^+} f = \lim\limits_{a^+} g = 0$. Donc on peut prolonger f et g par continuité sur $[a,b[$ en posant $\boxed{f(a)=0}$ et $\boxed{g(a)=0}$

④ Soit $h \in]0, b-a[$. Alors $[a,a+h] \subset [a,b]$.

f et g sont donc continues sur $[a,a+h]$, dérivables sur $]a,a+h[$

D'après la 1re partie, il existe $c_h \in]a,a+h[$ tel que

$$\boxed{(f(a+h)-f(a))\,g'(c_h) = (g(a+h)-g(a))\,f'(c_h).}$$

⑤ On a posé $f(a) = g(a) = 0$. Donc $f(a+h)\,g'(c_h) = g(a+h)\,f'(c_h)$.

De plus $g(a+h) \neq 0$ et $g'(c_h) \neq 0$ car g et g' ne s'annulent pas sur $]a,b[$. Donc $\boxed{\dfrac{f(a+h)}{g(a+h)} = \dfrac{f'(c_h)}{g'(c_h)}}$

⑥ On a $a < c_h < a+h$. Donc par encadrement, $\boxed{c_h \xrightarrow[h\to 0]{} a}$

⑦ Supposons $\dfrac{f'}{g'} \xrightarrow[a^+]{} \ell \in \overline{\mathbb{R}}$.

Soit V un voisinage de ℓ

Soit $0 < \eta < b-a$ tel que $\forall x \in]a,a+\eta[$, $\dfrac{f'(x)}{g'(x)} \in V$

Soit $x \in]a,a+\eta[$ et $h = x-a$, si bien que $x = a+h$

Alors $\dfrac{f(x)}{g(x)} = \dfrac{f(a+h)}{g(a+h)} = \dfrac{f'(c_h)}{g'(c_h)}$ avec $c_h \in]a,a+h[\subset]a,a+\eta[$

Donc $\dfrac{f(x)}{g(x)} \in V$. Ceci montre $\boxed{\dfrac{f}{g} \xrightarrow[a^+]{} \ell}$

Problème 2

Pierre de Fermat était un magistrat français du XVII^e siècle, il était 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 Prémiminaires

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 sommes 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. 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) Démontrons le résultat par récurrence sur le nombre de facteurs dans le produit en question. Pour $r \in \mathbb{N}^*$, on considère l'assertion $\mathcal{H}_r$:

   si $(t_i)_{1\leq i\leq r}$ est une famille d'entiers congrus à 1 modulo 4 alors $\displaystyle\prod_{i=1}^{r} t_i$ est congru à 1 modulo 4.

   Init. Si $r=1$, le résultat est évident.

   Hér. Soit $r \in \mathbb{N}^*$. On suppose que $\mathcal{H}_r$ est vraie. 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, on obtient

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

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

$\boxed{\text{Un produit d'entiers naturels congrus à 1 modulo 4 est congru à 1 modulo 4}}$.

(b) On pose $M = \left(4\prod_{i=1}^{n} p_i\right) - 1$.

i. 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 strictement supérieur à chacun des p_i où $i \in [\![1, n]\!]$. Donc $\boxed{M \text{ n'est pas premier}}$.

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 3a, M est également congru à 1 modulo 4, ce qui n'est pas le cas.

$\boxed{M \text{ possède un diviseur premier congru à 3 modulo 4}}$.

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

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

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

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 $p \mid a(u-u')$ mais p est premier avec a, ce qui implique via le théorème de Gauss que $p \mid u-u'$. 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.

$\boxed{\text{Si } p \text{ est premier, pour tout } a \in [\![1, p-1]\!],\ a \text{ possède un unique inverse modulo } p}$.

On notera dans toute la suite cet inverse a^{-1}.

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.

On notera dans toute la suite cet opposé $-a$.

B Une équation modulaire

Le but de cette partie est de démontrer le lemme suivant.

Lemme 1

L'équation $s^2 \equiv -1\ [p]$ d'inconnue s possède

- *deux solutions appartenant à $[\![1, p-1]\!]$ si 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 $p = 2$.*

6. 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 $p = 2$.

7. (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. Soit $(x, y) \in [\![1, p-1]\!]^2$, 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 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 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. Soit $(x, y, z) \in [\![1, p-1]\!]^3$, 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 $x\mathcal{R}z$.

Donc $\boxed{\mathcal{R} \text{ est une relation d'équivalence}}$.

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

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

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

(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,

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

8. (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 $p \mid 2x$, or p est impair donc il est premier avec 2, en vertu du théorème de Gauss ceci entraîne que $p \mid x$. Ceci est absurde puisque $x \in [\![1, p-1]\!]$. Donc $\boxed{\forall x \in [\![1, p-1]\!],\ x \neq -x}$.

   (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 $p \mid x^2 - 1 = (x+1)(x-1)$, comme p est premier ceci entraîne que $p \mid x+1$ ou $p \mid x-1$.

   - On a $x + 1 \in [\![2, p]\!]$ puisque $x \in [\![1, p-1]\!]$, ce qui démontre que si $p \mid x+1$ 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 $p \mid x-1$ 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

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

     Comme p est premier, ceci implique que $p \mid x + x_0$ ou $p \mid x - x_0$. Or $x + x_0 \in [\![2, 2p-2]\!]$, donc si $p \mid x + x_0$ 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 $p \mid x - x_0$ 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 8a, il n'est pas possible que $x_0 = -x_0$.

   Finalement,

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

   (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 8a.
   - $x = x^{-1} \Leftrightarrow x = 1$ ou $x = p - 1$, d'après la question 8b. 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 8c. 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 8c. 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.

9. D'après le résultat de la question 8d, 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 :

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

- 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 8c, 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 6, on a achevé la démonstration de ce lemme.

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 cette partie $\Gamma = [\![0, \lfloor\sqrt{p}\rfloor]\!]$.

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

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

D'autre part, d'après les propriétés usuelles de la partie entière, on a : $\sqrt{p} < \lfloor\sqrt{p}\rfloor + 1$. 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 $[\![0, \lfloor\sqrt{p}\rfloor]\!]$, on a

$$0 \leq x \leq \lfloor\sqrt{p}\rfloor \text{ et } -\lfloor\sqrt{p}\rfloor \leq -x' \leq 0.$$

En sommant ces deux inégalités, on obtient

$$-\lfloor\sqrt{p}\rfloor \leq x - x' \leq \lfloor\sqrt{p}\rfloor,$$

ce qui implique que $\widehat{x} = |x - x'| \leq \lfloor\sqrt{p}\rfloor$ et par conséquent $\widehat{x} \in [\![0, \lfloor\sqrt{p}\rfloor]\!]$. De même $\widehat{y} \in [\![0, \lfloor\sqrt{p}\rfloor]\!]$. 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,

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

Or $\widehat{x} \in \Gamma$, c'est-à-dire que : $0 \leq \widehat{x} \leq \lfloor\sqrt{p}\rfloor$ et par suite $0 \leq \widehat{x}^2 \leq \lfloor\sqrt{p}\rfloor^2$. D'autre part $\lfloor\sqrt{p}\rfloor < \sqrt{p}$ 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, on a $0 \leq \widehat{x}^2 + \widehat{y}^2 < 2p$. 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 $p \mid \widehat{x}^2 + \widehat{y}^2$, 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 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

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

Theorème 1

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. Soit on vérifie en développant que
$$mn = (x^2+y^2)(t^2+u^2) = x^2t^2 + x^2u^2 + y^2t^2 + y^2u^2 = (xt+yu)^2 + (|xu-yt|)^2,$$
soit on pose astucieusement $z = x+iy$ et $w = t+iu$ dans $\mathbb{C}$.
Alors $m = x^2+y^2 = |z|$ et $n = t^2+u^2 = |u|$. Et $mn = |zw|$ et on retrouve
$$\boxed{mn = (xt+yu)^2 + (|xu-yt|)^2},$$
avec $xt+yu \in \mathbb{N}$ et $|xu-yt| \in \mathbb{N}$.

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 $n = x^2+y^2$. Alors
$$nz^2 = (x^2+y^2)z^2 = (xz)^2 + (yz)^2$$
$$\boxed{nz^2 \text{ est la somme de deux carrés d'entiers naturels}}.$$

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.
$$n = 2^k \times \Big(\prod_{\substack{1 \leqslant i \leqslant r \\ p_i \equiv 1\,[4]}} p_i^{\alpha_i} \Big) \times \Big(\prod_{\substack{1 \leqslant i \leqslant r \\ p_i \equiv 1\,[4]}} q_j^{\beta_j} \Big)$$
où $(k,r,s) \in \mathbb{N}^3$, $(\alpha_i)_{1 \leq i \leq r} \in \mathbb{N}^r$ 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 ; on démontre par récurrence qu'un produit quelconque d'entiers qui sont sommes de deux carrés est une somme de deux carrés. Ainsi $2^k \times \Big(\prod_{i=1}^{r} p_i^{\alpha_i} \Big)$ est une somme de deux carrés. D'autre part, on a
$$\Big(\prod_{j=1}^{s} q_j^{\beta_j} \Big) = \Big(\prod_{j=1}^{s} q_j^{\beta_j/2} \Big)^2.$$
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. Ainsi,

$$\boxed{\text{si pour tout nombre premier } p \text{ congru à 3 modulo 4, } \nu_p(n) \text{ est pair alors } n \text{ est somme de deux carrés}}.$$

4. (a) Comme $p \mid n$, 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 ; notons u cet inverse. En multipliant la relation $x^2+y^2 \equiv 0\ [p]$ par u^2, on obtient
$$u^2x^2 + u^2y^2 \equiv 0\ [p] \Leftrightarrow 1 + u^2y^2 \equiv 0\ [p] \Leftrightarrow (uy)^2 \equiv -1\ [p].$$
Cette dernière relation est absurde, d'après le lemme 1, puisque $p \equiv 3\ [4]$ par hypothèse. Donc
$$\boxed{x \equiv 0\ [p]}.$$

(b) On montre de la même manière que $y \equiv 0\ [p]$. Donc $p \mid x$ et $p \mid y$, ce qui implique que $p^2 \mid x^2$ et $p^2 \mid y^2$ et donc $p^2 \mid x^2 + y^2$. Finalement, $\boxed{p^2 \mid n}$.

(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 4a que p divise x et p divise y, c'est-à-dire que $\dfrac{x}{p}$ et $\dfrac{y}{p}$ sont des entiers naturels. Donc

$$\boxed{\frac{n}{p^2} \text{ est une somme de deux carrés d'entiers naturels}}.$$

(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 $\dfrac{n}{p^2}$, 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 4c. Ainsi $p^2 \mid \dfrac{n}{p^2}$ donc $p^4 \mid n$.

On répète le raisonnement précédent (c'est un processus fini car $p^{2k} > n$ àpcr), ce qui démontre que p apparaît à une puissance paire dans la décomposition en facteurs premiers de n.

$$\boxed{\text{Si } p \equiv 3\ [4] \text{ et } p \mid n \text{ alors } \nu_p(n) \text{ est pair}}.$$

5. On a $\displaystyle\prod_{i=1}^{k} p_i$ qui est un nombre impair donc il est congru à 1 ou 3 modulo 4. Dans les deux cas $\left(\displaystyle\prod_{i=1}^{k} p_i\right)^2 \equiv 1\ [4]$ 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 $p \mid M_k$ et $p \mid \left(\displaystyle\prod_{i=1}^{k} p_i\right)^2$, ce qui implique, en faisant la différence, que $p \mid 4$. 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 4a, ce facteur premier 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 $\lim\limits_{k \to +\infty} p_k = +\infty$. Ceci montre qu'il y a des nombres premiers congrus à 1 modulo 4 aussi grands que l'on veut.

$$\boxed{\text{Il y a une infinité de nombres premiers congrus à 1 modulo 4}}.$$

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

Remarque. *Un théorème dû à Lagrange assure que tout entier naturel est somme de 4 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
```

Remarque. Dans ce programme, on a cherché les décompositions en tant que sommes 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.