Devoir Surveillé n° 8 (4h)

La présentation, la lisibilité, l'orthographe, la qualité de la rédaction, la clarté, la précision et la concision des raisonnements entreront pour une part importante dans l'appréciation des copies.

Les candidats sont invités à encadrer dans la mesure du possible les résultats de leurs calculs.

L'usage de tout document et de tout matériel électronique est interdit. Notamment, les téléphones portables doivent être éteints *et* rangés.

Problème 1 – Le dernier théorème de Fermat pour les exposants $n = 4$ et $n = 3$

Le but de ce problème est de démontrer l'assertion suivante lorsque $n = 3$ et $n = 4$:

> Pour tout $n \geqslant 3$, il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $x^n + y^n = z^n$ et $xyz \neq 0$
> (théorème de Fermat-Wiles, ou dernier théorème de Fermat ; « dernier » dans le sens où c'est le dernier à avoir été démontré ou réfuté ; au moment ou cette appelation s'est installée, c'était le dernier qui restait encore à démontrer...)

Pierre de Fermat croyait en avoir une démonstration dans le cas général, ainsi que l'indique sa célèbre citation, en marge d'une traduction par Bachet de Mériziac des *Arithmétiques* de Diophante :

> *« Décomposer un cube en deux autres cubes, une quatrième puissance, et généralement une puissance quelconque en deux puissances de même nom, au dessus de la seconde puissance, est chose impossible et j'en ai assurément trouvé l'admirable démonstration. La marge trop exiguë ne la contiendrait pas. »*

Le cas le plus simple à traiter est le cas $n = 4$, qui utilise des techniques et résultats connus de Fermat. C'est probablement à cette preuve que pensait Fermat, et qu'il pensait pouvoir généraliser. Euler a prouvé le cas $n = 3$, mais en utilisant implicitement une propriété de l'anneau $\mathbb{Z}[\mathrm{i}\sqrt{3}]$ qui s'avère fausse (mais son erreur est facilement rattrapable, car cet anneau est contenu dans $\mathbb{Z}[j]$ qui possède cette propriété). Gauss a d'ailleurs adapté cette démonstration en se plaçant d'emblée dans $\mathbb{Z}[j]$. Nous étudierons la preuve « à la Fermat » du cas $n = 4$, et la preuve (rectifiée) d'Euler pour le cas $n = 3$. Les cas $n = 5$ (Lejeune Dirichlet et Legendre) et $n = 7$ (Lamé) peuvent encore se démontrer par des moyens élémentaires, mais cela deviendrait beaucoup trop technique. Sophie Germain a montré le théorème pour les valeurs de n premières inférieures à 100, sous certaines restrictions sur x, y et z. Kummer a réussi à prouver le théorème pour presque toutes les valeurs de n inférieures à 100, en introduisant la notion de nombres idéaux. Il a fallu attendre 1994 et le génie d'Andrew Wiles (et de quelques uns de ses prédécesseurs) pour avoir une démontration complète, utilisant des techniques sophistiquées portant sur l'étude de courbes elliptiques.

Question préliminaire
Soit a et b deux entiers positifs premiers entre eux, et n et r deux entiers strictement positifs. Montrer que si $ab = n^r$, il existe deux entiers k et ℓ tels que $a = k^r$ et $b = \ell^r$. Justifier que si r est impair, l'hypothèse de positivité de a et b et n est inutile.

Partie I – Le théorème de Fermat pour l'exposant $n = 4$

1. **Un lemme arithmétique**
   Soit a et b deux entiers premiers entre eux, et $q \in \mathbb{Q}^*$. Montrer que si qa et qb sont entiers alors q est entier.
2. **Triplets pythagoriciens.**
   Un triplet pythagoricien est un triplet $(a, b, c) \in (\mathbb{N}^*)^3$ tel que $a^2 + b^2 = c^2$. Un triangle pythagoricien est un triangle donc les côtés forment un triplet pythagoricien. Un triplet pythagoricien est dit primitif si $a \wedge b = 1$.
   (a) Soit (a, b, c) un triplet pythagoricien. Montrer que les propriétés suivantes sont équivalentes :
      (i) (a, b, c) est primitif
      (ii) a, b et c sont premiers entre eux dans leur ensemble,
      (iii) a, b et c sont premiers entre eux deux à deux.

(b) On suppose que (a, b, c) est un triplet pythagoricien primitif. Montrer que a et b sont de parité opposée, et c est impair.

Quitte à échanger a et b, on peut donc supposer que a est pair et b est impair, choix que nous ferons désormais.

(c) Soit p et q deux entiers premiers entre eux, de parité différente, tels que $p > q$. Montrer que $(2pq, p^2 - q^2, p^2 + q^2)$ est un triplet pythagoricien primitif.

(d) On veut montrer que réciproquement, tout triplet pythagoricien primitif (a, b, c) tel que a est pair est de cette forme.

i. On suppose qu'il existe un couple (p, q) tel que (a, b, c) s'écrive sous la forme donnée dans la question (c), avec $p > q$ et p et q de parité différente, premiers entre eux. Exprimer $\frac{p}{q}$ en fonction de a et $c - b$. En déduire comment définir p et q.

ii. Pour p et q ainsi définis, montrer qu'il existe un entier α tel que

$$p^2 + q^2 = \alpha c \qquad \text{et} \qquad p^2 - q^2 = \alpha b.$$

iii. En considérant $p^2 \wedge q^2$, montrer que $\alpha = 1$, puis conclure que (p, q) répond à la question.

3. **L'aire d'un triangle pythagoricien n'est pas un carré (Fermat)**

Le but de cette question est de prouver l'assertion donnée dans le titre de cette question. Soit (a, b, c) un triplet pythagoricien.

(a) Montrer qu'on peut se limiter au cas où (a, b, c) est primitif.

On suppose désormais que cette condition est satisfaite, avec a pair, et p et q comme dans la question 2. On suppose que l'aire du triangle pythgoricien associé à (a, b, c) est un carré, et on cherche à construire un triangle pythagoricien plus petit satisfaisant la même propriété, en vue d'appliquer le principe de descente infinie.

(b) Exprimer l'aire du triangle pythagoricien associé au triplet (a, b, c) en fonction de p et q.

(c) Montrer que p, q, $p - q$ et $p + q$ sont des carrés (respectivement x^2, y^2, v^2 et u^2).

(d) Montrer que le pgcd de $u + v$ et de $u - v$ est 2.

(e) En déduire que soit $\frac{u+v}{2}$ et $\frac{u-v}{4}$ sont des carrés, soit $\frac{u+v}{4}$ et $\frac{u-v}{2}$ sont des carrés (on pourra étudier le produit $(u - v)(u + v)$).

On se place dans la première situation, la seconde étant similaire, et on note r^2 et s^2 ces deux carrés respectivement.

(f) Montrer que $(r^2, 2s^2, x)$ est un triplet pythagoricien primitif. Quelle est son aire ? Conclure.

4. **Le théorème de Fermat pour l'exposant $n = 4$**

On suppose que x, y et z sont trois entiers non nuls tels que $x^4 + y^4 = z^4$. On peut bien entendu supposer que x, y et z sont positifs.

(a) Montrer qu'on peut supposer que x et y sont premiers entre eux, et x pair. On fait désormais cette hypothèse.

(b) Montrer qu'il existe des entiers a et b tels que $z^2 - y^2 = 8a^4$ et $z^2 + y^2 = 2b^4$.

(c) Trouver une contradiction à l'aide de la question 3.

Partie II – Le théorème de Fermat pour l'exposant $n = 3$ (Euler, Gauss)

Soit $\mathbb{Z}[j]$ le sous-ensemble de $\mathbb{C}$ formé des $a + bj$, où a et b sont entiers, et $j = \mathrm{e}^{\mathrm{i}\frac{2\pi}{3}}$. On vérifie sans difficulté que $\mathbb{Z}[j]$ est un sous-anneau de $\mathbb{C}$. On admet que les unités de $\mathbb{Z}[j]$ sont les éléments de module 1. Soit a et b dans $\mathbb{Z}[j]$. On dit que a divise b s'il existe c dans $\mathbb{Z}[j]$ tel que $ac = b$. On dit qu'un nombre $a \in \mathbb{Z}[j]$ est premier (au sens d'Eisenstein) si a ne se décompose pas dans $\mathbb{Z}[j]$ comme produit de deux entiers dont aucun des deux n'est une unité.
Enfin, on admet (et c'est là le point crucial, qui fait qu'Euler eut de la chance, point que Gauss admit sans le justifier) que $\mathbb{Z}[j]$ est un anneau factoriel, c'est-à-dire que le théorème fondamental de l'arithmétique est vrai dans $\mathbb{Z}[j]$: tout élément de $\mathbb{Z}[j]$ se décompose de façon unique (à unités près et à ordre près) comme produit de nombres premiers d'Eisenstein.

1. **Résolution de $p^2 + 3q^2 = s^3$.**

Un résultat plus général (résolution de $p^2 + 3q^2 = s^r$) fait l'objet d'un autre problème.
On suppose que p, q et s sont trois entiers vérifiant $p^2 + 3q^2 = s^3$, tels que $p \wedge q = 1$.

(a) Montrer que p et q sont premiers entre eux dans $\mathbb{Z}[j]$.

(b) Montrer que $p + \mathrm{i}\sqrt{3} \cdot q$ et $p - \mathrm{i}\sqrt{3} \cdot q$ sont éléments de $\mathbb{Z}[j]$ et sont premiers entre eux.

(c) En déduire que $p + \mathrm{i}\sqrt{3} \cdot q$ est un cube d'un élément $u + \mathrm{i}\sqrt{3} \cdot v$ de $\mathbb{Z}[j]$. Exprimer p et q en fonction de u et v.

(d) Montrer que u et v sont premiers entre eux.

2. **Un changement de variables**

On suppose que (x, y, z) sont trois entiers relatifs non nuls tels que $x^3 + y^3 = z^3$.

(a) Montrer qu'on peut supposer x, y et z premiers entre eux deux à deux, et x et y impairs (donc z pair). On se place désormais sous ces hypothèses

(b) En posant p et q tels que $x = p + q$ et $y = p - q$ (pourquoi p et q sont-ils entiers ?), montrer que

$$\frac{p}{4}(p^2 + 3q^2) = \left(\frac{z}{2}\right)^3.$$

(c) Quelle est la parité de $p^2 + 3q^2$?

(d) Justifier que $\frac{p}{4}$ est entier, puis déterminer la parité de p et q.

3. **Premier cas : z non divisible par 3**

On suppose dans cette question que z n'est pas divisible par 3.

(a) Montrer qu'il existe deux entiers r et s tels que $\frac{p}{4} = r^3$ et $p^2 + 3q^2 = s^3$.

(b) Justifier l'existence d'entiers u et v premiers entre eux tels que

$$p = u(u + 3v)(u - 3v) \qquad \text{et} \qquad q = 3v(u^2 - v^2).$$

(c) Déterminer la parité de u et de v.

(d) Justifier que $\frac{u}{4}$, $u + 3v$ et $u - 3v$ sont des cubes (respectivement a^3, b^3 et c^3), et construire à l'aide de ces cubes une autre solution de l'équation de Fermat pour $n = 3$.

(e) Conclure.

4. **Second cas : z divisible par 3**

On suppose dans cette question que z est divisible par 3. Adapter la preuve précédente en inversant les rôles de p et q (on pourra exprimer $\left(\frac{z}{6}\right)^3$ à l'aide de la quantité $q^2 + 3\left(\frac{p}{3}\right)^2$)

Partie III – Le théorème de Sophie Germain

Par souci de symétrie, et sans modifier la problématique, on peut réécrire, pour n impair, l'équation sous la forme $x^n + y^n + z^n = 0$, quitte à changer le signe de z. Le but de cette partie est de démontrer le théorème de Sophie Germain :

Théorème de Sophie Germain :

Soit p un nombre premier impair tel qu'il existe un nombre premier auxiliaire q tel que :

(i) $\forall (x, y, z) \in \mathbb{Z}^3$, $x^p + y^p + z^p \equiv 0\ [q] \Longrightarrow x, y$ ou $z \equiv 0\ [q]$;

(ii) $\forall x \in \mathbb{Z}$, $\quad x^p \not\equiv p\ [q]$.

Alors, si $x^p + y^p + z^p = 0$, x, y ou z est divisible par p.

Soit p un entier tel que dans le théorème de Sophie Germain. Soit x, y, z premiers entre eux tels que $x^p + y^p + z^p = 0$. On suppose que ni x, ni y, ni z ne sont divisibles par p.

1. Montrer que $y + z$ et $\displaystyle\sum_{k=0}^{p-1} (-1)^k y^{p-1-k} z^k$ sont premiers entre eux.

Indication : on pourra étudier la divisibilité simultanée par un entier premier r quelconque, et contredire soit le fait que x n'est pas divisible par p si $r = p$, soit le fait que y et z sont premiers entre eux si $r \neq p$.

2. Montrer qu'il existe des entiers a, b, c, a', b', c' tels que :

$$y + z = a^p \qquad \sum_{k=0}^{p-1} (-1)^k y^{p-1-k} z^k = a'^p \qquad x = -aa'$$

$$z + x = b^p \qquad \sum_{k=0}^{p-1} (-1)^k z^{p-1-k} x^k = b'^p \qquad y = -bb'$$

$$x + y = c^p \qquad \sum_{k=0}^{p-1} (-1)^k x^{p-1-k} y^k = c'^p \qquad z = -cc'$$

3. Justifier qu'on peut supposer que $x \equiv 0\ [q]$, et que dans ce cas, $a \equiv 0\ [q]$ (considérer $(-a)^p + b^p + c^p$).
4. En déduire l'existence de c'' tel que $(a'c'')^p \equiv p\ [q]$ et conclure.
5. Soit p un nombre premier impair. Montrer que si $2p+1$ est un nombre premier, les conditions (i) et (ii) du théorème de Sophie Germain sont satisfaites avec $q = 2p+1$.

Les nombres premiers p tels que $2p+1$ est aussi premier sont appelés nombres premiers de Sophie Germain. Un nombre premier sûr est un nombre premier $2p+1$ tel que p soit un nombre premier. Ainsi, tous les nombres premiers de Sophie Germain sont associés à des nombres premiers sûrs, et réciproquement. Un nombre premier peut être simultanément sûr et de Sophie Germain. C'est le cas par exemple de 5, 11 ou 23. D'ailleurs, ces nombres de suivent : 11 est à la fois sûr associé à 5 et de Sophie Germain associé à 23. On voit qu'on peut donc contruire des séquences finies $(p_1, \cdots, p_n)$ de nombres premiers tels que pour tout $i \in [\![1, n]\!]$, $p_{i+1} = 2p_i + 1$. Ainsi, les p_i sont tous de Sophie Germain, sauf éventuellement p_n, et tous sûrs, sauf éventuellement p_1. Un telle séquence est appelée chaîne de Cunningham. Par exemple $(2, 5, 11, 23, 47)$ est une chaîne de Cunningham.
On conjecture qu'il y a une infinité de nombres premiers de Sophie Germain, mais à l'heure actuelle, cette conjecture n'est pas démontrée.

Problème 2 – Polynômes irréductibles sur $\mathbb{F}_p$.
Soit p un nombre premier, et soit $n \in \mathbb{N}^*$ un entier fixé. On note pour tout $k \in \mathbb{N}^*$, $A(k)$ l'ensemble des polynômes irréductibles unitaires de degré k de $\mathbb{F}_p[X]$, et $I(k) = \mathrm{Card}(A(k))$. Le but de l'exercice est de donner une formule pour le calcul de $I(n)$.

1. Soit d un diviseur de n et $P \in A(d)$.
   (a) On définit la relation de congruence modulo P sur $\mathbb{F}_p[X]$ par $Q_1 \equiv Q_2\ [P]$ si et seulement si $Q_1 - Q_2$ est divisible par P. Montrer que la relation de congruence est une relation d'équivalence.
   (b) Soit $\mathbb{K}$ le quotient de $\mathbb{F}_p[X]$ par la relation de congruence modulo P. Montrer que la somme et le produit de $\mathbb{F}_p[X]$ passent au quotient, et que $\mathbb{K}$ muni de ces lois est un corps fini.

   On note $\chi \in \mathbb{K}$ la classe d'équivalence du monôme X de $\mathbb{F}_p[X]$, et on identifie les éléments de $\mathbb{F}_p$ aux classes d'équivalence des polynômes constants. Ainsi, on peut considérer que $\mathbb{F}_p \subset \mathbb{K}$, et en particulier, tout polynôme de $\mathbb{F}_p[X]$ peut être vu comme un polynôme de $\mathbb{K}[X]$.

   (c) Montrer que P admet une racine dans $\mathbb{K}$, en tant que polynôme de $\mathbb{K}[X]$ (on donnera explicitement une racine de P).
   (d) Montrer que $\mathbb{K}$ est un espace vectoriel de dimension d sur $\mathbb{F}_p$, puis que
   $$\mathrm{Card}(\mathbb{K}) = p^d.$$
2. Montrer que pour tout $x \in \mathbb{K}$, $x^{p^d} = x$. En considérant $P \wedge (X^{p^n} - X)$, en déduire que P divise $X^{p^n} - X$.
3. Nous établissons la réciproque :
   (a) Montrer qu'il existe un corps $\mathbb{K}'$ contenant $\mathbb{F}_p$ tel que $X^{p^n} - X$ soit scindé sur $\mathbb{K}'$. Justifier que ses racines sont toutes simples.
   (b) Soit $\mathbb{F}_{p^n}$ le sous-ensemble de $\mathbb{K}'$ constitué des racines de $X^{p^n} - X$. Montrer que $\mathbb{F}_{p^n}$ est un corps fini dont on précisera le cardinal, et que $\mathbb{F}_p \subset \mathbb{F}_{p^n}$.
   (c) Soit P un facteur irréductible sur $\mathbb{F}_p$ de $X^{p^n} - X$, et $\mathbb{K}$ et χ comme dans la question 1. Montrer que l'identification de χ à une racine x de P dans $\mathbb{F}_{p^n}$ permet de considérer $\mathbb{K}$ comme sous-corps de $\mathbb{F}_{p^n}$.
   (d) En déduire que $d \mid n$.
4. Déduire des questions précédentes que :
   $$\sum_{d|n} dI(d) = p^n \qquad \text{puis:} \qquad I(n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d,$$
   où μ est la fonction de Möbius, définie sur $\mathbb{N}^*$ par :
   $$\mu(n) = \begin{cases} 0 & \text{si } n \text{ admet dans sa décomposition un facteur premier de valuation au moins 2} \\ (-1)^k & \text{sinon,} \end{cases}$$
   où k est le nombre de facteurs premiers distincts dans la décomposition primaire de n.