Devoir Surveillé n° 8 (4h)

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

Question préliminaire

Soit n une entier positif, et a et b positifs tels que $ab = n^r$. Pour tout $p \in \mathbb{P}$, $v_p(n^r) = rv_p(n)$, et est divisible par r. Par ailleurs, $v_p(a) + v_p(b) = v_p(n^r)$, et $v_p(a)$ et $v_p(b)$ ne peuvent pas être non nuls simultanément. Ainsi, l'un est nul et l'autre est égal à $v_p(n^r)$.
Si r est impair, on obtient la même propriété sur $\mathbb{Z}$: le signe éventuel de n peut être transféré à a ou b en multipliant par $(-1)^r$, donc à k ou ℓ par multiplication par -1.
En revanche, la situation n'est plus aussi simple si r est pair. En effet, n^r étant positif, étant donnée une décomposition $ab = n^r$, a et b ont même signe. Quitte à changer le signe des deux, on trouvera alors des décompositions avec $a < 0$ et $b < 0$. Dans ce cas, r étant pair, il sera impossible de trouver k et ℓ tels que $k^r = a$ et $\ell^r = b$.

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

1. **Un lemme arithmétique**

   On pose $q = \frac{n}{d}$, avec $n, d \in \mathbb{Z}^*$, $n \wedge d = 1$ et $d > 0$. On a alors $\frac{an}{d} \in \mathbb{Z}$, et $\frac{bn}{d} \in \mathbb{Z}$, donc d divise an et bn. Comme d et n sont premiers entre eux, le lemme de Gauss nous permet alors d'affirmer que d divise a et b. Comme a et b sont premiers entre eux, $d = 1$. Ainsi, $q = n$, donc $\boxed{q \text{ est entier.}}$

2. **Triplets pythagoriciens.**

   (a)
   - Supposons (a, b, c) primitif. On a alors $a \wedge b = 1$, donc aussi $a \wedge b \wedge c = 1$. Ainsi, a, b, c sont premiers entre eux dans leur ensemble.
   - Supposons a, b, c premiers entre eux dans leur ensemble. Soit p un diviseur premier commun de a et b. Comme $a^2 + b^2 = c^2$, p divise aussi c^2, donc, d'après le lemme d'Euclide, p divise c. Les entiers a, b et c étant supposés premiers entre eux dans leur ensemble, ceci n'est pas possible. Ainsi, a et b n'admettent pas de diviseur premier commun, donc $a \wedge b = 1$. Le raisonnement est le même pour montrer que $a \wedge c = 1$ (la seule différence est le signe entre les carrés : $c^2 - a^2 = b^2$, mais ce signe n'intervient pas dans le raisonnement), et que $b \wedge c = 1$.
   - Si a, b et c sont premiers entre eux deux à deux, par définition, a et b sont premiers entre eux.

   On a donc $\boxed{\text{l'équivalence entre les 3 propriétés.}}$

   (b) On suppose que (a, b, c) est un triplet pythagoricien primitif.
   - a et b sont tous les deux pairs, car le triplet est primitif.
   - Si a et b sont tous les deux impairs, alors $a^2 + b^2$ est pair, donc c est pair. Ainsi, c^2 est divisible par 4. Or on a $a^2 \equiv 1$ [4] (écrire $a = 2k + 1$ et développer le carré !), et $b^2 \equiv 1$ [4], donc $a^2 + b^2 = c^2 \equiv 2$ [4]. D'où une contradiction.
   - Ainsi, $\boxed{a \text{ et } b \text{ sont de parité opposée}}$, disons a impair b pair (ce qui n'est pas restrictif par symétrie), et par conséquent c^2 est impair, donc $\boxed{c \text{ est impair.}}$

   (c) Soit p et q deux entiers premiers entre eux, de parité différente, tels que $p > q$.
   - Pour commencer, vérifions la relation de Pythagore :

   $$(2pq)^2 + (p^2 - q^2)^2 = 4p^2q^2 + p^4 + q^4 - 2p^2q^2 = (p^2 + q^2)^2.$$

   - Pour montrer que le triplet est primitif, il faut montrer que deux quelconques des 3 entiers sont premiers entre eux. Or, si r est un entier premier divisant $p^2 + q^2$ et $p^2 - q^2$, il divise leur somme et leur différence,

donc $2p^2$ et $2q^2$. Comme p et q sont de parité différente, p^2+q^2 est impair, donc $r \neq 2$. D'après le lemme d'Euclide, r divise donc p et q, ce qui n'est pas possible. Ainsi, p^2+q^2 et p^2-q^2 sont premiers entre eux, donc le triplet est primitif.

Ainsi, p et q étant premiers entre eux, $\boxed{(2pq, p^2-q^2, p^2+q^2) \text{ est un triplet pythagoricien primitif.}}$

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

i. Supposons $(a,b,c) = (2pq, p^2-q^2, p^2+q^2)$. On a donc

$$\frac{p}{q} = \frac{a}{2q^2} \qquad \text{donc:} \qquad \boxed{\frac{p}{q} = \frac{a}{c-b}}.$$

On définit donc les entiers positifs p et q comme définissant l'unique représentation irréductible à coefficients positifs du rationnel positif $\frac{a}{c-b}$. La positivité de ce rationnel vient du fait que la relation $a^2+b^2=c^2$ et la non nullité des a, b et c impliquent que $c-b>0$.

ii. Si p et q sont définis ainsi, pour commencer, p et q sont premiers entre eux. Par ailleurs,

$$\frac{p^2-q^2}{p^2+q^2} = \frac{\left(\frac{p}{q}\right)^2 - 1}{\left(\frac{p}{q}\right)^2 + 1} = \frac{a^2-(c-b)^2}{a^2+(c-b)^2} = \frac{a^2-b^2-c^2+2bc}{a^2+b^2+c^2-2bc} = \frac{-2b^2+2bc}{2c^2-2bc} = \frac{b(-2b+2c)}{c(2c-2b)} = \frac{b}{c}$$

Ainsi, la représentation $\frac{b}{c}$ étant irréductible, il existe un entier α tel que

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

iii. Par ailleurs, par définition, p et q sont premiers entre eux, donc aussi p^2 et q^2. De même que ci-dessus, ceci implique que les entiers impairs p^2-q^2 et p^2+q^2 sont premiers entre eux. On en déduit que $\boxed{\alpha = 1}$.
On a donc $p^2+q^2=c$, $p^2-q^2=b$, et

$$a^2 = c^2-b^2 = (p^2+q^2)-(p^2-q^2) = 4p^2q^2,$$

donc par positivité, $2pq=a$.

On a bien obtenue $\boxed{\text{une représentation comme en 2(c), avec } p \text{ et } q \text{ premiers entre eux.}}$

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) Soit un triplet pythagoricien quelconque (a,b,c). Supposons que l'aire du triangle associé soit un carré. Notons donc d^2 cette aire. On a donc $ab=2d^2$. Soit p un entier premier divisant simultanément a, b et c. Les entiers $a'=\frac{a}{p}, b'=\frac{b}{p}, c'=\frac{c}{p}$ forment encore un triplet pythagoricien et $2d^2 = p^2a'b'$. Quitte à simplifier par un facteur 2 dans le cas où $p=2$, on obtient dans tous les cas $p \mid d^2$, donc, d'après le lemme d'Euclide, p divise d. Ainsi, en posant $d'=\frac{d}{p}$, on a $\boxed{a'b' = 2d'^2.}$

On a donc obtenu un triplet pythagocien primitif dont l'aire du triangle associé est un carré.

Ainsi, si on parvient à montrer qu'aucune aire de triangle pythagoricien primitif n'est un carré, ce ne pourra pas non plus être le cas pour les triangles pythagoriciens quelconques.

(b) L'aire du triangle pythagoricien est $\frac{1}{2}ab = \boxed{pq(p^2-q^2)}$.

(c) L'entier $pq(p-q)(p+q)$ est un carré. Or, soit r un entier premier divisant pq. Alors, p et q étant premiers entre eux, r divise p ou r divise q, mais pas l'autre. Ainsi, r ne divise ni $p-q$ ni $p+q$. Comme r est premier, d'après Euclide, r ne divise pas $(p-q)(p+q)$. Ainsi, pq et $(p-q)(p+q)$ sont premiers entre eux, et leur produit est un carré. La question préliminaire est alors utilisable du fait que tous les facteurs sont positifs : pq et $(p-q)(p+q)$ sont des carrés. On applique une deuxième fois la question préliminaire pour obtenir le fait que $\boxed{p \text{ et } q \text{ sont des carrés, ainsi que } p-q \text{ et } p+q}$ (qui sont bien premiers entre eux, d'après un raisonnement déjà effectué).

Notons $p=x^2$, $q=y^2$, $p-q=v^2$ et $p+q=u^2$.

(d)
- Soit r un entier premier divisant $u+v$ et $u-v$. Alors r divise $2u$ et $2v$ (somme et différence). Si $r \neq 2$, r divise u et v (Euclide), donc r divise $p-q$ et $p+q$ qui sont premiers entre eux ; d'où une contradiction. Ainsi, le seul diviseur premier possible commun à $u+v$ et $u-v$ est 2.
- Puisque p et q sont de parité différente, $p-q$ et $p+q$ sont impairs, donc u et v sont impairs. On en déduit que $u+v$ et $u-v$ sont pairs. Ainsi, 2 est bien un diviseur commun.
- Par ailleurs, v étant impair, on a $2v \equiv 2[4]$, donc $(u+v)-(u-v) \equiv 2[4]$. Ainsi, $u+v$ et $u-v$ ne peuvent pas être tous deux divisibles par 4.
- En conclusion, $\boxed{(u+v) \wedge (u-v) = 2.}$

(e) On a $(u+v)(u-v) = u^2 - v^2 = 2p = 2x^2$. La question précédente montre que 4 divise $(u+v)(u-v)$ (et même 8), donc 2 divise x^2, puis x. Écrivons $x' = \frac{x}{2}$. On a alors :

$$(u+v)(u-v) = 8x'^2.$$

Par ailleurs, plaçons-nous dans le cas où $u-v$ est divisible par 4 et $u+v$ seulement par 2 (une des deux possibilités découlant de l'étude faite dans la question précédente ; la seconde s'étudie de façon similaire). On a alors

$$\frac{u-v}{4} \cdot \frac{u+v}{2} = x'^2.$$

Comme $(u+v) \wedge (u-v) = 2$, les entiers $\frac{u+v}{2}$ et $\frac{u-v}{2}$ sont premiers entre eux, donc aussi $\frac{u+v}{2}$ et $\frac{u-v}{4}$. On déduit alors de la question préliminaire que $\boxed{\frac{u+v}{2} \text{ et } \frac{u-v}{4} \text{ sont des carrés,}}$ les entiers $u+v$ et $u-v$ étant positifs (après échange des valeurs de u et v dans l'énoncé)

On obtient les dénomiateurs inversés dans l'autre cas. On suppose qu'on est dans le premier cas, et on note $r^2 = \frac{u+v}{2}$ et $s^2 = \frac{u-v}{4}$.

(f) On obtient alors :

$$(r^2)^2 + (2s^2)^2 = r^4 + 4s^4 = \frac{1}{4}\left((u+v)^2 + (u-v)^2\right) = \frac{1}{2}(u^2+v^2) = \frac{1}{2}((p-q)+(p+q)) = \frac{1}{2}p = x^2.$$

Ainsi, $\boxed{(r^2, 2s^2, x) \text{ est un triplet pythagoricien}}$

Comme r et s sont premiers entre eux, il en est de même de r^2 et s^2. Comme de plus, r est impair, r^2 et $2s^2$ sont aussi premiers entre eux. Ainsi, le triplet ci-dessus est **primitif**.

Son aire est $r^2s^2 = (rs)^2$, c'est donc un carré.

Par ailleurs, le paramètre x vérifie $x \leqslant x^2 \leqslant p \leqslant p^2 < p^2 + q^2$, donc le troisième paramètre du triplet décroît strictement, tout en restant entier positif. Le principe de descente infini nous dit donc que cette situation est impossible.

Ainsi, pour tout triplet pythagoricien primitif dont l'aire du triangle associé est un carré, on en a construit un autre vérifiant la même propriété, et dont la troisième composante est entière, positive, strictement plus petite.

Ainsi, $\boxed{\text{l'aire d'un triangle pythagoricien ne peut pas être un carré.}}$

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

(a) Étant donnée une solution $x^4 + y^4 = z^4$, on peut diviser par le pgcd des entiers x, y et z. On obtient alors une solution primitive non triviale, dans le même sens que pour les triplets pythagoriciens. On montre de même qu'avant que dans ce cas, x, y et z sont premiers entre eux dans leur ensemble si et seulement si x et y sont premiers entre eux. Ainsi, l'existence d'une solution implique l'existence d'une solution primitive. On peut donc se contenter de montrer qu'il n'existe pas de solution primitive.

De plus, étant donnée une solution primitive (x, y, z), x et y n'étant alors pas tous deux divisibles par 2, l'un au moins est impair, disons y. Si x est impair aussi, on a alors $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$, donc aussi $x^4 \equiv y^4 \equiv 1\ [4]$. Ainsi, $x^4 + y^4 \equiv 2\ [4]$, ce qui n'est pas possible (si z est impair, z^4 aussi, et si z est pair, z^4 est divisible par 2^4, donc par 4). Ainsi, x est pair.

Il suffit de montrer $\boxed{\text{qu'il n'existe pas de solution primitive avec } x \text{ pair.}}$

(b) Soit (x, y, z) une solution primitive, vérifiant donc $x^4 + y^4 = z^4$. On a alors

$$x^4 = z^4 - y^4 = (z^2 - y^2)(z^2 + y^2).$$

Puisque z et y sont impairs, on est dans la même situation que précédemment avec u et v : l'un de ces termes est divisible par 2 mais pas par 4, l'autre étant divisible par 4 au moins. Or, z^2 et y^2 étant tous deux congrus à 1 modulo 4, $z^2 - y^2$ est divisible par 4, et $z^2 + y^2$ est divisible par 2 mais pas par 4.
Par ailleurs, $v_2(x^4)$ étant un multiple de 4, on en déduit que $v_p(z^2 - y^2)$ est au moins 3 : $z^2 - y^2$ est divisible par 8. On a alors :

$$\frac{z^2 - y^2}{8} \cdot \frac{z^2 + y^2}{2} = \left(\frac{x}{2}\right)^4.$$

Par ailleurs, le même raisonnement que pour u et v montre que les entiers $\frac{z^2-y^2}{8}$ et $\frac{z^2+y^2}{2}$ sont premiers entre eux. Comme ils sont positifs, la question préliminaire permet alors de conclure qu'ils sont les puissances quatrièmes d'entiers positifs a et b : il existe a et b entiers tels que

$$\boxed{z^2 - y^2 = 8a^4} \qquad \text{et} \qquad \boxed{z^2 + y^2 = 2b^4}.$$

(c) On a alors $(2a^2)^2 + (b^2)^2 = z^2$, donc $(2a^2, b^2, z)$ est un triplet pythagoricien, l'aire du triangle associé étant $a^2b^2 = (ab)^2$, ce qui contredit la question précédente.
Ainsi, $\boxed{\text{l'équation } x^4 + y^4 = z^4 \text{ n'admet pas de solution dans } (\mathbb{N}^*)^3.}$

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 $j = \mathrm{e}^{\mathrm{i}\frac{2\pi}{2}}$. 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) Ceci est un argument important, valable aussi pour passer du pgcd de deux polynômes sur un corps $\mathbb{K}$, au pgcd sur un corps plus gros $\mathbb{K}'$: d'après le théorème de Bezout, il existe des entiers u et v tels que

$$up + vq = 1.$$

Cette relation peut aussi être vue comme une relation de Bézout dans $\mathbb{Z}[j]$, donc p et q sont premiers entre eux dans $\mathbb{Z}[j]$.
De façon plus formelle,

$$1 \in p\mathbb{Z} + q\mathbb{Z} \subset p\mathbb{Z}[j] + q\mathbb{Z}[j],$$

et un idéal contenant 1 étant l'anneau tout entier, on a

$$p\mathbb{Z}[j] + q\mathbb{Z}[j] = \mathbb{Z}[j].$$

Étant donné r un entier d'Eisentein divisant p et q, on a alors (les idéaux étant pris dans $\mathbb{Z}[j]$) :

$$(p) \subset (r) \qquad \text{et} \qquad (q) \subset (r), \qquad \text{donc:} \qquad (p) + (q) \subset (r) \qquad \text{donc:} \qquad (r) = \mathbb{Z}[j].$$

Ceci équivaut à $r \in \mathbb{U}_6$ (i.e. r est une unité de $\mathbb{Z}[j]$), donc p et q n'ont pas de diviseurs communs autre que les unités.
Ainsi, $\boxed{p \text{ et } q \text{ sont premiers entre eux dans } \mathbb{Z}[j]}$.

(b) On a $j = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}$, donc $\mathrm{i}\sqrt{3} = 2j + 1 \in \mathbb{Z}[j]$. Ainsi, pour tous entiers x et y, $x + \mathrm{i}y\sqrt{3} \in \mathbb{Z}[j]$.
En particulier,

$$p + \mathrm{i}\sqrt{3}q = p + (2j+1)q \qquad \text{et} \qquad p - \mathrm{i}\sqrt{3}q = p - (2j+1)q.$$

Soit r un diviseur premier commun de $p - \mathrm{i}\sqrt{3}q$ et $p + \mathrm{i}\sqrt{3}q$ (au sens d'Eisenstein). L'entier premier d'Eisenstein r divise alors $2p$ et $2\,\mathrm{i}\sqrt{3}q$.

Montrons dans un premier temps que 2 est un entier premier au sens d'Eisenstein. On utilise la norme $N(z) = |z|^2$. On vérifie sans peine (on l'a déjà fait dans un DM ou un DS) que N est à valeurs dans $\mathbb{N}$ et est multiplicative. Si 2 se décompose de façon non triviale (c'est-à-dire sans unité) sous la forme $2 = z_1 z_2$, on a alors $4 = N(z_1)N(z_2)$. De plus, z_1 et z_2 ne sont pas des unités, donc $N(z_1)$ et $N(z_2)$ sont strictement supérieurs à 1. Ainsi, $N(z_1) = N(z_2) = 2$. Cherchons les éléments de z de norme 2. Soit $z = a + bj$, avec a et b entiers. On a $N(z) = a^2 + b^2 - ab = 2$. Obtenons une contradiction sur la parité :

- Si a et b sont de parité opposée, $a^2 + b^2 - ab$ est impair d'où une contradiction.
- Si a et b sont tous deux impairs, $a^2 + b^2 - ab$ est impair aussi ;
- a et b ne peuvent pas être tous deux pairs, car sinon, 2 divise z donc $4 \leqslant N(2) \leqslant N(z) = 2$.

Ainsi, il n'existe pas d'éléments de $\mathbb{Z}[j]$ de norme 2, donc $\boxed{\text{2 est premier d'Eisenstein.}}$
Nous avons obtenu $r \mid 2p$, et 2 est premier d'Eisenstein. Donc $r = 2$ ou r divise p.
Si $r = 2$, 2 divise $p + \mathrm{i}\sqrt{3}q = p + (2j+1)q = p + q + 2jq$. On peut donc trouver u et v tels que

$$p + q + 2jq = 2a + 2bj.$$

Or, la décomposition d'un complexe sous la forme $a + bj$ est unique (se ramener à une identification des parties réelles et imaginaires), donc $2b = 2q$ et $2a = p + q$. La deuxième égalité nous indique que p et q sont de même parité, et comme ils sont premiers entre eux, ils sont impairs. En écrivant $p = 2k+1$ et $q = 2\ell+1$, il vient $p^2 + 3q^2 = 4k(k+1) + 12\ell(\ell+1) + 4$. Puisque $k(k+1)$ est pair, on obtient donc :

$$p^2 + 3q^2 \equiv 4[8],$$

donc $p^2 + 3q^2$ est divisible par 4 mais pas par 8. Or, puisqu'il s'agit d'un cube, les valuations p-adiques doivent être multiples de 3, d'où une contradiction.
Ainsi, $r \neq 2$.
On en déduit que r divise p. D'un autre côté, r divise $2q\,\mathrm{i}\sqrt{3}$, et $r \neq 2$. Comme $\mathrm{i}\sqrt{3}$ est premier, de même, on en déduit que $r = \mathrm{i}\sqrt{3}$ ou r divise q.
Supposons donc que $r = \mathrm{i}\sqrt{3} = 2j+1$. On a alors $\mathrm{i}\sqrt{3} \mid p + \mathrm{i}\sqrt{3}$ et $\mathrm{i}\sqrt{3} \mid p - \mathrm{i}\sqrt{3}$ et, donc 3 divise le produit $p^2 + 3q^2$, donc 3 divise p^2, donc p. Ainsi, comme p et q sont premiers entre eux (donc q non divisible par 3) $p^2 + 3q^2 \not\equiv 0$ [9], ce qui n'est pas possible, puisque 3 divise s^3, donc s, donc 9 (et même 27) divise $p^2 = 3p^2$.
Ainsi, $r \neq \mathrm{i}\sqrt{3}$. Il en résulte que r divise q, ce qui contredit le fait que p et q sont premiers entre eux.
Par conséquent, $\boxed{p - \mathrm{i}q\sqrt{3} \text{ et } p + \mathrm{i}q\sqrt{3} \text{ sont premiers entre eux.}}$

(c) On utilise alors la question préliminaire, adaptable dans $\mathbb{Z}[j]$ (mais il faut faire attention aux unités : le résultat donné n'est vrai qu'à unité près, problème qu'on avait souligné dans le cas d'une puissance impaire, dans $\mathbb{Z}$) : les entiers d'Eisenstein $(p - \mathrm{i}\sqrt{3}\cdot q)$ et $(p + \mathrm{i}\sqrt{3}\cdot q)$ étant premiers entre eux, et leur produit valant $p^2 + 3q^2 = s^3$, la question préliminaire donne l'existence d'un élément $\alpha + \beta j$ et d'une unité x tels que $x(\alpha + \beta j)^3 = p + \mathrm{i}\sqrt{3}\cdot q$. On a alors aussi :

$$p + \mathrm{i}\sqrt{3}\cdot q = x(\alpha j + \beta j^2)^3 = x(-\beta + (\alpha - \beta)j)^2,$$

ainsi que

$$p + \mathrm{i}\sqrt{3}\cdot q = x(\alpha j^2 + \beta)^3 = x(\beta - \alpha - \alpha j)^2.$$

Or des entiers β, $\alpha - \beta$ et $-\alpha$ (coefficients de j dans cette écriture), l'un au moins est pair, et l'entier d'Eisenstein correspondant sera alors dans $\mathbb{Z}[\mathrm{i}\sqrt{3}]$. Ainsi, il existe des éléments u et v de $\mathbb{Z}$ tels que $p + \mathrm{i}\sqrt{3}\cdot q = x(u + \mathrm{i}v\sqrt{3})^3$. Il reste donc à montrer que $x = \pm 1$.
Notons $(u + \mathrm{i}v\sqrt{3})^3 = u' + \mathrm{i}v'\sqrt{3}$. On suppose que $x = j = \frac{1}{2}(-1 + \mathrm{i}\sqrt{3})$. On a alors

$$x(u + \mathrm{i}v\sqrt{3})^3 = \frac{1}{2}\left((-u' - 3v') + \mathrm{i}\sqrt{3}(-v' + u')\right)$$

Par ailleurs, en développant et en identifiant parties réelles et imaginaires, on a :

$$u' = u^3 - 9uv^2 = u(u-3v)(u+3v) \qquad \text{et} \qquad v' = 3u^2v - 3v^3 = 3v(u-v)(u+v).$$

- Si u' est impair, alors u, $u-3v$ et $u+3v$ sont impairs, donc u est impair et v est pair. On en déduit que v' est pair. Ainsi, $-u'-3v'$ et $-v'+u'$ sont impairs, donc $x(u+\mathrm{i}\,v\sqrt{3})^3 \notin \mathbb{Z}[\mathrm{i}\sqrt{3}]$;
- De même, si v' est impair, alors v est impair et u pair, donc u' est pair, et on conclut de même.

Ces deux cas amenant une contradiction, on en déduit que u' et v' sont pairs. Mais dans ce cas, $p+\mathrm{i}\sqrt{3}q$ est divisible par 2 dans $\mathbb{Z}[j]$. On a même mieux que cela. En effet, u' et v' étant pairs, supposons que u et v ne soient pas tous les deux pairs. Dans ce cas, u ne peut pas être pair, car alors v est impair ainsi que $u-v$ et $u+v$, ce qui contredit la parité de v'. De même v ne peut pas être pair. Ainsi u et v sont impairs. Chaque facteur $u+v$, $u-v$, $u+3v$ et $u-3v$ est divisible par 2, donc u' et v' sont divisibles par 4.

Ainsi, $p+\mathrm{i}\,q\sqrt{3}$ est divisible par 4 dans $\mathbb{Z}[j]$. Il existe donc a et b tels que

$$p+\mathrm{i}\,q\sqrt{3} = 4(a+bj) = 4(a-\frac{b}{2}(-1+\mathrm{i}\sqrt{3})).$$

L'identification des parties réelles et imaginaires montre alors que 2 divise p et q, ce qui contredit le fait qu'ils sont premiers entre eux.

Ainsi, l'unité x ne peut pas être égale à j.

On montre par le même principe (il n'y a que certains signes qui changent) que x ne peut pas être égal à j^2, à $j+1$ ou à j^2+1. Ainsi, $x=1$ ou -1, et quitte à changer le signe de u et v si $x=-1$, on peut supposer que $x=1$.

Il existe donc des entiers u et v tels que

$$\boxed{p+\mathrm{i}\,q\sqrt{3} = (u+\mathrm{i}\,v\sqrt{3})^3}$$

Au passage, on a donc $u'=p$ et $v'=q$, donc on a déjà établi les relations

$$\boxed{p = u^3-9uv^2} \qquad \text{et} \qquad \boxed{q = 3u^2v-3v^3}.$$

(d) Les deux relations précédentes montrent que $p \in (u)+(v)$ et $q \in (u)+(v)$, donc $(p) \subset (u)+(v)$ et $(q) \subset (u)+(v)$, d'où $(p)+(q) \subset (u)+(v)$. Or, p et q sont premiers entre eux, donc $(p)+(q)=\mathbb{Z}$, d'où $(u)+(v)=\mathbb{Z}$.

On en déduit que $\boxed{u \text{ et } v \text{ sont premiers entre eux.}}$

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) Comme précédemment, si une solution existe, en divisant par le pgcd global de x, y et z, on trouve une solution constituée d'entiers x, y et z premiers entre eux dans leur ensemble. Le même raisonnement que pour les triplets pythagoriciens montre qu'alors x, y et z sont premiers entre eux deux à deux.

En particulier, au moins deux des trois entiers x, y et z sont impairs. Comme les entiers considérés sont relatifs, quitte à changer leur signe pour les passer de part et d'autre de l'égalité, on peut supposer que $\boxed{x \text{ et } y \text{ sont impairs (et donc } z \text{ pair)}}$.

(b) On pose $p=\frac{x+y}{2}$ et $q=\frac{x-y}{2}$. Comme x et y sont impairs, p et q sont entiers, et $p+q=x$, $p-q=y$.

On a alors :

$$z^3 = (p+q)^3+(p-q)^3 = 2p^3+6pq^2 = 8\frac{p}{4}(p^2+3q^2).$$

On a bien la relation $\boxed{\left(\frac{z}{2}\right)^3 = \frac{p}{4}(p^2+3q^2).}$

(c) Puisque x et y sont impairs, p et q ne peuvent pas être de même parité. Ainsi, p^2 et $3q^2$ ne sont pas de même parité, donc $\boxed{p^2+3p^2 \text{ est impair.}}$

(d) Puisque z est pair, $\left(\frac{z}{2}\right)^3$ est entier, donc 4 divise $p(p^2+3q^2)$. Comme de plus, 4 est premier avec p^2+3q^2 d'après la question précédente, on en déduit que $\boxed{4 \text{ divise } p}$. Ainsi, $\boxed{p \text{ est pair et } q \text{ est impair.}}$

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

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

(a) Pour commencer, justifions que p et q sont premiers entre eux. Si k est un entier premier divisant p et q, comme p et q n'ont pas même parité, $k \neq 2$, et k divise $p+q$ et $p-q$ donc x et y, ce qui contredit que x et y sont premiers entre eux.

Montrons ensuite que $\frac{p}{4}$ et p^2+3q^2 sont premiers entre eux. Supposons qu'il existe un diviseur premier commun k. L'entier k divise alors p, et donc p^2, puis $3q^2$. Si $k=3$, 3 diviserait $\left(\frac{z}{2}\right)^3$, donc z, ce qui n'est pas le cas. Donc k est premier avec 3, donc divise q^2, puis q. Cela contredit le fait que p et q sont premiers entre eux.

Ainsi, $\boxed{\frac{p}{4} \text{ et } p^2+3q^2 \text{ sont premiers entre eux.}}$

Le produit de ces entiers est un cube : on utilise alors la question préliminaire pour conclure que chacun d'eux est un cube (il n'y a ici pas de problème d'unité : on est dans $\mathbb{Z}$ avec un exposant impair) : il existe des entiers r et s tels que $\boxed{\frac{p}{4} = r^3 \text{ et } p^2+3q^2 = s^3.}$

(b) La question 1(c) nous donne alors l'existence d'entiers u et v tels que $p+\mathrm{i}\sqrt{3}\cdot q = (u+\mathrm{i}\sqrt{3}\cdot v)^3$, et u et v premiers entre eux. Par ailleurs,

$$p = u^3 - 9uv^2 = u(u^2-9v^2) = \boxed{u(u+3v)(u-3v)} \qquad \text{et} \qquad q = 3vu^2 - 3uv^2 = \boxed{3v(u^2-v^2)}$$

(c) On a justifié ci-dessus que p est pair et q est impair. L'imparité de q et son expression en fonction de u et v nous assure que u et v ne peuvent pas être de la même parité et que v est impair. Ainsi, $\boxed{u \text{ est pair, et } v \text{ impair.}}$

(d) L'expression de p en fonction de u et v, et la divisibilité de p par 4, ainsi que l'imparité de $u-3v$ et $u+3v$ permet d'affirmer que u est divisible par 4. On considère alors :

$$r^3 = \frac{p}{4} = \frac{u}{4}(u+3v)(u-3v).$$

Comme précédemment, z étant non divisible par 3, on montre que $\frac{u}{4}$, $u+3v$ et $u-3v$ sont deux à deux premiers entre eux, donc d'après la question préliminaire, ils s'écrivent chacun comme un cube : il existe a, b et c des entiers tels que $\boxed{\frac{u}{4} = a^3,\ u+3v = b^3 \text{ et } u-3v = c^3}$

On a alors $\boxed{b^3+c^3 = (2a)^3}$, d'où une autre solution de l'équation de Fermat, b et c étant premiers entre eux (puisque $u-3v$ et $u+3v$ le sont).

(e)

$$|2abc|^3 = 2|u(u+3v)(u-3v)| = 2|p| < 2(p^2+3q^2) \leqslant |z|^3 \leqslant |xyz|^3.$$

Ainsi, on peut contruire une suite infinie de solutions $x^3+y^3=z^3$ tel que l'entier strictement positif $|xyz|^3$ soit strictement décroissant. Pour pouvoir utiliser le principe de descente infinie, il faut soit justifier que la solution vérifie toujours l'hypothèse de non divisibilité par 3, soit terminer d'abord la descente dans le second cas.

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

On rappelle que $\left(\frac{z}{2}\right)^3 = \frac{p}{4}(p^2+3q^2)$. Supposons que 3 ne divise pas p. Alors puisque 3 divise z, 3 divise p^2+3q^2 d'après le lemme d'Euclide, donc 3 divise p^2, et le lemme d'Euclide nous dit qu'alors 3 divise p, ce qui amène une contradiction. Ainsi, 3 divise p. Par ailleurs, 3 ne divise pas q (car p et q sont premiers entre eux). Ainsi, $3\left(\frac{p}{3}\right)^2+q^2$ est premier avec 3. Or, comme 3^3 divise $\frac{p}{4}(p^2+3q^2)$), on en déduit que 9 divise $\frac{p}{4}$, donc $\frac{p}{36}$ est un entier. On peut alors écrire :

$$\left(\frac{z}{6}\right)^3 = \frac{p}{36}\left(3\left(\frac{p}{3}\right)^2+q^2\right).$$

Soit r un diviseur premier de $\frac{p}{36}$. C'est donc un diviseur de p, donc pas de q (p et q étant premiers entre eux)

- Si $r \neq 3$, r divise $3\left(\frac{p}{3}\right)^2$ mais pas q^2, donc r ne divise pas $\left(3\left(\frac{p}{3}\right)^2+q^2\right)$.
- L'argument reste valable si $r=3$, du fait du facteur 3 devant le terme $\left(\frac{p}{3}\right)^2$.

Ainsi, r n'est pas un diviseur de $\left(3\left(\frac{p}{3}\right)^2+q^2\right)$. Cette conclusion étant vraie pour tout diviseur premier de $\frac{p}{36}$, on en déduit que $\frac{p}{36}$ et $\left(3\left(\frac{p}{3}\right)^2+q^2\right)$ sont premiers entre eux. Leur produit étant un cube, nous pouvons utiliser la question préliminaire pour en déduire que $\left(3\left(\frac{p}{3}\right)^2+q^2\right)$ est un cube, ainsi que $\frac{p}{36}$. Il existe alors, d'après II-1, des entiers u et v premiers entre eux tels que

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

On a de plus :

$$q=u^3-9uv^2=u(u+3v)(u-3v) \qquad \text{et} \qquad \frac{p}{3}=3u^2v-3v^3=3v(u^2-v^2),$$

et u et v sont premiers entre eux. En particulier, u et v n'ont pas même parité, donc u^2-v^2 est impair. Comme p est pair, v est nécessairement pair, et u est donc impair (u et v étant premiers entre eux).
Puisque 4 divise p et $u+v$ et $u-v$ sont impairs, l'expression de $\frac{p}{3}$ montre que 4 divise v. Ainsi, on a :

$$\frac{p}{36}=\frac{v}{4}(u+v)(u-v),$$

les trois termes étant entiers. De plus, la même preuve que précédemment montre que ces trois entiers sont premiers entre eux deux à deux. La question préliminaire permet de conclure que ce sont des cubes. Notons

$$a^3=\frac{v}{4}, \qquad b^3=u+v \qquad \text{et} \qquad c^3=u-v.$$

On a comme avant $(2a)^3=b^3-c^3=b^3+(-c)^3$, les trois termes $2a$, b et c étant premiers entre eux. De plus,

$$|2abc|^3=\frac{1}{2}|v(u+v)(u-v)|=\frac{p}{18}<\frac{|z|^3}{2^3}<|xyz|^3$$

Ainsi, dans les deux cas, on a construit, à partir d'une solution de l'équation, une autre solution, de sorte à avoir stricte décroissance de l'entier positif $|xyz|$.
D'après le principe de descente infinie, il n'existe pas de solution entère non triviale de l'équation $x^3+y^3=z^3$.

Partie III – Le théorème de Sophie Germain

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. Soit r un nombre premier divisant simultanément $y+z$ et $\sum_{k=0}^{p-1} y^{p-1-k}z^k$. Montrons d'abord que $r\neq p$. En effet,

$$(y+z)\sum_{k=0}^{p-1}(-1)^k y^{p-1-k}z^k=y^p+z^p=-x^p,$$

donc r divise x^p, donc x (d'après le lemme d'Euclide). Comme x n'est pas divisible par p, $r\neq p$.
Par ailleurs $y\equiv -z \mod [r]$, puis

$$0\equiv\sum_{k=0}^{p-1}(-1)^k y^{p-1-k}z^k\equiv\sum_{k=0}^{p-1}(-1)^k(-z)^{p-1-k}z^k=p(-1)^{p-1}z^{p-1}\ [r].$$

Comme $r\neq p$, et r premier, p est inversible modulo r, donc $z^{p-1}\equiv 0\ [r]$, puis $y\equiv 0\ [r]$. Ceci contredit le fait que y et z sont premiers entre eux.
Ainsi, il n'existe par de diviseur premier commun à $y+z$ et $\sum_{k=0}^{p-1}(-1)^k y^{p-1-k}z^k$, donc ces nombres sont premiers entre eux.

2. Comme on vient de le voir,

$$(y+z)\left(\sum_{k=0}^{p-1}(-1)^k y^{p-1-k}z^k\right)=-x^p=(-x)^p.$$

Ainsi, la question précédente et la question préliminaire permettent d'obtenir l'existence d'entiers a et a' tels que

$$\boxed{y+z=a^p} \qquad \text{et} \qquad \boxed{\sum_{k=0}^{p-1}(-1)^k y^{p-1-k}z^k = a'^p.}$$

De plus, $(aa')^p = (-x)^p$. Comme p est impair, $x \mapsto x^p$ est une bijection de $\mathbb{R}$ dans $\mathbb{R}$, donc $\boxed{aa' = -x}$

Les rôles de x, y et z étant symétriques, on obtient de même, par permutation des variables :

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

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

3. Du fait de la symétrie des hypothèses en x, y et z, et d'après la propriété (i), (l'égalité $x^P + y^p + z^p = 0$ nous autorise à l'utiliser), on peut supposer que $x \equiv 0\ [p]$. On a alors

$$(-a)^p + b^p + c^p \equiv -(y+z) + (x+y) + (x+z) \equiv 2x \equiv 0\ [q].$$

D'après la propriété (i), on a alors a, b ou c multiple de q. Mais comme x, y et z sont deux à deux premiers entre eux et $q \mid x$, q ne divise pas $x+y$, ni $x+z$. Donc q ne divise pas b^p ni c^p, donc q ne divise ni b ni c. On en déduit que $\boxed{a \equiv 0\ [q].}$

4. On a donc $b^p + c^P \equiv 0\ [q]$, donc $2x + y + z \equiv 0[q]$, donc $z \equiv -y[q]$. En remplaçant dans l'expression de $(a')^p$, on obtient :

$$(a')^p \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \equiv py^p y'\ [q],$$

où y' est un représentant de l'inverse modulo q de y (l'inversibilité étant assurée par le fait que q ne divise pas y et est premier). On a donc :

$$\boxed{p \equiv (a'y')^p y \equiv (a'y'c)^p\ [p]},$$

la dernière congruence étant assurée pas le fait que $c^p \equiv x + y \equiv y\ [q]$.

Cela entre en contradiction avec le point (ii). Ainsi, l'hypothèse faite en début de raisonnement est fausse. On en conclut que $\boxed{x,\ y \text{ ou } z \text{ est divisible par } p.}$

5. Soit p un nombre impair tel que $q = 2p+1$ soit aussi un nombre premier.

   (i) Supposons que x, y et z vérifient $x^p + y^p + z^p \equiv 0[q]$. Supposons que x, y et z ne soit pas divisibles par q. On sait alors, par le petit théorème de Fermat, que $x^{q-1} \equiv 1 \mod [q]$, donc $x^{2p} \equiv 1[q]$. L'équation $y^2 = 1$ n'ayant que les deux solutions 1 et -1 dans le corps $\mathbb{F}_q$, on en déduit que $x^p \equiv \pm 1\ [q]$. Il en est de même pour y^p et z^p. Ainsi,

   $$x^p + y^p + z^p \equiv -3, -1, 1, 3\ [q].$$

   Aucune de ces possibilités n'est compatible avec l'hypothèse $x^p + y^p + z^p \equiv 0\ [q]$, puisque $q = 2p+1 \geqslant 5$. Ainsi, $\boxed{x,\ y \text{ ou } z \text{ est divisible par } q.}$

   (ii) Soit x dans $\mathbb{Z}$. Si $x \equiv 0[q]$, $x^p \equiv 0 \not\equiv p\ [q]$, et si $x \not\equiv 0[q]$, l'argument précédent montre que $x^p \equiv \pm 1 \not\equiv p\ [q]$. Dans tous les cas, $\boxed{x^p \not\equiv p\ [p].}$

   Ainsi, $\boxed{\text{les nombres de Sophie Germain vérifient les hypothèses du théorème.}}$

Correction du 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 $I(k) = \text{Card}(A(k))$. 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) La relation de congruence est clairement reflexive, symétrique, et transitive (la propriété de divisibilité étant stable par somme). Ainsi, $\boxed{\text{la congruence modulo } P \text{ est une relation d'équivalence.}}$

(b) On montre que la relation de congruence est compatible avec + et × de $\mathbb{F}_p[X]$. Soient Q_1, Q_2, R_1, R_2 tels que $Q_1 \equiv Q_2\ [P]$ et $R_1 \equiv R_2 \mod P$.

- On a :
$$(Q_2 + R_2) - (Q_1 + R_1) = (Q_2 - Q_1) + (R_2 - R_1),$$
et, P divisant $Q_2 - Q_1$ et $R_2 - R_1$, P divise aussi $(Q_2 + R_2) - (Q_1 + R_1)$. Ainsi, $Q_1 + R_1 \equiv Q_2 + R_2\ [P]$.
- De même,
$$Q_2R_2 - Q_1R_1 = Q_2(R_2 - R_1) + R_1(Q_2 - Q_1),$$
donc P divise $Q_2R_2 - Q_1R_1$, puis $Q_1R_1 \equiv Q_2R_2\ [P]$.

Ainsi, les lois + et × passent au quotient, définissant deux lois, qu'on notera de la même façon, sur l'espace quotient $\mathbb{K}$. Les propriétés liées à la structure d'anneau de $\mathbb{F}_p[X]$ restent vérifiées par passage au quotient, ainsi, $\mathbb{K}$ est muni d'une structure d'anneau commutatif. Il reste à vérifier que tout élément non nul est inversible.

Soit donc $h \in \mathbb{K}$, non nul, représenté par un polynôme H de $\mathbb{F}_p[X]$. Comme P est irréductible et unitaire, $H \wedge P = 1$ ou $H \wedge P = P$. Puisque $h \neq 0$, H n'est pas divisible par P, donc $H \wedge P = 1$. D'après le théorème de Bézout, il existe donc deux polynômes U et V tels que
$$HU + PV = 1.$$
En notant u la classe d'équivalence de U modulo P, il vient donc, par passage au quotient, la relation suivante dans $\mathbb{K}$:
$$h \cdot u = 1_{\mathbb{K}}.$$
Nous avons bien montré que tout élément non nul de l'anneau commutatif $\mathbb{K}$ est inversible, $\mathbb{K}$ est un corps.

Par ailleurs, d'après le théorème de la division euclidienne, $h \in \mathbb{K}$ admet un représentant dans $\mathbb{F}_p[X]$ de degré au plus $d-1$. Il y a un nombre fini de polynômes de degré au plus $d-1$ (plus exactement p^d, puisque chacun des n coefficients peut prendre p valeurs différentes). Ainsi $\boxed{\mathbb{K} \text{ est un corps fini.}}$

(c) χ étant la classe de X, les lois de $\mathbb{K}$ étant obtenues de celles de $\mathbb{F}_p[X]$ par passage au quotient, $P(\chi)$ est la classe de $P(X)$, c'est-à-dire 0. Ainsi, $P(\chi) = 0_{\mathbb{K}}$, donc $\boxed{P \text{ admet au moins la racine } \chi \text{ dans } \mathbb{K}}$.

(d)
- Puisque $\mathbb{K}$ est un corps, $(\mathbb{K}, +)$ est un groupe abélien.
- Puisque $\mathbb{F}_p$ est un sous-corps de $\mathbb{K}$, la restriction du produit de $\mathbb{K}$ à $\mathbb{F}_p \times \mathbb{K}$ défini une loi de composition interne. La structure de corps de $\mathbb{K}$ nous assure alors que celle loi est distributive sur la somme de $\mathbb{K}$, ainsi que sur la somme de $\mathbb{F}_p$, qu'elle respecte le neutre de $\mathbb{F}_p$ (qui est aussi le neutre de $\mathbb{K}$), et qu'elle vérifie la propriété d'associativité externe, obtenue par restriction de l'associativité de × dans $\mathbb{K}$.

Ainsi, $\boxed{\mathbb{K} \text{ est un espace vectoriel sur } \mathbb{F}_p}$.

Comme on l'a dit plus haut, tout élément de $\mathbb{K}$ admet un représentant de degré au plus $d-1$. Ainsi, $(1, \chi, \ldots, \chi^{d-1})$ est une famille génératrice de $\mathbb{K}$ en tant que $\mathbb{F}_p$-ev. Par ailleurs, le seul polynôme de degré au plus $d-1$ divisible par P de degré d est le polynôme nul. On en déduit sans peine la liberté de la famille $(1, \chi, \ldots, \chi^{d-1})$. Il s'agit donc d'une base, de cardinal d.

Ainsi, $\boxed{\mathbb{K} \text{ est un espace vectoriel de dimension } d \text{ sur } \mathbb{F}_p}$.

Tout vecteur étant alors déterminé de façon unique par le choix de d coordonnées dans $\mathbb{F}_p$ (après choix d'une base), $\boxed{\text{Card}(\mathbb{K}) = p^d}$ (cela se formalise en disant que $\mathbb{K}$ est alors isomorphe à $\mathbb{F}_p^d$).

2. $(\mathbb{K}^*, \times)$ est un groupe de cardinal $p^d - 1$. Donc, d'après le théorème de Lagrange, pour tout $x \in \mathbb{K}^*$, $x^{p^d-1} = 1$, donc $x^{p^d} = x$. Cette relation étant trivialement vraie pour $x = 0$ aussi, il vient :
$$\forall x \in \mathbb{K}, \quad \boxed{x^{p^d} = x}.$$
Vous aurez reconnu une généralisation du petit théorème de Fermat.

En notant $d_1 = \frac{n}{d}$, on obtient alors $\chi^{p^n} = (((\chi^{p^d})^{p^d}) \cdots)^{p^d} = \chi$, obtenu en élevant d_1 fois à la puissance p^d. Ainsi, χ est racine commune de P et $X^{p^n} - X$, donc que $P \wedge X^{p^n} - X \neq 1$. Or, les polynômes P et $X^{p^n} - X$ étant à coefficients dans $\mathbb{F}_p$, l'algorithme d'Euclide pour le calcul du PGCD permet d'affirmer que $P \wedge X^{p^n} - X$ est aussi à coefficients dans $\mathbb{F}_p$. Comme il divise P (dans $\mathbb{F}_p[X]$), et est différent de 1, l'irréductibilité de P amène $P \wedge X^{p^n} - X = P$, donc $\boxed{P \text{ divise } X^{p^d} - X}$.

3. Nous établissons la réciproque :

   (a) On itère l'argument de la question 1 : à chaque étape, si $P = X^{p^n} - 1$ n'est pas scindé dans le corps $\mathbb{K}$ construit, on en considère un facteur irréductible Q de degré au moins 2, et on construit un corps $\mathbb{K}'$ de la même manière que dans la question 1, contenant $\mathbb{K}$ comme sous-corps, et dans lequel Q aura une racine. Dans ce corps $\mathbb{K}'$, le polynôme P a au moins une racine de plus que dans $\mathbb{K}$. On itère ce procédé jusqu'à ce que P soit scindé. On est assuré de la terminaison de cet algorithme du fait que P, dans n'importe quel sur-corps de $\mathbb{F}_p$ ne pourra jamais avoir plus de p^n racines. Le nombre de racines augmentant strictement à chaque étape, il y aura au maximum p^n étapes.

   Ainsi, $\boxed{\text{il existe un corps } \mathbb{K}' \text{ contenant } \mathbb{F}_p, \text{ tel que } X^{p^n} - X \text{ soit scindé sur } \mathbb{K}'.}$

   Ce procédé permet toujours de construire un « corps de décomposition » d'un polynôme P (corps dans lequel il sera scindé). La première étape donne un « corps de rupture » (corps dans lequel P admet une racine au moins)

   Puisque $\mathbb{K}'$ contient $\mathbb{F}_p$, $\mathbb{K}'$ est de caractéristique p. Ainsi, $P' = p^n X^{p^n-1} - 1 = -1 \neq 0$. Donc une racine de P ne peut pas être racine de P', ce qui assure que $\boxed{\text{les racines de } P \text{ sont simples.}}$

   (b)
   - $0 \in \mathbb{F}_{p^n}$
   - Pour tout $(\omega_1, \omega_2) \in \mathbb{F}_{p^n}$,
   $$(\omega_1 - \omega_2)^{p^n} = \omega_1^{p^n} - \omega_2^{p^n} = \omega_1 - \omega_2,$$
   car dans un corps de caractéristique p, $(x+y)^p = x^p + y^p$, et, en distinguant les cas p pair et p impair, on obtient facilement $(x-y)^p = x^p - y^p$, puis, par itération, $(x-y)^{p^n} = x^{p^n} - y^{p^n}$. Ainsi, $\omega_1 - \omega_2 \in \mathbb{F}_{p^n}$.
   - Pour tout $(\omega_1, \omega_2) \in \mathbb{F}_{p^n}$,
   $$(\omega_1 \omega_2^{-1})^{p^n} = (\omega_1^{p^n})(\omega_2^{p^n})^{-1} = \omega_1 \omega_2^{-1}.$$
   Donc $\omega_1 \omega_2^{-1} \in \mathbb{F}_{p^n}$.

   On en déduit que $\boxed{\mathbb{F}_{p^n} \text{ est un sous-corps de } \mathbb{K}'}$.

   Puisque pour tout $x \in \mathbb{F}_p$, on a $x^p = x$, on a, par itération, $x^{p^n} = x$, d'où $x \in \mathbb{F}_{p^n}$. Ainsi, $\boxed{\mathbb{F}_p \subset \mathbb{F}_{p^n}}$.

   Enfin, les racines de $X^{p^n} - X$ étant toutes simples, et ce polynôme étant scindé sur $\mathbb{K}'$, elles sont au nombre de p^n, donc $\boxed{\text{Card}(\mathbb{F}_{p^n}) = p^n.}$

   (c) P admet une racine x dans $\mathbb{F}_{p^n}$. Considérons $\varphi : \mathbb{F}_p[X] \mapsto \mathbb{F}_{p^n}$, le morphisme d'anneaux, bien et uniquement défini par $\varphi(k) = k$ si $k \in \mathbb{F}_p$ et $\varphi(X) = x$. Si Q est divisible par P, disons $Q = PR$, on a alors $\varphi(Q) = P(x)R(x) = 0$. Ainsi, φ passe au quotient, définissant un morphisme d'anneaux $\tilde{\varphi}$ de $\mathbb{K}$ vers $\mathbb{F}_{p^n}$, tel que $\tilde{\varphi}(\chi) = x$. C'est alors un morphisme de corps (par définition), et, comme tout morphisme de corps, il est injectif. En effet si $P \neq 0$, $\tilde{\varphi}(y) = 0$ implique

   $$\tilde{\varphi}(1) = \tilde{\varphi}(y)\tilde{\varphi}(y^{-1}) = 0,$$

   ce qui contredit $\tilde{\varphi}(1) = 1$. Ainsi, $\text{Ker}(\tilde{\varphi}) = \{0\}$, d'où l'injectivité.

   Par conséquent, $\tilde{\varphi}$ induit un isomophisme de corps de $\mathbb{K}$ sur son image dans $\mathbb{F}_{p^n}$. En identifiant le corps $\mathbb{K}$ à son image, $\boxed{\text{on peut donc considérer } \mathbb{K} \text{ comme sous-corps de } \mathbb{F}_{p^n}}$.

   (d) Comme dans 1(d), $\mathbb{F}_{p^n}$ est alors un espace vectoriel sur $\mathbb{K}$, de dimension finie. Comme $\mathbb{K}$ est de cardinal p^k, il existe donc un entier $k = \dim_{\mathbb{K}}(\mathbb{F}_{p^n})$ tel que

   $$p^n = (p^d)^k = p^{kd}, \qquad \text{donc:} \qquad n = kd.$$

   On en déduit que $\boxed{d \mid n.}$

4. Tout polynôme irréductible de degré $d \mid n$ divise $X^{p^n} - 1$ (question 2), et ceci une seule fois car les racines de ce dernier sont simples. Récirproquement, tout facteur irréductible de $X^{p^n} - 1$ est de degré $d \mid n$. Ainsi,

   $$X^{p^n} - 1 = \prod_{d|n} \prod_{P \in A(d)} P.$$

   En identifiant les degrés, il vient alors :

   $$p^n = \sum_{d|n} \sum_{P \in A(d)} d = \sum_{d|n} dI(d).$$

On obtient la dernière identité par la formule d'inversion de Möbius, qu'on redémontre rapidement dans ce cas particulier :

$$\begin{aligned}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d &= \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\sum_{d'|d}d'I(d')\\ &= \frac{1}{n}\sum_{d'|n}d'I(d')\sum_{d,d'|d}\mu\left(\frac{n}{d}\right).\end{aligned}$$

Le changement de variable $d'' = \frac{n}{d}$ dans la seconde somme amène

$$\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d = \frac{1}{n}\sum_{d'|n}d'I(d')\sum_{d''|\frac{n}{d'}}\mu\left(d''\right).$$

Or, étant donné $k \in [\![2, n]\!]$, de décomposition $p_1^{\alpha_1}, \ldots, p_\ell^{\alpha_\ell}$,

$$\sum_{d|k}\mu(d) = \sum_{(\varepsilon_1,\ldots,\varepsilon_k)\in\{0,1\}^\ell}(-1)^{\varepsilon_1+\cdots+\varepsilon_k} = \left(\sum_{\varepsilon_1=0}^{1}(-1)^{\varepsilon_1}\right)\cdots\left(\sum_{\varepsilon_\ell=0}^{1}(-1)^{\varepsilon_\ell}\right) = 0.$$

Pour $k = 1$, on obtient en revanche $\sum_{d|k}\mu(d) = \mu(1) = (-1)^0 = 1$ Ainsi, reprenant le calcul précédent, la plupart des termes sont nuls, et il reste :

$$\boxed{\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d = I(n).}$$