DEVOIR SURVEILLÉ 4

(durée : 4 h 00)

Rédigez vos réponses dans un français correct. Terminez chaque résolution d'exercice par une conclusion encadrée ou soulignée. Laissez une marge au correcteur.

Les exercices sont indépendants et peuvent être traités dans n'importe quel ordre. Dans un exercice avec plusieurs questions, on pourra, si besoin est, admettre le résultat d'une question pour répondre aux suivantes.

La calculatrice n'est pas autorisée.

EXERCICE 1

Theoremata circa residua ex divisione potestatum relicta
(ou Théorème d'Euler)

Soit $n \in \mathbb{N}^*$. On rappelle que l'indicatrice d'Euler de n, notée $\varphi(n)$, est le cardinal du groupe $\mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big)$ des éléments inversibles de l'anneau $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$.

Soit $a \in \mathbb{Z}$ tel que $a \wedge n = 1$. En vous inspirant de la démonstration du petit théorème de Fermat, démontrer que

$$a^{\varphi(n)} \equiv 1 \ [n].$$

EXERCICE 2

Pots de peinture

Soient $n, p \in \mathbb{N} \setminus \{0; 1\}$. Une cour est entièrement bordée de n murs. On désire les peindre de sorte que deux murs consécutifs quelconques soient toujours de couleurs différentes. On dispose pour cela de p couleurs.

On notera bien que, si l'on numérote les murs de 1 à n, alors le mur 1 est voisin du mur 2 mais aussi du mur n.

Pour $n \geqslant 2$, on note u_n le nombre de façons de peindre ces murs.

1. Calculer u_2 et u_3.
2. Démontrer que, pour tout $n \geqslant 2$,
$$u_{n+2} = (p-2)u_{n+1} + (p-1)u_n.$$
3. Justifier qu'il est cohérent de poser $u_1 = 0$ et $u_0 = p$.
4. Pour tout $n \geqslant 0$, déterminer une expression explicite de u_n en fonction de n et p.

EXERCICE 3

Topologie de Fürstenberg

L'objet de cet exercice est d'introduire la topologie de Fürstenberg de $\mathbb{Z}$ et de voir comment elle permet de redémontrer que l'ensemble $\mathbb{P}$ des nombres premiers est infini.

Pour tout $a \in \mathbb{Z}$ et tout $r \in \mathbb{N}^*$, on note $A_{a,r}$ le sous-ensemble de $\mathbb{Z}$ constitué des termes de la suite arithmétique de raison r dont a est l'un des termes, c'est-à-dire

$$A_{a,r} = \{a + kr : k \in \mathbb{Z}\}.$$

Soit U une partie de $\mathbb{Z}$. On dit que U est un ouvert de $\mathbb{Z}$ lorsque pour tout $x \in U$, il existe $r \in \mathbb{N}^*$ tel que $A_{x,r} \subset U$. *On notera bien que cette définition d'ouvert n'a rien à voir avec la définition classique d'un ouvert dans* $\mathbb{R}$.

Soit F une partie de $\mathbb{Z}$. On dit que F est un fermé de $\mathbb{Z}$ lorsque $\mathbb{Z} \setminus F$ est un ouvert de $\mathbb{Z}$.

1. a) Démontrer que :
   1) $\varnothing$ et $\mathbb{Z}$ sont des ouverts de $\mathbb{Z}$;
   2) toute réunion d'ouverts de $\mathbb{Z}$ est un ouvert de $\mathbb{Z}$;
   3) toute intersection finie d'ouverts de $\mathbb{Z}$ est un ouvert de $\mathbb{Z}$.

   b) Quelles propriétés analogues sur les fermés de $\mathbb{Z}$ peut-on énoncer ? On expliquera brièvement comment elles se démontrent.
2. Soient $a \in \mathbb{Z}$ et $r \in \mathbb{N}^*$. Démontrer que $A_{a,r}$ est à la fois un ouvert et un fermé de $\mathbb{Z}$.
3. Déterminer $\bigcup_{p \in \mathbb{P}} A_{0,p}$ et en déduire que $\mathbb{P}$ est infini.

EXERCICE 4

Ensemble dérivé

Soit A une partie de $\mathbb{R}$. On dit que $x \in \mathbb{R}$ est un point d'accumulation de A lorsque, pour tout $\varepsilon > 0$, on a $A \cap (]x - \varepsilon; x[\cup]x; x + \varepsilon[) \neq \varnothing$. L'ensemble des points d'accumulation de A est noté A' et s'appelle l'ensemble dérivé de A.

1. Reformuler la définition d'un point d'accumulation à l'aide de la notion d'adhérence.
2. a) Donner un exemple d'ensemble infini D tel que $D' = \varnothing$.
   b) On pose $H = \{1/n : n \in \mathbb{N}^*\}$. Démontrer que $0 \in H'$.
3. Démontrer que $x \in \mathbb{R}$ est un point d'accumulation de A si, et seulement si, pour tout $\varepsilon > 0$, l'ensemble $A \cap (]x - \varepsilon; x[\cup]x; x + \varepsilon[)$ est infini.
4. Démontrer que A' est un fermé de $\mathbb{R}$.
5. a) Démontrer que $\mathrm{Adh}(A) = A \cup A'$.
   b) Démontrer que A est un fermé de $\mathbb{R}$ si, et seulement si, $A' \subset A$.

EXERCICE 5

Le théorème des deux carrés de Fermat

L'objet de ce problème est de démontrer le théorème des deux carrés de Fermat : un entier $n \in \mathbb{N}^*$ est la somme de deux carrés si, et seulement si, pour tout nombre premier p congru à 3 modulo 4 la valuation p-adique de n est paire.

A. Le lemme d'Euler par la méthode d'Axel Thue

L'objet de cette partie est de démontrer, à l'aide d'une méthode due à Axel Thue, le lemme d'Euler : si p est un nombre premier qui divise une somme de deux carrés premiers entre eux, alors p est une somme de deux carrés.

Soit p un nombre premier. On suppose qu'il existe $a, b \in \mathbb{N}^*$ tels que p divise $a^2 + b^2$ et $a \wedge b = 1$.

1. Démontrer qu'il existe deux couples distincts (x_1, y_1) et (x_2, y_2) dans $\left([0; \sqrt{p}[\cap \mathbb{N} \right)^2$ tels que $ax_1 + by_1 \equiv ax_2 + by_2$ $[p]$.

   On pose $u = x_1 - x_2$ et $v = y_1 - y_2$.

2. Démontrer que p divise $a^2u^2 - b^2v^2$, puis que p divise $u^2 + v^2$ et enfin que $p = u^2 + v^2$.

B. Nombre premier somme de deux carrés

L'objet de cette partie est de démontrer qu'un nombre premier p est une somme de deux carrés si, et seulement si, $p = 2$ ou p est congru à 1 modulo 4.

Soit p un nombre premier impair.

1. Justifier que 2 est une somme de deux carrés.
2. On suppose que p est une somme de deux carrés, c'est-à-dire qu'il existe $a, b \in \mathbb{N}^*$ tels que $p = a^2 + b^2$. Démontrer que $p \equiv 1$ [4].
3. Réciproquement, on suppose que $p \equiv 1$ [4].
   a) On pose $m = (p-1)/2$.

      Justifier que $\mathbb{F}_p^* = [\![-m; m]\!] \setminus \{0\}$.

      En déduire que $(m!)^2 \equiv -1$ $[p]$.

   b) Justifier que p est une somme de deux carrés.

C. Le théorème des deux carrés de Fermat

Soit $n \in \mathbb{N}^*$.

1. a) Démontrer que le produit de deux entiers qui sont des sommes de deux carrés est une somme de deux carrés. *Indication : On pourra utiliser les nombres complexes.*

   b) On suppose que, pour tout nombre premier p congru à 3 modulo 4, $v_p(n)$ est pair. Démontrer que n est une somme de deux carrés.

2. Réciproquement, on suppose que n est une somme de deux carrés, c'est-à-dire qu'il existe $a, b \in \mathbb{N}^*$ tels que $n = a^2 + b^2$.

   Démontrer que, pour tout nombre premier p congru à 3 modulo 4 la valuation p-adique de n est paire.

EXERCICE 6

Nombres premiers dans les progressions arithmétiques de raison 6

Dans cet exercice, on admet le théorème de Lagrange : si G est groupe fini et H un sous-groupe de G alors $\operatorname{card} H$ divise $\operatorname{card} G$. Nous démontrerons ce théorème plus tard dans l'année.

1. Soit $p \in \mathbb{P} \setminus \{2;3\}$. Démontrer que p est congru à 1 ou 5 modulo 6.
2. Démontrer qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.
   Indication : $N = 6p_1 \dots p_n - 1$
3. a) Soit $p \in \mathbb{P} \setminus \{2;3\}$. On suppose que -3 est un carré dans $\mathbb{F}_p$, c'est-à-dire qu'il existe $a \in \mathbb{F}_p$ tel que $a^2 = -3$ dans $\mathbb{F}_p$. Toujours dans $\mathbb{F}_p$, on pose
   $$j = 2^{-1}(a-1).$$
   α] Justifier l'existence de j.
   β] Calculer j^2 et j^3 dans $\mathbb{F}_p$.
   γ] Démontrer que $H = \{1, j, j^2\}$ est un sous-groupe de $(\mathbb{F}_p^*, \times)$ de cardinal 3.
   δ] En déduire que $p \equiv 1$ [6].

   b) Démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 6.

Correction

CORRECTION DU DS 4

(durée : 4 h 00)

EXERCICE 1

Soit $n \in \mathbb{N}^*$. On rappelle que l'indicatrice d'Euler de n, notée $\varphi(n)$, est le cardinal du groupe $\mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big)$ des éléments inversibles de l'anneau $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$. Soit $a \in \mathbb{Z}$ tel que $a \wedge n = 1$. En vous inspirant de la démonstration du petit théorème de Fermat, démontrer que $a^{\varphi(n)} \equiv 1\ [n]$.

Comme $a \wedge n = 1$, on sait que $a \in \mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big)$.

Considérons l'application

$$\tau_a \left\{ \begin{array}{ccc} \mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big) & \longrightarrow & \mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big) \\ x & \longmapsto & ax \end{array} \right.$$

qui est bien définie puisque $\mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big)$ est un groupe multiplicatif.

L'application τ_a est une bijection puisque sa réciproque est clairement $\tau_{a^{-1}}$. C'est donc une permutation de $\mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big)$. Cela signifie que, si l'on note

$$\mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big) = \{x_1, x_2, \ldots, x_{\varphi(n)}\},$$

on peut encore s'écrire

$$\mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big) = \{\tau_a(x_1), \tau_a(x_2), \ldots, \tau_a(x_{\varphi(n)})\} = \{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}.$$

Du coup, dans $\mathbb{Z}/n\mathbb{Z}$, le produit des éléments de $\mathrm{U}\big(\mathbb{Z}/n\mathbb{Z}\big)$ vaut à la fois $x_1 \times x_2 \times \cdots \times x_{\varphi(n)}$ et $(ax_1) \times (ax_2) \times \cdots \times (ax_{\varphi(n)})$, ce qui donne

$$x_1 \times x_2 \times \cdots \times x_{\varphi(n)} = a^{\varphi(n)} \times x_1 \times x_2 \times \cdots \times x_{\varphi(n)}.$$

Comme $x_1 \times x_2 \times \cdots \times x_{\varphi(n)}$ est inversible (en tant que produit d'inversibles), on obtient dans $\mathbb{Z}/n\mathbb{Z}$:

$$1 = a^{\varphi(n)}.$$

Donc

$$\boxed{a^{\varphi(n)} \equiv 1\ [n].}$$

EXERCICE 2

Soient $n, p \in \mathbb{N} \setminus \{0;1\}$. Une cour est entièrement bordée de n murs. On désire les peindre de sorte que deux murs consécutifs quelconques soient toujours de couleurs différentes. On dispose pour cela de p couleurs. On notera bien que, si l'on numérote les murs de 1 à n, alors le mur 1 est voisin du mur 2 mais aussi du mur n. Pour $n \geqslant 2$, on note u_n le nombre de façons de peindre ces murs.

1. *Calculer u_2 et u_3.*

   Si la cour est bordée de 2 murs (il ne doit pas y avoir beaucoup de place !), on choisit une couleur pour le premier mur : p choix, puis une seconde couleur, différente de la précédente, pour le second mur : $p-1$ choix. Donc

   $$\boxed{u_2 = p(p-1).}$$

   Si la cour est bordée de 3 murs (c'est déjà plus confortable), on choisit une couleur pour le premier mur : p choix, puis une seconde couleur, différente de la précédente, pour le deuxième mur : $p-1$ choix, et enfin une troisième couleur pour le troisième mur, différente de celles des deux autres murs (qui sont tous les deux voisins du troisième mur) : $p-2$ choix. Donc

   $$\boxed{u_3 = p(p-1)(p-2).}$$

2. *Démonter que, pour tout $n \geqslant 2$, on a $u_{n+2} = (p-2)u_{n+1} + (p-1)u_n$.*

   Soit $n \in \mathbb{N} \setminus \{0;1\}$.

   Notons A_{n+2} l'ensemble des façons de peindre les $n+2$ murs d'une cour (avec p couleurs) de sorte qu'il n'y ait jamais deux murs consécutifs de la même couleur.

   Notons B_{n+2} le sous-ensemble de A_{n+2} constitué des façons de peindre les $n+2$ murs d'une cour (avec p couleurs) de sorte qu'il n'y ait jamais deux murs consécutifs de la même couleur et telles que le premier et le $(n+1)$-ème mur soient de la même couleur.

   Enfin, notons C_{n+2} le sous-ensemble de A_{n+2} constitué des façons de peindre les $n+2$ murs d'une cour (avec p couleurs) de sorte qu'il n'y ait jamais deux murs consécutifs de la même couleur et telles que le premier et le $(n+1)$-ème mur soient de couleurs différentes.

   On a bien sûr

   $$A_{n+2} = B_{n+2} \sqcup C_{n+2}$$

   où $\sqcup$ désigne le symbole d'union disjointe, donc

   $$\operatorname{card} A_{n+2} = \operatorname{card} B_{n+2} + \operatorname{card} C_{n+2}.$$

   D'après la définition de u_{n+2}, on a

   $$\operatorname{card} A_{n+2} = u_{n+2}.$$

   Dénombrons B_{n+2}. Pour cela, on commence par peindre les n premiers murs de sorte qu'il n'y ait jamais deux murs consécutifs de la même couleur et que le premier et le n-ème mur soient de couleurs différentes : cela laisse u_n choix puisque cela revient à dénombrer A_n. Ensuite, on peint le $n+1$-ème mur de la couleur du premier : 1 choix. Enfin, on peint le $n+2$-ème mur d'une couleur différente de la couleur commune du premier et du $n+1$-ème mur : $p-1$ choix. On a donc

   $$\operatorname{card} B_{n+2} = (p-1)u_n.$$

   Dénombrons C_{n+2}. Pour cela, on commence par peindre les $n+1$ premiers murs de sorte qu'il n'y ait jamais deux murs consécutifs de la même couleur et que le premier et le $n+1$-ème mur soient de couleurs différentes : cela laisse u_{n+1} choix puisque cela revient à dénombrer A_{n+1}. Ensuite, on peint le $n+2$-ème mur d'une couleur différente des couleurs du premier et du $n+1$-ème mur : $p-2$ choix. On a donc

   $$\operatorname{card} C_{n+2} = (p-2)u_{n+1}.$$

   En définitive, on obtient

   $$\boxed{\forall n \geqslant 2, \qquad u_{n+2} = (p-2)u_{n+1} + (p-1)u_n.}$$

3. *Justifier qu'il est cohérent de poser $u_1 = 0$ et $u_0 = p$.*

   Pour $n = 1$, la relation de récurrence de la question précédente nous dit que

   $$u_3 = (p-2)u_2 + (p-1)u_1.$$

   En y reportant les résultats de la question 1, il vient

   $$p(p-1)(p-2) = (p-2)p(p-1) + (p-1)u_1$$

   ce qui incite à poser

   $$\boxed{u_1 = 0.}$$

   Pour $n = 0$, la relation de récurrence de la question précédente donne

   $$u_2 = (p-2)u_1 + (p-1)u_0.$$

   En y reportant les résultats précédents, il vient

   $$p(p-1) = (p-2) \times 0 + (p-1)u_0$$

   ce qui incite à poser

   $$\boxed{u_0 = p.}$$

   Remarque :
   À première vue, cette valeur de u_1 surprend. Si la cour possède un seul mur (oui, je sais, c'est bizarre...), on a p choix de couleur pour ce mur et il serait donc logique d'attribuer à u_1 la valeur p. Mais en fait, avec ce raisonnement, on oublie l'une des contraintes du problème : le mur 1 et le mur n ne doivent pas être de la même couleur. Dans le cas où $n = 1$, cela signifie qu'il est impossible de peindre le mur. Par conséquent, il est tout à fait logique de poser $u_1 = 0$.
   Par contre, l'interprétation en terme de dénombrement de la valeur de u_0 relève de l'ésotérisme le plus complet...

4. *Pour tout $n \geqslant 0$, déterminer une expression explicite de u_n en fonction de n et p.*

   La suite (u_n) est une suite récurrente double dont l'équation caractéristique est

   $$x^2 = (p-2)x + p - 1.$$

   Le discriminant de cette équation vaut

   $$\Delta = (p-2)^2 + 4(p-1) = p^2,$$

   donc les solutions de cette équation sont

   $$x_1 = \frac{p-2-p}{2} = -1 \qquad \text{et} \qquad x_2 = \frac{p-2+p}{2} = p-1.$$

   Le cours nous dit alors qu'il existe $A, B \in \mathbb{R}$ tels que

   $$\forall n \geqslant 1, \qquad u_n = A(-1)^n + B(p-1)^n.$$

   On a

   $$\begin{cases} u_0 = p \\ u_1 = 0 \end{cases} \iff \begin{cases} A + B = p \\ -A + (p-1)B = 0 \end{cases} \iff \begin{cases} A = p-1 \\ B = 1 \end{cases}$$

   donc

   $$\boxed{\forall n \geqslant 0, \qquad u_n = (-1)^n(p-1) + (p-1)^n.}$$

EXERCICE 3

L'objet de cet exercice est d'introduire la topologie de Fürstenberg de $\mathbb{Z}$ et de voir comment elle permet de redémontrer que l'ensemble $\mathbb{P}$ des nombres premiers est infini. Pour tout $a \in \mathbb{Z}$ et tout $r \in \mathbb{N}^*$, on note $A_{a,r}$ le sous-ensemble de $\mathbb{Z}$ constitué des termes de la suite arithmétique de raison r dont a est l'un des termes, c'est-à-dire $A_{a,r} = \{a + kr : k \in \mathbb{Z}\}$. Soit U une partie de $\mathbb{Z}$. On dit que U est un ouvert de $\mathbb{Z}$ lorsque pour tout $x \in U$, il existe $r \in \mathbb{N}^*$ tel que $A_{x,r} \subset U$. Soit F une partie de $\mathbb{Z}$. On dit que F est un fermé de $\mathbb{Z}$ lorsque $\mathbb{Z} \setminus F$ est un ouvert de $\mathbb{Z}$.

1. a) *Démontrer que : $\varnothing$ et $\mathbb{Z}$ sont des ouverts de $\mathbb{Z}$; toute réunion d'ouverts de $\mathbb{Z}$ est un ouvert de $\mathbb{Z}$; toute intersection finie d'ouverts de $\mathbb{Z}$ est un ouvert de $\mathbb{Z}$.*

   L'assertion $\forall x \in \varnothing,\ \exists r \in \mathbb{N}^*,\ A_{x,r} \subset \varnothing$ est vraie puisqu'elle commence par « $\forall x \in \varnothing$ » donc

   $\boxed{\varnothing \text{ est un ouvert de } \mathbb{Z}.}$

   Pour tout $x \in \mathbb{Z}$, on a $A_{x,1} \subset \mathbb{Z}$ (évidemment !) donc l'assertion $\forall x \in \mathbb{Z},\ \exists r \in \mathbb{N}^*,\ A_{x,r} \subset \mathbb{Z}$ est vraie, ce qui signifie que

   $\boxed{\mathbb{Z} \text{ est un ouvert de } \mathbb{Z}.}$

   Soit $(U_i)_{i \in I}$ une famille d'ouverts de $\mathbb{Z}$ (où I est un ensemble d'indices quelconque). Soit $x \in \bigcup_{i \in I} U_i$. Il existe alors $i_0 \in I$ tel que $x \in U_{i_0}$. Comme U_{i_0} est ouvert dans $\mathbb{Z}$, il existe $r \in \mathbb{N}^*$ tel que $A_{x,r} \subset U_{i_0}$. Mézalors $A_{x,r} \subset \bigcup_{i \in I} U_i$. Cela démontre que $\bigcup_{i \in I} U_i$ est un ouvert de $\mathbb{Z}$. Donc

   $\boxed{\text{toute réunion d'ouverts de } \mathbb{Z} \text{ est un ouvert de } \mathbb{Z}.}$

   Soit $(U_1, \ldots, U_n)$ une famille finie d'ouverts de $\mathbb{Z}$. Soit $x \in U_1 \cap \cdots \cap U_n$. Alors, pour tout $i \in [\![1; n]\!]$, on a $x \in U_i$. Comme chaque U_i est un ouvert de $\mathbb{Z}$, on sait que, pour tout $i \in [\![1; n]\!]$, il existe $r_i \in \mathbb{N}^*$ tel que $A_{x,r_i} \subset U_1 \cap \cdots \cap U_n$. Posons $r = r_1 \vee \cdots \vee r_n$. Alors, pour tout $i \in [\![1; n]\!]$, on sait que r_i divise r, ce qui implique que $A_{x,r} \subset A_{x,r_i}$. Donc $A_{x,r} \subset U_1 \cap \cdots \cap U_n$. Cela démontre que $U_1 \cap \cdots \cap U_n$ est un ouvert de $\mathbb{Z}$. En conclusion,

   $\boxed{\text{toute intersection finie d'ouverts de } \mathbb{Z} \text{ est un ouvert de } \mathbb{Z}.}$

   b) *Quelles propriétés analogues sur les fermés de $\mathbb{Z}$ peut-on énoncer ? On expliquera brièvement comment elles se démontrent.*

   En passant aux complémentaires dans les propriétés de la question a), on obtient les résultats suivants sur les fermés de $\mathbb{Z}$:

   $\boxed{\begin{array}{l} 1)\ \varnothing \text{ et } \mathbb{Z} \text{ sont des fermés de } \mathbb{Z}\,; \\ 2)\ \text{toute intersection de fermés de } \mathbb{Z} \text{ est un fermé de } \mathbb{Z}\,; \\ 3)\ \text{toute réunion finie de fermés de } \mathbb{Z} \text{ est un fermé de } \mathbb{Z}. \end{array}}$

2. *Soient $a \in \mathbb{Z}$ et $r \in \mathbb{N}^*$. Démontrer que $A_{a,r}$ est à la fois un ouvert et un fermé de $\mathbb{Z}$.*

   Soit $x \in A_{a,r}$ de sorte qu'il existe $\ell \in \mathbb{Z}$ tel que $x = a + \ell r$. On a alors

   $$A_{x,r} = \{x + kr : k \in \mathbb{Z}\} = \{a + (\ell + k)r : k \in \mathbb{Z}\} = \{a + mr : m \in \mathbb{Z}\} = A_{a,r}.$$

   De cette égalité, on retient que $A_{x,r} \subset A_{a,r}$, ce qui démontre que

   $\boxed{A_{a,r} \text{ est un ouvert de } \mathbb{Z}.}$

   Les nombres $a, a+1, \ldots, a+r-1$ constituent une famille de représentants des différentes classes de congruence modulo r. Par conséquent, les ensembles $A_{a,r}, A_{a+1,r}, \ldots, A_{a+r-1,r}$ forment une partition de $\mathbb{Z}$. Il s'ensuit que

   $$\mathbb{Z} \setminus A_{a,r} = A_{a+1,r} \cup A_{a+2,r} \cup \cdots \cup A_{a+r-1,r}.$$

   Comme $A_{a+1,r} \cup A_{a+2,r} \cup \cdots \cup A_{a+r-1,r}$ est une réunion d'ouverts de $\mathbb{Z}$, on peut affirmer que c'est un ouvert de $\mathbb{Z}$. Par suite, $A_{a,r}$ est le complémentaire d'un ouvert de $\mathbb{Z}$, ce qui signifie que

   $\boxed{A_{a,r} \text{ est un fermé de } \mathbb{Z}.}$

3. *Déterminer $\bigcup_{p\in\mathbb{P}} A_{0,p}$ et en déduire que $\mathbb{P}$ est infini.*

On sait que tous les entiers sauf -1 et 1 admettent un diviseur premier (on peut prendre le plus petit diviseur positif strictement supérieur à 1 ou même invoquer le théorème de décomposition en nombres premiers). Par conséquent, on a

$$\boxed{\bigcup_{p\in\mathbb{P}} A_{0,p} = \mathbb{Z}\setminus\{-1;1\}.}$$

Par l'absurde : on suppose que $\mathbb{P}$ est un ensemble fini. Alors $\bigcup_{p\in\mathbb{P}} A_{0,p}$ est une réunion finie de fermés de $\mathbb{Z}$, donc c'est un fermé de $\mathbb{Z}$. L'égalité ci-dessus nous dit alors que $\{-1;1\}$ est un ouvert de $\mathbb{Z}$. Cela signifie qu'il existe $r\in\mathbb{N}^*$ tel que $A_{1,r}\subset\{-1;1\}$. C'est absurde puisque $A_{1,r}$ est infini. Donc

$$\boxed{\mathbb{P} \text{ est infini.}}$$

EXERCICE 4

Soit A une partie de $\mathbb{R}$. On dit que $x \in \mathbb{R}$ est un point d'accumulation de A lorsque, pour tout $\varepsilon > 0$, on a $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[\neq \varnothing$. L'ensemble des points d'accumulation de A est noté A' et s'appelle l'ensemble dérivé de A.

1. *Reformuler la définition d'un point d'accumulation à l'aide de la notion d'adhérence.*

   On peut reformuler la définition de point d'acumulation de la façon suivante :

   $$\boxed{x \in \mathbb{R} \text{ est un point d'accumulation de } A \text{ lorsque } x \in \mathrm{Adh}(A \setminus \{x\}).}$$

2. a) *Donner un exemple d'ensemble infini D tel que $D' = \varnothing$.*

   Nous allons démontrer que $\mathbb{Z}' = \varnothing$.

   Soit $x \in \mathbb{R}$.

   Si $x \in \mathbb{Z}$, on a $\mathbb{Z} \cap]x-1; x[\cup]x; x+1[= \varnothing$ donc $\forall \varepsilon > 0,\ \mathbb{Z} \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[\neq \varnothing$ est fausse (puisqu'elle admet $\varepsilon = 1$ comme contre-exemple). Ainsi x n'est pas un point d'accumulation.

   Si $x \notin \mathbb{Z}$, on pose $\varepsilon_0 = \min\{x - \lfloor x \rfloor, \lceil x \rceil - x\}$ de sorte que $\mathbb{Z} \cap]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[= \varnothing$. L'assertion $\forall \varepsilon > 0,\ \mathbb{Z} \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[\neq \varnothing$ est donc à nouveau fausse (cette fois, c'est $\varepsilon = \varepsilon_0$ qui donne un contre-exemple). Donc x n'est pas un point d'accumulation.

   On constate ainsi qu'aucun nombre réel n'est un point d'accumulation de $\mathbb{Z}$, c'est-à-dire

   $$\boxed{\mathbb{Z}' = \varnothing.}$$

   b) *On pose $H = \{1/n : n \in \mathbb{N}^*\}$. Démontrer que $0 \in H'$.*

   Pour tout $\varepsilon > 0$, on a

   $$H \cap]-\varepsilon; 0[\cup]0; \varepsilon[= \{1/n : n > 1/\varepsilon\} \neq \varnothing,$$

   donc

   $$\boxed{0 \in H'.}$$

3. *Démontrer que $x \in \mathbb{R}$ est un point d'accumulation de A si, et seulement si, pour tout $\varepsilon > 0$, l'ensemble $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$ est infini.*

   Soit $x \in \mathbb{R}$.

   $\Leftarrow$ Supposons que, pour tout $\varepsilon > 0$, l'ensemble $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$ est infini. A fortiori, pour tout $\varepsilon > 0$, l'ensemble $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$ est non vide. Donc x est un point d'accumulation.

   $\Rightarrow$ Supposons réciproquement que x est un point d'accumulation, c'est-à-dire que, pour tout $\alpha > 0$, l'ensemble $A \cap]x-\alpha; x[\cup]x; x+\alpha[$ est non vide.

   Soit $\varepsilon > 0$. On souhaite démontrer que $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$ est infini.

   L'hypothèse (avec $\alpha = \varepsilon$) nous dit que $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$ est non vide, donc il existe $x_0 \in A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$.

   On pose alors $\varepsilon_1 = |x_0 - x|$ de sorte que $\varepsilon_1 > 0$ (car $x_0 \neq x$) et $x_0 \notin]x-\varepsilon_1; x[\cup]x; x+\varepsilon_1[$. L'hypothèse (avec $\alpha = \varepsilon_1$) nous dit que $A \cap]x-\varepsilon_1; x[\cup]x; x+\varepsilon_1[$ est non vide, donc il existe $x_1 \in A \cap]x-\varepsilon_1; x[\cup]x; x+\varepsilon_1[$. On a nécessairement $x_1 \neq x_0$.

   On pose alors $\varepsilon_2 = |x_1 - x|$ de sorte que $\varepsilon_2 > 0$ (car $x_1 \neq x$) et $x_0, x_1 \notin]x-\varepsilon_2; x[\cup]x; x+\varepsilon_2[$. L'hypothèse (avec $\alpha = \varepsilon_2$) nous dit que $A \cap]x-\varepsilon_2; x[\cup]x; x+\varepsilon_2[$ est non vide, donc il existe $x_2 \in A \cap]x-\varepsilon_2; x[\cup]x; x+\varepsilon_2[$. On a nécessairement $x_2 \neq x_0$ et $x_2 \neq x_1$.

   Etc.

   On construit ainsi par récurrence une suite $(x_n)_{n \geqslant 0}$ d'éléments distincts qui appartiennent tous à $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$.

   Donc $A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[$ est infini.

   En conclusion,

   $$\boxed{\begin{array}{l} x \in \mathbb{R} \text{ est un point d'accumulation de } A \text{ si, et seulement si, pour} \\ \text{tout } \varepsilon > 0, \text{ l'ensemble } A \cap]x-\varepsilon; x[\cup]x; x+\varepsilon[\text{ est infini.} \end{array}}$$

4. *Démontrer que A' est un fermé de $\mathbb{R}$.*

   Démontrons que $\mathbb{R} \setminus A'$ est un ouvert de $\mathbb{R}$.
   Soit $x \in \mathbb{R} \setminus A'$.
   Comme x n'est pas un point d'accumulation, il existe $\varepsilon_0 > 0$ tel que $A \cap]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[= \varnothing$.
   Nous allons démontrer que $]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[$ est inclus dans $\mathbb{R} \setminus A'$.
   Soit $t \in]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[$. Comme $]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[$ est un ouvert de $\mathbb{R}$ (c'est l'union de deux intervalles ouverts), il existe $r > 0$ tel que $]t-r; t+r[\subset]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[$. Mézalors, comme $A \cap (]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[) = \varnothing$, on a aussi $A \cap]t-r; t+r[= \varnothing$. A fortiori, on en déduit que $A \cap (]t-r; t[\cup]t; t+r[) = \varnothing$. Cela démontre que t n'est pas un point d'accumulation de A, c'est-à-dire $t \in \mathbb{R} \setminus A'$.
   On a donc bien démontré que $]x-\varepsilon_0; x[\cup]x; x+\varepsilon_0[$ est inclus dans $\mathbb{R} \setminus A'$.
   Comme on savait déjà que $x \in \mathbb{R} \setminus A'$, on en déduit que $]x-\varepsilon_0; x+\varepsilon_0[$ est inclus dans $\mathbb{R} \setminus A'$.
   En résumé, on a démontré que, pour tout $x \in \mathbb{R} \setminus A'$, il existe $\varepsilon_0 > 0$ tel que $]x-\varepsilon_0; x+\varepsilon_0[\subset \mathbb{R} \setminus A'$, ce qui signifie que $\mathbb{R} \setminus A'$ est un ouvert de $\mathbb{R}$.
   Par conséquent,

   $$\boxed{A' \text{ est un fermé de } \mathbb{R}.}$$

5. a) *Démontrer que* $\mathrm{Adh}(A) = A \cup A'$.

   On procède par double inclusion.

   $\subset$ Soit $x \in \mathrm{Adh}(A)$. On veut démontrer que $x \in A \cup A'$, c'est-à-dire que $x \in A$ ou $x \in A'$.
   On suppose donc que $x \notin A$ et on va démontrer que $x \in A'$.
   Comme $x \in \mathrm{Adh}(A)$, on sait que, pour tout $\varepsilon > 0$, on a $A \cap]x-\varepsilon, x+\varepsilon[\neq \varnothing$.
   Or $x \notin A$, donc, pour tout $\varepsilon > 0$, on a $A \cap (]x-\varepsilon; x[\cup]x; x+\varepsilon[) \neq \varnothing$.
   Cela signifie que $x \in A'$.
   Donc $\mathrm{Adh}(A) \subset A \cup A'$.

   $\supset$ Soit $x \in A \cup A'$. On veut démontrer que $x \in \mathrm{Adh}(A)$.
   Comme $x \in A \cup A'$, on a $x \in A$ ou $x \in A'$.
   Si $x \in A$, on a immédiatement $x \in \mathrm{Adh}(A)$ puisque l'on sait que $A \subset \mathrm{Adh}(A)$.
   Si $x \in A'$, on a $x \in \mathrm{Adh}(A \setminus \{x\})$. Or $A \setminus \{x\} \subset A$ donc $\mathrm{Adh}(A \setminus \{x\}) \subset \mathrm{Adh}(A)$. Cela implique que $x \in \mathrm{Adh}(A)$.
   On a ainsi démontré que $A \cup A' \subset \mathrm{Adh}(A)$.

   En définitive, on a

   $$\boxed{\mathrm{Adh}(A) = A \cup A'.}$$

   b) *Démontrer que A est un fermé de $\mathbb{R}$ si, et seulement si, $A' \subset A$.*

   On a

   $$\begin{aligned} (A \text{ est un fermé de } \mathbb{R}) &\iff \big(A = \mathrm{Adh}(A)\big) && \text{c'est du cours} \\ &\iff \big(A = A \cup A'\big) && \text{d'après a)} \\ &\iff (A' \subset A). \end{aligned}$$

   Donc

   $$\boxed{A \text{ est un fermé de } \mathbb{R} \text{ si, et seulement si, } A' \subset A.}$$

EXERCICE 5

L'objet de ce problème est de démontrer le théorème des deux carrés de Fermat : un entier $n \in \mathbb{N}^*$ est la somme de deux carrés si, et seulement si, pour tout nombre premier p congru à 3 modulo 4 la valuation p-adique de n est paire.

A. *Soit p un nombre premier. On suppose qu'il existe $a, b \in \mathbb{N}^*$ tels que p divise $a^2 + b^2$ et $a \wedge b = 1$.*

1. *Démontrer qu'il existe deux couples distincts (x_1, y_1) et (x_2, y_2) dans $\left([0; \sqrt{p}[\cap \mathbb{N}\right)^2$ tels que $ax_1 + by_1 \equiv ax_2 + by_2\ [p]$.*

   Le cardinal de $\left([0; \sqrt{p}[\cap\mathbb{N}\right)^2$ est $(\lfloor\sqrt{p}\rfloor+1)^2$ et le cardinal de $\mathbb{F}_p$ est p. Comme $(\lfloor\sqrt{p}\rfloor+1)^2 > p$ car $\lfloor\sqrt{p}\rfloor > \sqrt{p} - 1$, on en déduit que l'application

$$\begin{cases} \left([0; \sqrt{p}[\cap \mathbb{N}\right)^2 & \longrightarrow & \mathbb{F}_p \\ (x, y) & \longmapsto & ax + by \end{cases}$$

   ne peut pas être injective (c'est le principe des tiroirs !). Il existe donc deux couples distincts (x_1, y_1) et (x_2, y_2) de $\left([0; \sqrt{p}[\cap \mathbb{N}\right)^2$ tels que $ax_1 + by_1 = ax_2 + by_2$ dans $\mathbb{F}_p$. Autrement dit,

   > il existe donc deux couples distincts (x_1, y_1) et (x_2, y_2) de $\left([0; \sqrt{p}[\cap \mathbb{N}\right)^2$ tels que $ax_1 + by_1 \equiv ax_2 + by_2\ [p]$.

2. *On pose $u = x_1 - x_2$ et $v = y_1 - y_2$. Démontrer que p divise $a^2u^2 - b^2v^2$, puis que p divise $u^2 + v^2$ et enfin que $p = u^2 + v^2$.*

   La question précédente nous dit que $a(x_1-x_2)+b(y_1-y_2) \equiv 0\ [p]$, c'est-à-dire que $au+bv \equiv 0\ [p]$ ou encore que p divise $au + bv$. Mézalors, p divise aussi $(au + bv)(au - bv)$, c'est-à-dire

   > p divise $a^2u^2 - b^2v^2$.

   L'astuce de Binet nous dit que

$$a^2u^2 - b^2v^2 = (a^2 + b^2)u^2 - b^2(u^2 + v^2).$$

   Dans cette égalité, on sait que p divise $a^2u^2 - b^2v^2$ et $a^2 + b^2$, donc aussi que

$$p \text{ divise } b^2(u^2 + v^2).$$

   Justifions que p est premier avec b^2. Pour cela, on raisonne par l'absurde en supposant que p n'est pas premier avec b^2. Comme p est un nombre premier, cela signifie que p divise b^2 et donc que p divise b. Mais (il y a toujours un mais...) comme p divise $a^2 + b^2$ et b^2, il divise aussi a^2, ce qui signifie que p divise a (toujours parce que p est un nombre premier). Comme a et b sont premiers entre eux, il est impossible que p les divise tous les deux. Nous tenons notre absurdité ! Donc

$$p \wedge b^2 = 1.$$

   Le lemme de Gauss nous dit alors que

   > p divise $u^2 + v^2$.

   Comme x_1, x_2, y_1, y_2 sont des éléments de $[0; \sqrt{p}[\cap\mathbb{N}$, on en déduit que $u = x_1-x_2$ et $v = y_1-y_2$ appartiennent à $]-\sqrt{p}; \sqrt{p}[\cap \mathbb{Z}$ et donc que u^2 et v^2 sont dans $[0; p[\cap \mathbb{N}$. Il s'ensuit que

$$u^2 + v^2 \in [0; 2p[\cap \mathbb{N}.$$

   Par ailleurs, comme les couples (x_1, y_1) et (x_2, y_2) sont distincts, on sait que $(u, v) \neq (0, 0)$, ce qui permet de préciser que

$$u^2 + v^2 \in]0; 2p[\cap \mathbb{N}.$$

   Enfin, comme $u^2 + v^2$ est un multiple de p et que le seul multiple de p dans $]0; 2p[\cap \mathbb{N}$ est p lui-même, on en conclut que

   > $p = u^2 + v^2$.

B. *Soit p un nombre premier impair.*

1. *Justifier que 2 est une somme de deux carrés.*

   On a
   $$\boxed{2 = 1^2 + 1^2.}$$

2. *On suppose que p est une somme de deux carrés, c'est-à-dire qu'il existe $a, b \in \mathbb{N}^*$ tels que $p = a^2 + b^2$. Démontrer que $p \equiv 1$ [4].*

   Dans $\mathbb{Z}/4\mathbb{Z}$, on a $0^2 = 0$, $1^2 = 1$, $2^2 = 0$ et $3^2 = 1$ donc les carrés de $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1. Il s'ensuit que $p = a^2 + b^2$ vaut 0, 1 ou 2 dans $\mathbb{Z}/4\mathbb{Z}$. Comme p est impair, il ne peut pas valoir 0 ou 2 modulo 4, donc il reste seulement la possibilité que
   $$\boxed{p \equiv 1 \ [4].}$$

3. *Réciproquement, on suppose que $p \equiv 1$ [4].*

   α] *On pose $m = (p-1)/2$. Justifier que $\mathbb{F}_p^* = [\![-m; m]\!] \setminus \{0\}$. En déduire que $(m!)^2 \equiv -1$ [p].*

   Pour avoir exactement un représentant de chaque classe de congruence modulo p, il suffit de prendre p entiers consécutifs. Dans l'intervalle $[\![-m; m]\!]$, on compte $2m+1 = p$ entiers. On a donc $\mathbb{F}_p = [\![-m; m]\!]$ et par suite
   $$\boxed{\mathbb{F}_p^* = [\![-m; m]\!] \setminus \{0\}.}$$

   Pour démontrer que $m!^2 \equiv -1$ [p], inspirons nous de la preuve du théorème de Wilson.
   Les éléments x de $\mathbb{F}_p^*$ qui sont leur propre inverse vérifie $x^2 = 1$, c'est-à-dire $x^2 - 1 = 0$ ou encore $(x-1)(x+1) = 0$, ce qui donne $x = \pm 1$ par intégrité (tout corps est intègre !).
   Dès lors, lorsqu'on calcule le produit de tous les éléments de $\mathbb{F}_p^*$, ils se simplifient tous par paire d'inversibles, sauf 1 et -1. Ce produit vaut donc -1 dans $\mathbb{F}_p$.
   Or, dans $\mathbb{F}_p$, le produit des éléments de $\mathbb{F}_p^* = [\![-m; m]\!] \setminus \{0\}$ vaut également
   $$\begin{aligned} & (-m) \times (-m+1) \times \cdots \times (-2) \times (-1) \times 1 \times 2 \times \cdots \times (m-1) \times m \\ = \ & (-1)^m (m!)^2 \\ = \ & (m!)^2, \end{aligned}$$
   car $(-1)^m = 1$ puisque m est pair (car $p \equiv 1$ [4]).
   On en déduit que, dans $\mathbb{F}_p$, on a
   $$(m!)^2 = -1,$$
   c'est-à-dire
   $$\boxed{(m!)^2 \equiv -1 \ [p].}$$

   β] *Justifier que p est une somme de deux carrés.*

   La question précédente nous dit que le nombre premier p divise $1 + (m!)^2$, qui est une somme de deux carrés. Comme 1 et $m!$ sont premiers entre eux (pardi, tout entier est premier avec 1 !), le lemme d'Euler démontré à la question A s'applique pour dire que
   $$\boxed{p \text{ est une somme de deux carrés.}}$$

C. *Soit $n \in \mathbb{N}^*$.*

a) α] *Démontrer que le produit de deux entiers qui sont des sommes de deux carrés est une somme de deux carrés.*

Soient r, s deux entiers qui sont sommes de deux carrés. Il existe alors $a, b, c, d \in \mathbb{Z}$ tels que $r = a^2 + b^2$ et $s = c^2 + d^2$. Alors
$$\begin{aligned} rs &= (a^2 + b^2)(c^2 + d^2) \\ &= |a + ib|^2 \times |c + id|^2 \\ &= |(a + ib)(c + id)|^2 \\ &= |(ac - bd) + i(ad + bc)|^2 \\ &= (ac - bd)^2 + (ad + bc)^2, \end{aligned}$$
ce qui prouve que rs est une somme de deux carrés puisque $ac - bd \in \mathbb{Z}$ et $ad + bc \in \mathbb{Z}$.
Donc
$$\boxed{\begin{array}{l}\text{le produit de deux entiers qui sont des sommes} \\ \text{de deux carrés est une somme de deux carrés.}\end{array}}$$

β] *On suppose que, pour tout nombre premier p congru à 3 modulo 4, $v_p(n)$ est pair. Démontrer que n est une somme de deux carrés.*

Dans la décomposition de n en nombres premiers, on isole le nombre premier 2 (qui ne fait jamais rien comme tout le monde) et l'on sépare les nombres premiers congrus à 1 modulo 4 des nombres premiers congrus à 3 modulo 4, ce qui donne

$$n = 2^{v_2(n)} \times \prod_{\substack{p\in\mathbb{P}\\ p\equiv 1\ [4]}} p^{v_p(n)} \times \prod_{\substack{p\in\mathbb{P}\\ p\equiv 3[4]}} p^{v_p(n)}.$$

On sait, d'après la question B, que 2 et les nombres premiers congrus à 1 modulo 4 sont des sommes de deux carrés. Par ailleurs, on sait que, pour tout nombre premier p congru à 3 modulo 4, la valuation $v_p(n)$ est paire, ce qui permet d'écrire que $p^{v_p(n)} = \left(p^{v_p(n)/2}\right)^2 + 0^2$ et donc d'affirmer que si $p \equiv 3$ [4], chaque terme $p^{v_p(n)}$ est une somme de deux carrés. Par conséquent, tous les facteurs de la décomposition de n sont des sommes de deux carrés.
Or on sait qu'un produit de sommes de deux carrés est une somme de deux carrés (il suffit d'itérer le résultat de la question précédente).
Par conséquent,

$\boxed{n \text{ est une somme de deux carrés.}}$

b) *Réciproquement, on suppose que n est somme de deux carrés, c'est-à-dire qu'il existe $a, b \in \mathbb{N}^*$ tels que $n = a^2 + b^2$. Démontrer que, pour tout nombre premier p congru à 3 modulo 4 la valuation p-adique de n est paire.*

Posons $\delta = a \wedge b$. Comme δ divise a et b, on sait que δ^2 divise $a^2 + b^2$, c'est-à-dire δ^2 divise n. On peut donc simplifier l'égalité $n = a^2 + b^2$ par δ^2, ce qui donne

$$\frac{n}{\delta^2} = \left(\frac{a}{\delta}\right)^2 + \left(\frac{b}{\delta}\right)^2 \qquad \text{avec} \qquad \frac{a}{\delta} \wedge \frac{b}{\delta} = 1.$$

Dès lors, si l'on considère un nombre premier p qui divise n/δ^2, alors il divise $(a/\delta)^2 + (b/\delta)^2$ avec $(a/\delta)\wedge(b/\delta) = 1$. Cela permet d'appliquer le lemme d'Euler de la question A pour affirmer que p est lui-même une somme de deux carrés. La question B nous dit alors que p est ou bien égal à 2 ou bien congru à 1 modulo 4.
Cela signifie que les facteurs premiers de n qui sont congrus à 3 modulo 4 sont dans la décomposition primaire de δ^2. Comme δ^2 est un carré, cela entraine la parité de la valuation p-adique de n lorsque p est congru à 3 modulo 4.
En conclusion,

$\boxed{\text{pour tout nombre premier } p \text{ congru à 3 modulo 4 la valuation } p\text{-adique de } n \text{ est paire.}}$

EXERCICE 6

Dans cet exercice, on admet le théorème de Lagrange : si G est groupe fini et H un sous-groupe de G alors $\operatorname{card} H$ *divise* $\operatorname{card} G$. *Nous démontrerons ce théorème plus tard dans l'année.*

1. *Soit $p \in \mathbb{P} \setminus \{2;3\}$. Démontrer que p est congru à 1 ou 5 modulo 6.*

   Les nombres congrus à 0, 2 ou 4 modulo 6 sont tous divisibles par 2 et ne sont donc pas premiers (sauf 2).

   Les nombres congrus à 3 modulo 6 sont tous divisibles par 3 et ne sont donc pas premiers (sauf 3).

   Par conséquent, les seules classes de congruences dans lesquelles peuvent se répartir les nombres premiers sont celles de 1 et 5. Autrement dit,

   $$\boxed{p \text{ est congru à 1 ou 5 modulo 6.}}$$

2. *Démontrer qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.*

   Raisonnons par l'absurde en supposant qu'il existe un nombre fini de nombres premiers congrus à 5 modulo 6 et notons les $p_1, \dots, p_n$. On pose alors

   $$N = 6p_1 \dots p_n - 1.$$

   Notons que $N \equiv 5\ [6]$.

   Par ailleurs, comme N est premier avec 2, 3 et tous les p_i (car $6p_1 \dots p_n$ est divisible par 2, 3 et tous les p_i mais pas par -1), tous les diviseurs premiers de N sont congrus à 1 modulo 6. Or, un produit de nombres congrus à 1 modulo 6 est lui-même congru à 1 modulo 6, donc $N \equiv 1\ [6]$.

   On a donc $5 \equiv 1\ [6]$, ce qui est absurde !

   Donc

   $$\boxed{\text{il existe une infinité de nombres premiers congrus à 5 modulo 6.}}$$

3. a) *Soit $p \in \mathbb{P} \setminus \{2;3\}$. On suppose que -3 est un carré dans $\mathbb{F}_p$, c'est-à-dire qu'il existe $a \in F_p$ tel que $a^2 = -3$ dans $\mathbb{F}_p$. Toujours dans $\mathbb{F}_p$, on pose $j = 2^{-1}(a-1)$.*

   α] *Justifier l'existence de j.*

   Comme $p \neq 2$, on a $2 \neq 0$ dans le corps $\mathbb{F}_p$, ce qui assure que 2 est inversible dans $\mathbb{F}_p$. Par conséquent,

   $$\boxed{j \text{ existe.}}$$

   β] *Calculer j^2 et j^3 dans $\mathbb{F}_p$.*

   On a

   $$\begin{aligned} j^2 &= 2^{-2}(a^2 - 2a + 1) \\ &= 2^{-2}(-3 - 2a + 1) \\ &= 2^{-2}(-2a - 2) \\ &= -2^{-1}(a+1) \end{aligned}$$

   et

   $$\begin{aligned} j^3 &= j^2 j \\ &= -2^{-1}(a+1)2^{-1}(a-1) \\ &= -2^{-2}(a^2 - 1) \\ &= -2^{-2}(-3 - 1) \\ &= 2^{-2} \times 2^2 \\ &= 1. \end{aligned}$$

   Donc

   $$\boxed{j^2 = -2^{-1}(a+1) \qquad \text{et} \qquad j^3 = 1.}$$

γ] *Démontrer que* $H = \{1, j, j^2\}$ *est un sous-groupe de* $(\mathbb{F}_p^*, \times)$ *de cardinal* 3.

On a $1 \in H$.

On a $1 \times j = j \in H$, $1 \times j^2 = j^2 \in H$ et $j \times j^2 = j^3 = 1 \in H$ donc H est stable par $\times$.

On a $1^{-1} = 1 \in H$, $j^{-1} = j^2 \in H$ et $(j^2)^{-1} = j \in H$ dont H est stable par passage à l'inverse.

On en déduit que

$$\boxed{H \text{ est un sous-groupe de } (\mathbb{F}_p^*, \times).}$$

Démontrons que H est de cardinal 3, c'est-à-dire $1 \neq j$, $j \neq j^2$ et $1 \neq j^2$.

Par l'absurde, supposons que $1 = j$. On a alors $2 = a - 1$, c'est-à-dire $a = 3$. Comme $a^2 = -3$, cela donne $9 = -3$ dans $\mathbb{F}_p$. Mézalors p doit diviser 12, ce qui donne $p = 2$ ou $p = 3$. C'est absurde !

Par l'absurde, supposons que $j = j^2$. On a alors $a - 1 = -a - 1$, c'est-à-dire $a = 0$. Comme $a^2 = -3$, cela donne $0 = -3$ dans $\mathbb{F}_p$. Mézalors p doit diviser 3, ce qui donne $p = 3$. C'est absurde !

Par l'absurde, supposons que $1 = j^2$. On a alors $2 = -a - 1$, c'est-à-dire $a = -3$. Comme $a^2 = -3$, cela donne à nouveau $9 = -3$ dans $\mathbb{F}_p$. C'est toujours absurde !

Par conséquent,

$$\boxed{\operatorname{card} H = 3.}$$

δ] *En déduire que* $p \equiv 1\ [6]$.

Le théorème de Lagrange nous dit que le cardinal de H divise celui de $\mathbb{F}_p^*$, c'est-à-dire que 3 divise $p - 1$.

Par ailleurs, comme p est impair, $p - 1$ est pair, c'est-à-dire divisible par 2.

Comme 2 et 3 sont premiers entre eux, l'indépendance divisorielle nous dit que 6 divise $p - 1$, c'est-à-dire

$$\boxed{p \equiv 1\ [6].}$$

b) *Démontrer qu'il existe une infinité de nombres premiers congrus à* 1 *modulo* 6.

Raisonnons par l'absurde en supposant qu'il existe un nombre fini de nombres premiers congrus à 1 modulo 6 et notons les $p_1, \ldots, p_n$. On pose alors

$$N = (2p_1 \ldots p_n)^2 + 3.$$

Comme N est premier avec 2 et 3, il admet un facteur premier $p \in \mathbb{P} \setminus \{2; 3\}$. Dans $\mathbb{F}_p$, on a alors $(2p_1 \ldots p_n)^2 = -3$, ce qui prouve que -3 est un carré. Par conséquent, la question a) nous dit que p est congru à 1 modulo 6.

Par ailleurs, p divisant N, il est nécessairement distinct de $p_1, \ldots, p_n$.

C'est absurde !

Donc

$$\boxed{\text{il existe une infinité de nombres premiers congrus à 1 modulo 6.}}$$