

EXERCICES MPSI 2010

TANCRÈDE LEPOINT

Table des matières

1 Géométrie dans le plan	2
Corrigés	2
2 Espaces Euclidiens	3
Corrigés	4
3 Arithmétique	8
Corrigés	9
Petit théorème de Fermat	15
Exercices d'applications	16
Corrigés	16

1 Géométrie dans le plan

ENONCÉS

Exercice 1 : (*Mines-Ponts*) Soient trois points A , B et C dans le plan \mathbb{R}^2 . On note I le milieu de $[B, C]$. Montrer que

$$\|\vec{AB}\|^2 + \|\vec{AC}\|^2 = 2\|\vec{AI}\|^2 + \frac{1}{2}\|\vec{BC}\|^2.$$

en se servant de l'identité du parallélogramme.

Exercice 2 : (*Point de Gergonne – simplifié X*) Soit ABC un triangle de cercle circonscrit Γ . Les tangentes à Γ en A et B se coupent en C' . On définit de même A' et B' . Montrer que les droites (AA') , (BB') et (CC') sont concourantes en J défini par :

$$\frac{1}{\alpha}\vec{JA'} + \frac{1}{\beta}\vec{JB'} + \frac{1}{\gamma}\vec{JC'} = \vec{0}$$

avec

$$\alpha = A'B = A'C, \quad \beta = B'C = B'A, \quad \gamma = C'A = C'B.$$

On pourra raisonner en termes de barycentres partiels.

Exercice 3 : (*Partage équitable – X*) On considère 1000 points dans le plan \mathbb{R}^2 . Montrer qu'il existe une droite ayant, au sens strict, 500 points d'un côté et 500 points de l'autre.

Exercice 4 : (*CNS pour être équilatère – X, ENS*) Soit $(a, b, c) \in \mathbb{C}^3$. Montrer l'équivalence des propositions suivantes :

- i) le triangle (a, b, c) est équilatéral
- ii) $a^2 + b^2 + c^2 = ab + bc + ca$

CORRIGÉS

Correction de l'exercice 1 : On rappelle que l'identité du parallélogramme est

$$\forall (x, y) \in \mathbb{R}^2 \times \mathbb{R}^2, 2(\|x\|^2 + \|y\|^2) = \|x + y\|^2 + \|x - y\|^2$$

On applique cette formule avec $x = \vec{AB}$ et $y = \vec{AC}$. On obtient

$$2(\|\vec{AB}\|^2 + \|\vec{AC}\|^2) = \|\vec{AB} + \vec{AC}\|^2 + \|\vec{AB} - \vec{AC}\|^2.$$

Comme I est le milieu de $[B, C]$, on a $\vec{AB} + \vec{AC} = 2\vec{AI}$, et $\vec{AB} - \vec{AC} = \vec{CB}$, d'où l'égalité recherchée.

Correction de l'exercice 2 : Comme $A \in [B'C']$, on a :

$$\frac{\vec{AB'}}{\vec{AC'}} = -\frac{\beta}{\gamma}, \quad \beta, \gamma > 0$$

D'où $\frac{1}{\beta}\vec{AB'} + \frac{1}{\gamma}\vec{AC'} = \vec{0}$. A est le barycentre de $(B', \frac{1}{\beta})(C', \frac{1}{\gamma})$. De même, B est le barycentre de $(A', \frac{1}{\alpha})(C', \frac{1}{\gamma})$ et C celui de $(A', \frac{1}{\alpha})(B', \frac{1}{\beta})$.

Soit J le barycentre de $(A', \frac{1}{\alpha})(B', \frac{1}{\beta})(C', \frac{1}{\gamma})$. Par associativité du barycentre, on a J barycentre de $(A', \frac{1}{\alpha})(A, \frac{1}{\beta} + \frac{1}{\gamma})$, de $(B', \frac{1}{\beta})(B, \frac{1}{\alpha} + \frac{1}{\gamma})$ et $(C', \frac{1}{\gamma})(C, \frac{1}{\alpha} + \frac{1}{\beta})$, donc HJ point de concours des droites (AA') , (BB') et (CC') .

Correction de l'exercice 3 :

- *Méthode 1 :* On munit le plan \mathbb{R}^2 de sa structure euclidienne et on note $(A_i)_{1 \leq i \leq 1000}$ les points. Les vecteurs unitaires $\frac{\overrightarrow{A_i A_j}}{\|A_i A_j\|}$, $i \neq j$, sont en nombre fini et le cercle unité du plan est infini. On choisit un vecteur unitaire u qui n'est pas parmi l'ensemble précédent et on considère un repère $R = (O, u, v)$. Les ordonnées y_i des points a_i dans ce repère sont deux à deux distinctes. On peut renuméroter les points pour avoir $y_1 < y_2 < \dots < y_{1000}$. Il suffit alors de choisir un réel $\alpha \in]y_{500}, y_{501}[$ et de prendre la droite d'équation $y = \alpha$ dans le repère R .
- *Méthode 2 :* Soit \mathcal{D} la réunion de toutes les droites passant par deux des 1000 points et soit \mathcal{C} le bord d'un disque qui contient tous les 1000 points dans son intérieur. On prend une tangente au cercle \mathcal{C} non parallèle à une droite de \mathcal{D} . Tous les points se trouvent d'un côté. Puis on fait tourner cette tangente autour de son point de contact (elle devient sécante) ; elle va balayer les points un par un, et on s'arrête lorsqu'on a passé 500 points.

Correction de l'exercice 4 : Si (a, b, c) est équilatéral, c'est équivalent au fait que par la rotation $r(a, \frac{\pi}{3})$ de centre a et de rayon $\frac{\pi}{3}$, on ait soit $b \mapsto c$ ou bien $c \mapsto b$. Or, r s'écrit $r(a, \frac{\pi}{3}) : z \in \mathbb{C} \mapsto a + e^{i\frac{\pi}{3}}(z - a)$.

Une condition nécessaire est suffisante est donc que $c = a + e^{i\frac{\pi}{3}}(b - a)$ ou $b = a + e^{i\frac{\pi}{3}}(c - a)$, i.e. que le produit $(c - a - e^{i\frac{\pi}{3}}(b - a))(b - a - e^{i\frac{\pi}{3}}(c - a)) = 0$. Quand on le développe, on trouve la seconde proposition, et comme on a raisonné par équivalence, ceci conclut la preuve.

2 Espaces Euclidiens

ENONCÉS

Exercice 5 : Montrer que, pour tout $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$:

$$(x_1 + x_2 + \dots + x_n)^2 \leq n(x_1^2 + x_2^2 + \dots + x_n^2).$$

Dans quel cas a-t-on égalité ?

Exercice 6 : (*Intersection et orthogonal*) Soient F et G deux sous-espaces vectoriels d'un espace euclidien E . Montrer que :

$$(F + G)^\perp = F^\perp \cap G^\perp, \quad (F \cap G)^\perp = F^\perp + G^\perp$$

Exercice 7 : Soient E un espace euclidien ainsi que f et g deux endomorphismes de E qui commutent. On suppose que les matrices de f et de g dans une base orthonormale sont respectivement symétrique et antisymétrique. Montrer que :

$$\forall x \in E, \langle f(x), g(x) \rangle = 0$$

puis que :

$$\forall x \in E, \|(f - g)(x)\| = \|(f + g)(x)\|$$

Exercice 8 : (Dimension de $\mathcal{C}([0, 1], \mathbb{R})$ – Centrale) Soit $E = \mathcal{C}([0, 1], \mathbb{R})$. Pour tout $(f, g) \in E^2$, on pose

$$\langle f, g \rangle = \int_0^1 f(t)g(t)dt.$$

1. Prouver que $\langle \cdot, \cdot \rangle$ est un produit scalaire sur E .
2. On pose $F = \{f \in E \mid f(0) = 0\}$.
 - (a) Soit $f \in F^\perp$. Montrer que $f^2 \in F^\perp$.
 - (b) Prouver que $F^\perp = \{0\}$.
 - (c) E est-il de dimension finie ?

Exercice 9 : (Rotation comme produit de symétries orthogonales) Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien orienté de dimension 3.

1. Rappeler la définition de $SO(E)$.
2. La boule unité de E est notée $B = \{a \in E \mid \langle a, a \rangle = 1\}$. Pour $a \in B$, s_a désigne la symétrie orthogonale par rapport à la droite $\mathbb{R}a$.
 - (a) Pourquoi a-t-on $s_a \in SO(E)$?
 - (b) Soit $a \in B$. Pour tout $x \in E$, montrer que $s_a(x) = 2\langle x, a \rangle a - x$.
 - (c) Soit (a, a') une famille libre de vecteurs de B . Montrer que $s_{a'} \circ s_a$ est une rotation. Préciser son axe et son angle en fonction de l'angle formé par les vecteurs a et a' .
 - (d) Montrer que toute rotation peut s'écrire $s_a \circ s_b$ avec $(a, b) \in B^2$.

Exercice 10 : (Produit scalaire de $\mathbf{M}_n(\mathbb{R})$ – adapté X) On pose $\Phi: \mathbf{M}_n(\mathbb{R}) \times \mathbf{M}_n(\mathbb{R}) \rightarrow \mathbb{R}$.

$$(A, B) \mapsto \text{Tr}({}^tAB)$$

1. Montrer que Φ est un produit scalaire sur $\mathbf{M}_n(\mathbb{R})$.
2. Montrer que $\forall A \in \mathbf{M}_n(\mathbb{R}), |\text{Tr}(A)| \leq \sqrt{n}\sqrt{\Phi(A, A)}$.
3. Montrer que $\forall O \in O_n(\mathbb{R}), \forall A \in \mathbf{M}_n(\mathbb{R}), \Phi(OA, AO) = \Phi(OA, OA) = \Phi(A)$.

Exercice 11 : (Familles obtusangles – adapté X) Soit (u_1, \dots, u_p) une famille de vecteurs de \mathbb{R}^n vérifiant $\langle u_i, u_j \rangle < 0$ pour $i \neq j$.

1. Montrer que $p - 1$ vecteurs parmi eux forment toujours une famille libre de \mathbb{R}^n .
Indication : On pourra séparer les scalaires selon leurs signes.
2. Montrer que l'on ne peut trouver plus de $n + 1$ vecteurs réunissant ces conditions.

Remarque. En fait on peut en trouver $n + 1$. L'idée de la démonstration est de considérer une base orthonormée (e_1, \dots, e_n) de \mathbb{R}^n et de poser $u_{n+1} = -\sum_{i=1}^n e_i$. En faisant cela, on a $\langle e_i, u_{n+1} \rangle = -1$ et $\langle e_i, e_j \rangle = \delta_{i,j}$. On déforme alors un peu les vecteurs e_i en leur ajoutant un multiple de u_{n+1} suffisamment petit (qui ne va dépendre que de la dimension de l'espace, i.e. n)

CORRIGÉS

Correction de l'exercice 5 : Il suffit d'écrire l'inégalité de Cauchy-Schwarz dans \mathbb{R}^n muni de sa structure euclidienne canonique avec les vecteurs $u = (1, 1, \dots, 1)$ et $v = (x_1, x_2, \dots, x_n)$. Il y a égalité si et seulement si u et v sont colinéaires, i.e. v est de la forme $v = (\lambda, \lambda, \dots, \lambda)$ avec $\lambda \in \mathbb{R}$.

Correction de l'exercice 6 : Montrons ces égalités par doubles inclusions.

– $(F + G)^\perp \subset F^\perp \cap G^\perp$: Soit $z \in (F + G)^\perp$. Puisque, $\forall (f, g) \in F \times G$, on a

$$\langle z, f \rangle = 0, \quad \langle z, g \rangle = 0$$

(car $F \subset F + G$ et $G \subset F + G$), alors $z \in F^\perp \cap G^\perp$.

– $\underline{F^\perp \cap G^\perp \subset (F+G)^\perp}$: Soit $z \in F^\perp \cap G^\perp$. Soit $y \in F+G$. Il existe $f \in F$ et $g \in G$ tels que $y = f+g$.
On a donc :

$$\langle z, y \rangle = \langle z, f \rangle + \langle z, g \rangle = 0 + 0 = 0$$

– $\underline{F^\perp + G^\perp \subset (F \cap G)^\perp}$: Soit $z \in F^\perp + G^\perp$. Soit $h \in F \cap G$. Il existe $(f, g) \in F^\perp \times G^\perp$ tel que $z = f+g$.
On a donc :

$$\langle z, h \rangle = \langle f, h \rangle + \langle g, h \rangle = 0 + 0 = 0$$

– $\underline{(F \cap G)^\perp \subset F^\perp + G^\perp}$: On raisonne sur les dimensions des espaces. On rappelle que pour tout espace H inclus dans un espace euclidien de dimension n , on a

$$\dim(H^\perp) = n - \dim(H)$$

On obtient donc :

$$\begin{aligned} & \dim(F^\perp + G^\perp) \\ &= \dim(F^\perp) + \dim(G^\perp) - \dim(F^\perp \cap G^\perp) \\ &= (n - \dim F) + (n - \dim G) - \dim((F+G)^\perp) \\ &= 2n - \dim F - \dim G - (n - \dim(F+G)) \\ &= n - \dim(F \cap G) \\ &= \dim((F \cap G)^\perp) \end{aligned}$$

Correction de l'exercice 7 : On considère une base \mathcal{B} de E . Notons A et B les matrices respectives de f et de g dans \mathcal{B} . Soit $x \in E$ un vecteur ayant pour vecteur colonne X dans \mathcal{B} . On a :

$$\langle f(x), g(x) \rangle = {}^t(AX)BX = {}^tXABX$$

et

$$\langle g(x), f(x) \rangle = {}^t(BX)AX = -{}^tXBAAX = -{}^tXABX$$

Ainsi, $\langle f(x), g(x) \rangle = 0$. On applique ensuite le théorème de Pythagore et, pour tout $x \in E$:

$$\|f(x) + g(x)\|^2 = \|f(x)\|^2 + \|g(x)\|^2 = \|f(x) - g(x)\|^2$$

Correction de l'exercice 8 :

1. L'application $\langle \cdot, \cdot \rangle$ est bilinéaire du fait de la linéarité de l'intégrale. Elle est symétrique parce que le produit sur \mathbb{R} est commutatif. De plus, $\forall f \in E$, $\langle f, f \rangle = \int_0^1 f^2(t) dt \geq 0$: l'application $\langle \cdot, \cdot \rangle$ est positive. De plus, $\forall f \in E$,

$$\langle f, f \rangle = 0 \iff \int_0^1 f^2(t) dt = 0 \iff f^2 = 0 \iff f = 0$$

La forme bilinéaire $\langle \cdot, \cdot \rangle$ est alors définie.

2. (a) On a $\forall g \in F, \langle f, g \rangle = 0$. Or, $\forall g \in F, fg \in F$ donc

$$\forall g \in F, \langle f, fg \rangle = 0 = \langle f^2, g \rangle$$

et $f^2 \in F^\perp$.

(b) Notons $g: [0, 1] \rightarrow \mathbb{R}$ définie par $g(t) = t$ pour tout $t \in [0, 1]$. Clairement, $g \in F$. Soit $f \in F^\perp$. Par ce qui précède, $f^2 \in F^\perp$. Ainsi, $\langle f^2, g \rangle = 0$, c'est-à-dire $\int_0^1 t f^2(t) dt = 0$, d'où

$$\forall t \in [0, 1], t f^2(t) = 0$$

En particulier, on déduit que $\forall t \in]0, 1], f(t) = 0$ et comme f est continue, $f(0) = 0$ et $f \in F$. Ainsi, $f = 0$.

(c) En dimension finie, on a $F^\perp = \{0\}$ si et seulement si $F = E$, ce qui est évidemment faux!

Correction de l'exercice 9 :

1. $SO(E)$ est l'ensemble des éléments de $O(E)$ de déterminant +1. Les éléments de $SO(E)$ sont les rotations.

2. (a) $s_a \in SO(E)$ car s_a est une rotation d'angle π .

(b) Soit $x \in E$. Notons p la projection orthogonale sur $\mathbb{R}a$. On a donc

$$\forall x \in E, p(x) = \langle x, a \rangle a.$$

Comme $s = 2p - \text{id}_E$, on a le résultat voulu.

(c) (a, a') est une famille libre de vecteurs de B , donc a et a' engendrent un plan. Soit un vecteur b orthogonal à a dans ce plan. a' est une combinaison linéaire de a et b telle que $\langle a, a' \rangle = 1$. Il existe $\alpha \in \mathbb{R}$ tel que $a' = \cos(\alpha)a + \sin(\alpha)b$.

Complétons la famille (a, b) en une base orthonormée (a, b, c) de E . On va montrer que $s_{a'} \circ s_a$ est une rotation d'axe porté et dirigé par c et d'angle 2α .

– C'est une rotation car c'est une composée de deux rotations.

– $c \perp a$ et $c \perp a'$ donc c est transformé en $-c$ par s_a et par $s_{a'}$. Finalement, c est un vecteur fixe de $s_{a'} \circ s_a$.

– Soit la rotation $r = s_{a'} \circ s_a$ d'angle θ définie par $r(a) = \cos(\theta)a + \sin(\theta)b$. Comme $s_{a'}(x) = 2\langle x, a' \rangle a' - x$, on obtient

$$(s_{a'} \circ s_a)(a) = s_{a'}(a) = 2\langle a, a' \rangle a' - a$$

Comme a et b sont orthogonaux et $a' = \cos(\alpha)a + \sin(\alpha)b$, on en déduit que $\langle a, a' \rangle = \cos(\alpha)$. On en déduit donc que :

$$\begin{aligned} r(a) &= (s_{a'} \circ s_a)(a) \\ &= 2\cos(\alpha)a' - a \\ &= (2\cos(\alpha)^2 - 1)a + 2\cos(\alpha)\sin(\alpha)b \\ &= \cos(2\alpha)a + \sin(2\alpha)b \end{aligned}$$

d'où $\theta = 2\alpha$.

- (d) Soit r une rotation d'angle θ et d'axe $c \in E$. Soient a et b des vecteurs de E tels que (a, b, c) soit une base orthonormée. Posons $a' = \cos(\theta/2)a + \sin(\theta/2)b$. D'après ce qui précède, $r = s_{a'} \circ s_a$.

Correction de l'exercice 10 :

1. Φ est bilinéaire par linéarité du produit dans $\mathbf{M}_n(\mathbb{R})$ et de la trace. Soient A et B deux matrices de $\mathbf{M}_n(\mathbb{R})$.

$$\Phi(A, B) = \text{Tr}({}^tAB) = \text{Tr}({}^t({}^tAB)) = \text{Tr}({}^tBA) = \Phi(B, A)$$

Quand au caractère défini positif, il provient du fait que si $A = (a_{i,j})_{1 \leq i, j \leq n}$, alors

$$\Phi(A, A) = \sum_{1 \leq i, j \leq n} a_{i,j}^2$$

qui est strictement positif pour A non nulle.

2. On utilise l'inégalité de Cauchy-Schwarz pour Φ :

$$|\text{Tr}(A)| = |\text{Tr}(IA)| \leq \sqrt{\Phi(I, I)} \sqrt{\Phi(A, A)} = \sqrt{n} \sqrt{\Phi(A, A)}$$

3. Soient $O \in O_n(\mathbb{R})$ et $\forall A \in \mathbf{M}_n(\mathbb{R})$. On a, du fait que ${}^tOO = I_n$:

$$\Phi(OA, OA) = \text{Tr}({}^t(OA)OA) = \text{Tr}({}^tO{}^tAAO) = \text{Tr}({}^tAAO{}^tO) = \text{Tr}({}^tAA)$$

et

$$\Phi(OA, OA) = \text{Tr}({}^t(OA)OA) = \text{Tr}({}^tA{}^tOOA) = \text{Tr}({}^tAA).$$

Correction de l'exercice 11 :

1. Quitte à permuter les vecteurs, on peut se contenter de le montrer pour la famille (u_1, \dots, u_{p-1}) . Soit $(\lambda_1, \dots, \lambda_{p-1}) \in \mathbb{R}^{p-1}$ tel que $\sum_{i=1}^{p-1} \lambda_i u_i = 0$. On suit l'indication de l'énoncé et on va séparer selon le signe des scalaires. Notons $I_1 = \{i \in \llbracket 1, p-1 \rrbracket \mid \lambda_i > 0\}$ et $I_2 = \llbracket 1, p-1 \rrbracket \setminus I_1$. On a donc :

$$\sum_{i \in I_1} \lambda_i u_i = - \sum_{j \in I_2} \lambda_j u_j$$

D'où,

$$\begin{aligned} \left\| \sum_{i \in I_1} \lambda_i u_i \right\|^2 &= \left\langle \sum_{i \in I_1} \lambda_i u_i, - \sum_{j \in I_2} \lambda_j u_j \right\rangle \\ &= - \sum_{i \in I_1, j \in I_2} \lambda_i \lambda_j \underbrace{\langle u_i, u_j \rangle}_{< 0} \end{aligned}$$

D'où $0 \leq \left\| \sum_{i \in I_1} \lambda_i u_i \right\|^2 \leq 0$, donc $\sum_{i \in I_1} \lambda_i u_i = - \sum_{j \in I_2} \lambda_j u_j = 0$.

On multiplie scalairement par u_p et on obtient :

$$0 = \left\langle \sum_{i \in I_1} \lambda_i u_i, u_p \right\rangle = \sum_{i \in I_1} \lambda_i \underbrace{\langle u_i, u_p \rangle}_{< 0}$$

On en déduit donc que pour tout $i \in I_1$, $\lambda_i = 0$. On fait de même pour λ_j avec $j \in I_2$. La famille (u_1, \dots, u_{p-1}) est donc libre.

2. Si on trouve p vecteurs qui correspondent, $p - 1$ d'entre eux forment une famille libre, donc $p - 1 \leq n = \dim(\mathbb{R}^n)$, d'où $p \leq n + 1$. On ne peut trouver plus de $n + 1$ vecteurs vérifiant ces conditions.

3 Arithmétique

ENONCÉS

Exercice 12 : Montrer que $6 | n(n+1)(n+2)$ pour tout $n \in \mathbb{Z}$.

Exercice 13 : Montrer que $5 | (2^{3n+5} + 3^{n+1})$ pour tout $n \in \mathbb{N}$.

Exercice 14 : Quel est le reste de la division euclidienne de $16^{2^{1000}}$ par 7 ?

Exercice 15 : Trouver tous les $n \in \mathbb{Z}$ tels que $\sqrt{\frac{8n-18}{n+2}} \in \mathbb{N}$.

Exercice 16 : Montrer que si la somme de deux rationnels est entière, leurs représentants irréductibles ont même dénominateur.

Exercice 17 : Montrer que l'équation $x^4 + x + 1 = 0$, d'inconnue rationnelle x , n'a pas de solution.

Exercice 18 : Quel est le dernier chiffre de l'écriture en base 10 et $7^{(7^7)}$?

Exercice 19 : Soit p un entier naturel qui n'est divisible ni par 2 ni par 3. Montrer que $24 | p^2 - 1$.

Exercice 20 : (Nombres de Mersenne $M_n = 2^n - 1$) Dans cet exercice, nous allons rechercher les nombres premiers de la forme $a^n - 1$ où a et n sont des entiers supérieurs ou égaux à 2.

1. Par un raisonnement simple, montrer que a est nécessairement pair.
2. Enoncer la formule de la somme des séries géométriques, et en déduire que a est égal à 2.
3. Soit $n \in \mathbb{N}$. Montrer que si $2^n - 1$ est premier, alors n est nécessairement premier. On pourra raisonner par l'absurde.

Remarque. Bien entendu, la réciproque de ce résultat est fautive ! C'est en 1536 que Hudalricus Regius a trouvé le contre-exemple $2^{11} - 1 = 2047 = 23 \times 89$.

Exercice 21 : (Nombres parfaits) Un entier naturel n est dit *nombre parfait* s'il est égal à la somme de tous ses diviseurs positifs, en excluant n lui-même.

Montrer que si p un nombre premier tel que $2^p - 1$ est également premier, alors $2^p(2^p - 1)$ est un nombre parfait.

Remarque. Le résultat précédent est en fait la proposition 36 du livre IX des Éléments d'Euclide. Ce qui est vraiment intéressant, sans être difficile à montrer, c'est que réciproquement, tous les nombres parfaits pairs s'écrivent de cette façon. On ne sait toujours pas si il existe un nombre parfait impair, et s'il existe une infinité de nombres parfaits pairs.

Exercice 22 : (Racines rationnelles de $P \in \mathbb{Z}[X]$)

1. Soit $P \in \mathbb{Q}[X]$ tel que tous ses coefficients soient entiers, P non nul. Soit $x = a/b$ une racine rationnelle de P avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ premiers entre eux. En exprimant $P(x) = 0$, trouver des conditions sur a et b n'utilisant que les coefficients dominant et constant.
2. Application. Soit $P = 6X^4 - 7X^3 + 8X^2 - 7X + 2$. Trouver les racines rationnelles de P .

Exercice 23 : (Infinité de nombres premiers – TPE MP 2006) Montrer qu'il y a une infinité de nombres premiers de la forme $4k - 1$ avec $k \in \mathbb{N}^*$. On pourra s'inspirer fortement de la preuve de l'infinité des nombres premiers due à Euclide.

Exercice 24 : Soit un nombre rationnel positif p/q avec $p \in \mathbb{N}$, $q \in \mathbb{N}^*$ et p et q premiers entre eux. Montrer que l'équation

$$\frac{1}{x} + \frac{1}{y} = \frac{p}{q}$$

n'admet qu'un nombre fini d'entiers solutions.

Exercice 25 : On considère l'équation

$$N - 10 = x^3(3x + 1) = y^2(y + 1)^3$$

d'inconnues x et y des nombres entiers naturels premiers entre eux. Montrer qu'il n'y a qu'une valeur possible pour N et la trouver.

Exercice 26 : (Système de congruences) Résoudre le système de congruence :

$$(\mathcal{S}) : \begin{cases} x \equiv 5 \pmod{13} \\ x \equiv 4 \pmod{9} \end{cases}$$

Exercice 27 : (Système de congruences) Résoudre le système de congruence :

$$(\mathcal{S}) : \begin{cases} 7x \equiv 11 \pmod{13} \\ 11x \equiv 13 \pmod{7} \\ 13x \equiv 7 \pmod{11} \end{cases}$$

Exercice 28 : (Carrés commençant par 2010) Déterminer le plus petit entier qui est un carré et donc l'écriture en base 10 commence par 2010.

Exercice 29 : (CNS pour diviser une somme d'entiers) Un entier naturel $n \geq 3$ a la propriété \mathcal{P} s'il existe des entiers p et q tels que $0 < p < q < n$ et que la somme $p + (p + 1) + \dots + q$ est divisible par n . Montrer que n a la propriété \mathcal{P} si et seulement si n n'est pas une puissance de deux.

Exercice 30 : (Autour de Bezout – Gourdon)

1. Soient a et b deux entiers naturels plus grand que 2 premiers entre eux. Montrer qu'il existe un unique couple $(u_0, v_0) \in \mathbb{N}^2$ tel que $u_0 a - v_0 b = 1$ avec $u_0 < b$ et $v_0 < a$. Exprimer tous les couples $(u, v) \in \mathbb{N}^2$ solutions de l'équation $au - bv = 1$.
2. Trouver un couple $(u, v) \in \mathbb{N}^2$ tel que $47u + 111v = 1$.

Exercice 31 : (Gourdon) Soit A la somme des chiffres de 4444^{4444} (écrit dans le système décimal) et B la somme des chiffres de A . Que vaut C la somme des chiffres de B ?

On pourra raisonner modulo 9

CORRIGÉS

Correction de l'exercice 12 : Dans trois entiers consécutifs, il y en a divisible par 2 et un divisible par 3, et comme 2 et 3 sont premiers entre eux, $\forall n \in \mathbb{Z}, 6 \mid n(n + 1)(n + 2)$.

Correction de l'exercice 13 : Soit $n \in \mathbb{N}$. On a $2^5 \equiv 2 \pmod{5}$ et $2^{3n} \equiv 8^{3n} \equiv 3^n \pmod{5}$ donc $2^{3n+5} \equiv 2 \times 3^n \pmod{5}$. Ainsi, $2^{3n+5} + 3^{n+1} \equiv 2 \times 3^n + 3 \times 3^n \equiv 3^n \times 5 \equiv 0 \pmod{5}$.

Correction de l'exercice 14 : On a $16 \equiv 2 \pmod{7}$, donc $16^3 \equiv 8 \equiv 1 \pmod{7}$. On cherche donc à

combien est congru 2^{1000} modulo 3. On a $2^2 \equiv 1 \pmod{3}$, donc $2^{1000} \equiv 1 \pmod{3}$. Il existe $k \in \mathbb{Z}$ tel que $2^{1000} = 3k + 1$, donc $16^{2^{1000}} = 16^{3k+1} \equiv 16 \equiv 2 \pmod{7}$.

Correction de l'exercice 15 : Soit $n \in \mathbb{Z}$ tel que $\sqrt{\frac{8n-18}{n+2}} \in \mathbb{N}$. On a alors $n+2 \mid 8n-18$. Or, $8n-18 = 8(n+2) - 34$ donc $n+2 \mid 34$. Ainsi,

$$n+2 \in \{-34, -17, -2, -1, 1, 2, 17, 34\}$$

d'où

$$n \in \{-36, -19, -4, -3, -1, 0, 15, 32\}$$

On teste tous les cas et on obtient sous la forme d'un tableau :

n	-36	-19	-4	-3	-1	0	15	32
$\frac{8n-18}{n+2}$	9	10	25	42	-26	-9	6	7

On conclut que, pour tout $n \in \mathbb{Z}$:

$$\sqrt{\frac{8n-18}{n+2}} \in \mathbb{N} \iff n \in \{-36, -4\}$$

Correction de l'exercice 16 : Soient deux rationnels p/q et p'/q' avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux et $p' \in \mathbb{Z}$ et $q' \in \mathbb{N}^*$ premiers entre eux. On sait qu'il existe $n \in \mathbb{Z}$ tel que $\frac{p}{q} + \frac{p'}{q'} = n$. En mettant au même dénominateur, on obtient

$$pq' + p'q = nqq'$$

On obtient donc $q(nq' - p') = pq'$, et comme p et q sont premiers entre eux, par le théorème de Gauss, on déduit que $q \mid q'$. De même en factorisant par q , on obtient que $q' \mid q$, c'est-à-dire que $q = \pm q'$. Comme q et q' sont des nombres entiers naturels, on a $q = q'$.

Correction de l'exercice 17 : Soient $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ avec p et q premiers entre eux. On suppose que p/q est solution de l'équation $x^4 + x + 1 = 0$, c'est-à-dire $\left(\frac{p}{q}\right)^4 + \frac{p}{q} + 1 = 0$. On multiplie par $q^4 > 0$, et on obtient :

$$p^4 + pq^3 + q^4 = 0$$

On peut réécrire cette équation $p(p^3 + q^3) = -q^4$, d'où $p \mid q^4$. Comme p et q sont premiers entre eux, p et q^4 sont premiers entre eux, donc p divise 1, c'est-à-dire $p = \pm 1$. De même, on peut réécrire l'équation $q(pq^2 + q^3) = -p^4$, d'où $q \mid p^4$. Par le même argument que précédemment, q divise 1 donc $q = 1$. Finalement, si le rationnel x est une solution de l'équation initiale, $x = \pm 1$. Cependant, 1 et -1 ne sont pas solution. Finalement, l'équation $x^4 + x + 1 = 0$, d'inconnue rationnelle x , n'a pas de solution.

Correction de l'exercice 18 : On sait que $7^2 \equiv 49 \equiv -1 \pmod{10}$, donc $7^4 \equiv 1 \pmod{10}$. On cherche donc à combien est congru 7^7 modulo 4. Comme $7 \equiv 3 \pmod{4}$, on a $7^2 \equiv 1 \pmod{4}$. Ainsi, $7^7 \equiv 3 \pmod{4}$. Il existe $k \in \mathbb{Z}$ tel que $7^7 = 4k + 3$, donc $7^{7^7} \equiv 7^{4k+3} \equiv 7^3 \pmod{10}$. Donc finalement, $7^{7^7} \equiv 3 \pmod{10}$.

Correction de l'exercice 19 : On a $p^2 - 1 = (p - 1)(p + 1)$. Comme p n'est pas divisible par 3, alors 3 divise $p - 1$ ou $p + 1$. De plus, 2 ne divise pas p , alors 2 divise $p - 1$ ou $p + 1$ et l'un des deux est divisible par 4. Ainsi, $(p - 1)(p + 1)$ est divisible par 8. Comme 3 et 8 sont premiers entre eux, $24 \mid (p - 1)(p + 1)$.

Correction de l'exercice 20 :

1. Si a est impair, a^n est impair, donc $a^n - 1$ est pair, et premier, donc $a^n - 1 = 2$. Or, $a^n \geq 4$ donc on en déduit que a est pair.
2. La formule de la somme des séries géométriques est :

$$(x^n - 1) = (x - 1) \sum_{k=0}^{n-1} x^k$$

On en déduit que $a^n - 1 = (a - 1) \sum_{k=0}^{n-1} a^k$. Comme $a^n - 1$ est premier, ses seuls diviseurs sont 1 et $a^n - 1$. On en déduit que $a - 1 = 1$, d'où $a = 2$ (l'autre cas est exclu car $n \geq 2$).

3. Supposons que n n'est pas premier. Il existe donc $(p, q) \in \mathbb{N}^2$ tel que $n = pq$ avec $p > 1$ et $q > 1$. On en déduit donc que

$$2^n - 1 = 2^{pq} - 1 = 2^{p^q} - 1 = (2^p - 1) \sum_{k=1}^{q-1} 2^{pk}$$

Comme $2^n - 1$ est premier, on a $2^p - 1 = 2^n - 1$ (c'est-à-dire $p = n$, ce qui est absurde) ou $2^p - 1 = 1$ (c'est-à-dire $p = 1$, ce qui est absurde)... Ainsi, n est premier.

Correction de l'exercice 21 : Soit p un nombre premier tel que $2^p - 1$ soit premier. On va lister les diviseurs de $2^p(2^p - 1)$: comme $2^p - 1$ est premier, ses diviseurs sont 1 et $2^p - 1$. Les diviseurs de 2^p sont les 2^k avec $k \in \llbracket 0, p \rrbracket$, donc les diviseurs de $2^p(2^p - 1)$ sont :

$$2^0 = 1, 2, 2^2, \dots, 2^p, (2^p - 1), 2(2^p - 1), 2^2(2^p - 1), \dots, 2^p(2^p - 1)$$

On somme tous ces nombres, et on obtient :

$$\begin{aligned} \sum_{k=0}^p 2^k + \sum_{k=0}^p 2^k(2^p - 1) &= 2^p - 1 + (2^p - 1)^2 \\ &= (2^p - 1)(1 + 2^p - 1) \\ &= 2^p(2^p - 1) \end{aligned}$$

Correction de l'exercice 22 :

1. Soit $d \in \mathbb{N}$ le degré de P . Il existe des entiers $(c_0, \dots, c_d) \in \mathbb{Z}^{d+1}$ tels que $P(X) = \sum_{k=0}^d c_k X^k$. On a donc :

$$P(x) = 0 = c_d \left(\frac{a}{b}\right)^d + c_{d-1} \left(\frac{a}{b}\right)^{d-1} + \dots + c_1 \frac{a}{b} + c_0$$

En multipliant par b^d , on obtient

$$c_d a^d + c_{d-1} a^{d-1} b + \dots + c_1 a b^{d-1} + c_0 b^d = 0$$

donc

$$c_d a^d = -b \left(c_{d-1} a^{d-1} + \dots + c_1 a b^{d-2} + c_0 b^{d-1} \right)$$

ce qui montre que $b \mid c_d a^d$. Les entiers a et b étant premiers entre eux, a^d et b sont aussi premiers entre eux donc par le théorème de Gauss, $b \mid c_d$.

De même, en factorisant cette fois-ci par a , on obtient $a \mid c_0$.

2. Soit $x = a/b$ une racine rationnelle de P avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ premiers entre eux. Par ce qui précède, $b \mid 6$, d'où $b \in \{1, 2, 3, 6\}$ et $a \mid 2$ d'où $a \in \{-2, -1, 1, 2\}$. Tester tous les cas permet de trouver que P admet deux racines rationnelles : $\frac{1}{2}$ et $\frac{2}{3}$. On en déduit qu'une factorisation de P est : $P = (2X - 1)(3X - 2)(X^2 + 1)$.

Correction de l'exercice 23 : On suppose qu'il n'y en a qu'un nombre fini $p_1 < p_2 < \dots < p_n$. Considérons alors l'entier $N \equiv 4p_1 \dots p_n - 1$. $N \equiv -1 \pmod{4}$ donc N est impair et tous ses diviseurs premiers sont impairs. De plus, ils ne peuvent tous être congrus à 1 modulo 4 sinon N serait congru à 1 modulo 4. Donc il existe $i \in \llbracket 1, n \rrbracket$ tel que $p_i \mid N$, d'où $p_i \mid 1$, ce qui est absurde.

Correction de l'exercice 24 : On peut considérer que $\frac{1}{x} \geq \frac{1}{y}$, l'autre cas étant similaire en inversant les rôles de x et y . On a donc $\frac{1}{x} \geq \frac{1}{2} \cdot \frac{p}{q}$ donc $x \leq \frac{2q}{p}$. Il n'y a qu'un nombre fini d'entiers x inférieurs à $\frac{2q}{p}$, et pour chaque x solution, il n'y a qu'un seul y qui convient, donc finalement, il n'y a qu'un nombre fini de solutions.

Correction de l'exercice 25 : Comme x et y sont premiers entre eux, le théorème de Gauss dit que $x^3 \mid (y+1)^3$, donc que $x \mid y+1$, d'où $x \leq y+1$.

De même, $y^2 \mid (3x+1)$ donc $y^2 \leq 3x+1$.

En combinant les inégalités, on obtient :

$$x^2 - 5x \leq 0$$

D'où $x \in \{0, 1, 2, 3, 4, 5\}$. On teste les différentes valeurs possibles pour x et on trouve que la seule possibilité est $x = 5$ et $y = 4$. Finalement, $N - 10 = 4^2 \times 5^3 = 2000$ donc $N = 2010$.

Correction de l'exercice 26 : Soit x_0 une solution de (\mathcal{S}) . Il existe $j \in \mathbb{Z}, k \in \mathbb{Z}$ tels que $5 + 13k = x_0 = 4 + 9j$, d'où $9j - 13k = 1$. On choisit $j = 3$ et $k = 2$, c'est-à-dire $x_0 = 5 + 26 = 31$. On obtient donc :

$$(\mathcal{S}) \iff \begin{cases} x \equiv 31 \pmod{13} \\ x \equiv 31 \pmod{9} \end{cases} \iff x \equiv 31 \pmod{117}$$

Ainsi, l'ensemble des solutions est $31 + 117\mathbb{Z}$.

Correction de l'exercice 27 :

$$(\mathcal{S}) \iff \begin{cases} 14x \equiv x \equiv 22 \equiv 9 \pmod{13} \\ 22x \equiv x \equiv 26 \equiv 5 \pmod{7} \\ 12x \equiv x \equiv 42 \equiv 9 \pmod{11} \end{cases}$$

Notons

$$(\mathcal{S}_1): \begin{cases} x \equiv 9 \pmod{13} \\ x \equiv 5 \pmod{7} \end{cases}$$

Soit x_1 une solution de (\mathcal{S}_1) . Il existe $j \in \mathbb{Z}, k \in \mathbb{Z}$ tels que $9 + 13k = x_1 = 5 + 7j$, d'où $7j - 13k = 4$. On choisit $j = 8$ et $k = 4$, c'est-à-dire $x_0 = 5 + 56 = 61$. On obtient donc :

$$(\mathcal{S}) \iff \begin{cases} x \equiv 61 \pmod{13 \times 7} \\ x \equiv 9 \pmod{11} \end{cases}$$

Soit x_0 une solution de (\mathcal{S}) . Il existe $j' \in \mathbb{Z}, k' \in \mathbb{Z}$ tels que $61 + 91k' = x_0 = 9 + 11j'$, d'où $11j' - 91k' = 52$.

Calculons le PGCD de 11 et 91 via l'algorithme d'Euclide. On effectue d'abord la division euclidienne de 91 par 11

$$91 = 11 \times 8 + 3$$

puis on recommence en divisant toujours le dividende par le reste, jusqu'à ce que le reste égale 0 :

$$11 = 3 \times 3 + 2, \quad 3 = 2 \times 1 + 1, \quad 2 = 1 \times 1 + 0$$

On déduit donc que 91 et 11 sont premiers entre eux. Il existe donc un couple $(u, v) \in \mathbb{Z}^2$ tel que $91u + 11v = 1$. On part maintenant de $1 = 3 - 2 \times 1$ et on remonte :

$1 = 3 - 2 \times 1 = 3 - (11 - 3 \times 3) \times 1 = 4 \times 3 - 11 \times 1 = 4 \times (91 - 11 \times 8) - 11 \times 1 = 4 \times 91 - 11 \times 33$, d'où le résultat avec $u = 4$ et $v = -33$.

On choisit $j = -33 \times 52 = -1716$ et $k = -4 \times 52 = -208$, c'est-à-dire $x_0 = -18867$. On obtient donc :

$$\begin{aligned} (\mathcal{S}) &\iff \begin{cases} x \equiv -18867 \pmod{91} \\ x \equiv -18867 \pmod{11} \end{cases} \\ &\iff x \equiv -18867 \pmod{1001} \end{aligned}$$

Ainsi, l'ensemble des solutions est $-18867 + 1001\mathbb{Z}$.

Correction de l'exercice 28 : Le plus petit entier $N = x^2$ recherché doit vérifier :

$$2010 \times 10^n \leq x^2 < 2011 \times 10^n$$

où $n \in \mathbb{N}$ est tel que $n + 4$ est le nombre de chiffres de N .

- Cas où $n = 2p$, $p \in \mathbb{N}$: on remplace et on prend la racine de l'inégalité

$$44,8330 \dots 10^p \leq x < 44,8441 \dots 10^p$$

Le plus petit p qui permet d'obtenir un x convenable est $p = 2$ et $x = 4484$. Ainsi, $N = 20106256$.

- Cas où $n = 2p + 1$, $p \in \mathbb{N}$: On a

$$20100 \times 10^{2p} \leq x^2 < 20110 \times 10^{2p}$$

D'où, en prenant la racine de l'expression

$$141,7744 \dots \times 10^p \leq x < 141,8097 \dots \times 10^p$$

Le plus petit p qui permet d'obtenir un x convenable est $p = 1$ et $x = 1418$. Ainsi, $N = 2010724$.

Finalement, la solution est $N = 2010724$.

Correction de l'exercice 29 :

- Si n n'est pas une puissance de deux, alors il existe deux entiers $r \in \mathbb{N}$ et $k \in \mathbb{N}^*$ tels que $n = 2^r(2k+1)$. Notons $a = \max(2^{r+1}, 2k+1)$ et $b = \min(2^{r+1}, 2k+1)$. On a donc $n \geq a > b \leq 2$, et a et b ne sont pas de même parité. Posons alors

$$p = \frac{a-b+1}{2}, \quad q = \frac{a+b-1}{2}.$$

Alors p et q sont des entiers, et $0 < p < q < n$. De plus,

$$p + (p+1) + \dots + q = \frac{1}{2}(p+q)(q-p+1) = \frac{1}{2}ab = n$$

Donc n divise bien la somme.

- Si n est une puissance de deux, $n = 2^k$, avec $k \leq 2$ et $n \mid \frac{1}{2}(p+q)(q-p+1)$, alors $2^{k+1} \mid (p+q)(q-p+1)$. Un des deux facteurs est impair, donc 2^{k+1} divise $p+q$ ou $q-p+1$. Mais,

$$2^{k+1} = 2n > p+q > q-p+1$$

Il y a donc une contradiction.

Correction de l'exercice 30 :

1. Le théorème de Bezout assure l'existence de deux entiers u_1 et v_1 vérifiant $au_1 - bv_1 = 1$. On effectue ensuite la division euclidienne de u_1 par b : il existe $q \in \mathbb{Z}$ et $u_0 \in \mathbb{N}$ tels que $u_0 < b$ et $u_1 = bq + u_0$. On obtient donc $(bq + u_0)a - v_1b = 1 = u_0a - v_0b$ avec $v_0 = v_1 - aq$. Donc $-1 \leq v_0b = u_0a - 1 < u_0a < ba$, et en divisant par $b \geq 2$, on tire $0 \leq v_0 < a$. Ceci étant, considérons un couple (u, v) vérifiant $au - bv = 1$. On obtient donc

$$a(u - u_0) = b(v - v_0) \quad (**)$$

Ceci montre que $a \mid (v - v_0)b$ et comme a et b sont premiers entre eux, le théorème de Gauss entraîne $a \mid (v - v_0)$. Soit $k \in \mathbb{Z}$ tel que $v = v_0 + ka$. En remplaçant dans (**), on a $(u, v) = (u_0 + kb, v_0 + ka)$ avec $k \in \mathbb{Z}$. Réciproquement, on vérifie facilement que ce couple est solution.

2. Les nombres 47 et 111 sont premiers entre eux, d'où l'existence de u et v . Nous allons les déterminer grâce à l'algorithme d'Euclide. On effectue d'abord la division euclidienne de 111 par 47

$$111 = 47 \times 2 + 17$$

puis on recommence en divisant toujours le dividende par le reste, jusqu'à ce que le reste égale 1 :

$$47 = 17 \times 2 + 13, \quad 17 = 13 \times 1 + 4, \quad 13 = 4 \times 3 + 1$$

On part maintenant de $1 = 13 - 4 \times 3$ et on remonte :

$$1 = 13 - 4 \times 3 = 13 - (17 - 13 \times 1) \times 3 = 4 \times 13 - 3 \times 17 = 4 \times (47 - 17 \times 2) - 17 \times 3 = 4 \times 47 - 11 \times 17 = 4 \times 47 - 11 \times (111 - 47 \times 2) = 26 \times 47 - 11 \times 111, \text{ d'où le résultat avec } u = 26 \text{ et } v = -11.$$

Correction de l'exercice 31 : Lemme. Un nombre est congru à la somme des chiffres modulo 9. Soit un nombre n dont l'écriture décimale est $\overline{a_p a_{p-1} a_{p-2} \cdots a_1 a_0}$, avec $p \geq 0$ et $\forall i \in \llbracket 0, p \rrbracket$, $a_i \in \llbracket 0, 9 \rrbracket$, c'est-à-dire $n = \sum_{i=0}^p a_i 10^i$. Comme $10 \equiv 1 \pmod{9}$, on a $\forall i \in \llbracket 0, p \rrbracket$, $a_i 10^i \equiv a_i \pmod{9}$, d'où finalement $n \equiv \sum_{i=0}^p a_i \pmod{9}$.

On déduit du lemme que $4444^{4444} \equiv A \equiv B \equiv C \pmod{9}$. On a $4444 \equiv 7 \pmod{9}$. Ainsi, $4444^2 \equiv 4 \pmod{9}$ et $4444^3 \equiv 1 \pmod{9}$. On cherche ainsi le reste de la division euclidienne de 4444 par 3 et on obtient $4444 \equiv 1 \pmod{3}$, donc il existe $k \in \mathbb{Z}$ tel que $4444 = 3k + 1$, donc $4444^{4444} \equiv 4444^{3k+1} \equiv 4444 \equiv 7 \pmod{9}$. Ainsi, $C \equiv 7 \pmod{9}$.

Mais ceci ne donne pas C ! Nous allons majorer C de manière à montrer que $C = 7$. On sait que $4444^{4444} \leq 10000^{5000} = 10^{20000}$: il a donc au plus 20000 chiffres. Ainsi, A vaut, au plus, $9 \times 20000 = 180000$ et a donc au plus 6 chiffres. Du coup, B vaut au plus $6 \times 9 = 54$, d'où $C \leq 5 + 9 = 14$. Comme $C \equiv 7 \pmod{9}$, on en déduit que $C = 7$.

PETIT THÉORÈME DE FERMAT

Exercice 32 : (Petit théorème de Fermat) Soit p un nombre premier. Montrer que, pour tout $k \in \llbracket 1, p-1 \rrbracket$, $p \mid \binom{p}{k}$. En déduire que, pour tout $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$, et que pour tout $a \in \mathbb{Z}$ non multiple de p , $a^{p-1} \equiv 1 \pmod{p}$.

Correction de l'exercice 32 : Soit $k \in \llbracket 1, p-1 \rrbracket$. On a

$$k \binom{p}{k} = \frac{kp!}{k!(p-k)!} = \frac{kp(p-1)!}{k(k-1)!(p-1-(k-1))!} = p \binom{p-1}{k-1}$$

Ainsi,

$$p \mid k \binom{p}{k}$$

Comme p est premier, p et k sont premiers entre eux, donc on déduit par le théorème de Gauss que $p \mid \binom{p}{k}$.

Soient $(a, b) \in \mathbb{Z}^2$. Le binôme de Newton donne :

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^k b^{p-k}$$

On prend donc cette relation modulo p , et, avec ce qui précède, on obtient :

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Montrons par récurrence sur $a \in \mathbb{N}$ le résultat. On a bien $0^p \equiv 0 \pmod{p}$. Supposons maintenant la propriété vraie pour $a \in \mathbb{N}$. Par ce qui précède, on a

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

Par hypothèse de récurrence, on en déduit que

$$(a+1)^p \equiv a+1 \pmod{p}.$$

Le résultat se généralise à \mathbb{Z} sans problème.

Si maintenant a n'est pas divisible par p , alors a est premier avec p et par le théorème de Gauss, $p \mid a^{p-1} - 1$.

Exercices d'application

Exercice 33 : Montrer que $30 \mid n^5 - n$ pour tout $n \in \mathbb{N}$.

Exercice 34 : Démontrer que :

$$\forall x \in \mathbb{Z}, x^3 \equiv x \pmod{6} \quad \text{et} \quad x^7 \equiv x \pmod{42}$$

Exercice 35 : (Centrale MP 2006) Soient a, b, c des entiers. Montrer que si 7 divise $a^3 + b^3 + c^3$, alors $7 \mid abc$. En déduire que le système

$$(\mathcal{S}) : \begin{cases} x^3 + y^3 + z^3 = 7 \\ xyz = 7(x^2 + y^2 + z^2) + 1 \end{cases}$$

n'a pas de solution de \mathbb{Z}^3 .

On pourra raisonner par contraposée.

Corrigés

Correction de l'exercice 33 : Soit $n \in \mathbb{N}$. On sait que n et n^5 sont de même parité, $n^5 - n \equiv 0 \pmod{2}$. On peut ensuite appliquer deux fois le petit théorème de Fermat aux nombres premiers 3 et 5. On obtient donc :

$$n^3 \equiv n \pmod{3}$$

$$n^5 \equiv n \pmod{5}$$

Mais si $n^3 \equiv n \pmod{3}$, ça signifie que $n^5 \equiv n^3 \equiv n \pmod{3}$. Comme les entiers 2, 3 et 5 sont premiers entre eux dans leur ensemble, on a $n^5 - n \equiv 0 \pmod{2 \times 3 \times 5}$, et c'est ce que l'on voulait.

Correction de l'exercice 34 : Soit $x \in \mathbb{Z}$. On sait que x^3 et x sont de même parité. De plus, le petit théorème de Fermat donne que $x^3 \equiv x \pmod{3}$. Comme 2 et 3 sont premiers entre eux, on a $x^3 \equiv x \pmod{6}$. On en déduit donc que $x^7 = x \times x^3 \times x^3 \equiv x \times x \times x \equiv x \pmod{6}$. De plus, le petit théorème de Fermat donne $x^7 \equiv x \pmod{7}$. Comme 6 et 7 sont premiers entre eux, $x^7 \equiv x \pmod{42}$.

Correction de l'exercice 35 : Supposons que $7 \nmid abc$, alors $7 \nmid a$, $7 \nmid b$ et $7 \nmid c$. Le petit théorème de Fermat donne que $a^6 \equiv 1 \pmod{7}$, $b^6 \equiv 1 \pmod{7}$ et $c^6 \equiv 1 \pmod{7}$. Comme $a^6 - 1 = (a^3 - 1)(a^3 + 1)$, on a $a^3 \equiv \pm 1 \pmod{7}$. De même $b^3 \equiv \pm 1 \pmod{7}$ et $c^3 \equiv \pm 1 \pmod{7}$. On en déduit aisément que $a^3 + b^3 + c^3 \not\equiv 0 \pmod{7}$.

Si le système (\mathcal{S}) admet au moins une solution $(x, y, z) \in \mathbb{Z}^3$, alors, d'après la première équation, $7 \mid x^3 + y^3 + z^3$. Donc, d'après ce qui précède, $7 \mid xyz$ ce qui contredit la seconde équation. Ainsi, (\mathcal{S}) n'a pas de solution dans \mathbb{Z}^3 .