DS 5 : Énoncé.

Les calculatrices sont interdites.

Premier problème : une application du théorème de Ramsey

Pour tout ce problème, on fixe un entier naturel p. On suppose que p est premier.
On notera $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.
Lorsque E est un ensemble fini, on notera $|E|$ le cardinal de E.

Partie I : Racines d'un polynôme modulo p

On note $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{Z}$.
Par exemple, $P_0(X) = 2X^2 - 3X + 1$ est un élément de $\mathbb{Z}[X]$.

1°) Déterminer les racines réelles de P_0.

Lorsque $P \in \mathbb{Z}[X]$, on note $\overline{P}$ l'application de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$ définie par :
pour tout $h \in \mathbb{Z}$, $\overline{P}(\overline{h}) = \overline{P(h)}$.

2°) Lorsque $P \in \mathbb{Z}[X]$, montrer que $\overline{P}$ est correctement définie.

Lorsque $\alpha \in \mathbb{Z}/p\mathbb{Z}$, on dit que α est une racine de P modulo p si et seulement si $\overline{P}(\alpha) = 0$.

3°) Déterminer les racines modulo 7 de P_0.

4°) Soit $P \in \mathbb{Z}[X]$.
On suppose que $\overline{P} \neq 0$, c'est-à-dire qu'il existe $y \in \mathbb{Z}/p\mathbb{Z}$ tel que $\overline{P}(y) \neq 0$.
Soit $\alpha \in \mathbb{Z}/p\mathbb{Z}$. On suppose que α est une racine de P modulo p.
Montrer que $\deg(P) \geq 1$ et qu'il existe $Q \in \mathbb{Z}[X]$ avec $\deg(Q) \leq \deg(P) - 1$ tel que, pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $\overline{P}(x) = (x - \alpha)\overline{Q}(x)$.

5°) Soit $P \in \mathbb{Z}[X]$ tel que $\overline{P} \neq 0$.
Soit $k \in \mathbb{N}$. On suppose qu'il existe dans $\mathbb{Z}/p\mathbb{Z}$ au moins k racines de P modulo p.
Montrer que $\deg(P) \geq k$.

Partie II : Puissances n-ièmes dans $\mathbb{Z}/p\mathbb{Z}$

Dans cette partie, on fixe $n \in \mathbb{N}^*$.
On note $S = \{x^n \ / \ x \in (\mathbb{Z}/p\mathbb{Z})^*\}$.

6°) Montrer que S est un groupe pour le produit.

7°) On définit sur $(\mathbb{Z}/p\mathbb{Z})^*$ une relation binaire en convenant que,
pour tout $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$, $x \ R \ y \iff x^{-1}y \in S$.
Montrer que R est une relation d'équivalence.
Pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^*$, notons $aS = \{as \ / \ s \in S\}$.
Montrer que $\{aS \ / \ a \in (\mathbb{Z}/p\mathbb{Z})^*\}$ constitue une partition de $(\mathbb{Z}/p\mathbb{Z})^*$.

8°) À l'aide de la question 5, montrer que $|S| \geq \dfrac{p-1}{n}$.

9°) Montrer que $|\{aS \ / \ a \in (\mathbb{Z}/p\mathbb{Z})^*\}| \leq n$.

Partie III : Théorème de Schur

Dans cette partie, on fixe un entier $n \in \mathbb{N}^*$.

On admettra le théorème de Ramsey (démontré lors du DS 4), dont voici une version simplifiée, qui suffira pour cette partie :
Théorème de Ramsey :
Définitions et données : Lorsque V est un ensemble fini, on note $\mathcal{P}_2(V)$ l'ensemble des parties de V de cardinal 2. On dit que les éléments de $\mathcal{P}_2(V)$ sont les arêtes du graphe complet dont les sommets sont les éléments de V. On notera $K(V)$ ce graphe complet. Soit C un ensemble de cardinal n, dont les éléments sont appelés des couleurs. On appelle coloriage de $K(V)$ dans C toute application c de $\mathcal{P}_2(V)$ dans C. Pour un tel coloriage c, lorsque α, β, γ sont trois éléments distincts de V,
on dit qu'ils constituent un triangle monochrome
si et seulement si $c(\{\alpha, \beta\}) = c(\{\alpha, \gamma\}) = c(\{\beta, \gamma\})$.
Conclusion : il existe $N \in \mathbb{N}^*$ tel que, pour tout ensemble V de cardinal supérieur ou égal à N, pour tout ensemble C de cardinal n, pour tout coloriage de $K(V)$ dans C, il existe dans V un triangle monochrome.

10°) Montrer qu'il existe $N \in \mathbb{N}^*$ tel que, lorsque $p \geq N$ (avec $p \in \mathbb{P}$),
pour tout ensemble C de cardinal n, pour toute application d de $(\mathbb{Z}/p\mathbb{Z})^*$ dans C, il existe $x, y, z \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $d(x) = d(y) = d(z)$ et $x + y = z$.

11°) En déduire qu'il existe N tel que, lorsque $p \geq N$ (avec $p \in \mathbb{P}$),
il existe des entiers relatifs x, y, z tels que, modulo p, $x^n + y^n \equiv z^n$ (Équation de Fermat modulo p), alors que x, y et z sont tous les trois non congrus à 0 modulo p.

Second problème :
Inverses généralisés d'applications linéaires

Dans ce problème, $\mathbb{K}$ désigne un corps quelconque.

Lorsque u et v sont deux applications pour lesquelles la composée $u \circ v$ est définie, on notera aussi uv au lieu de $u \circ v$.
En particulier, u^2 désigne $u \circ u$.

Pour tout le problème, on suppose que E et F sont deux $\mathbb{K}$-espaces vectoriels de dimensions finies.
Lorsque $u \in L(E,F)$, on appelle rang de u et on note $\mathrm{rg}(u)$ la quantité $\dim(\mathrm{Im}(u))$.

Partie I : préliminaires

1°) Soit F et G deux sous-espaces vectoriels de E tels que $F \oplus G = E$.
Si $(e_1, \ldots, e_p)$ est une base de F et si $(e_{p+1}, \ldots, e_n)$ est une base de G, montrer que $(e_1, \ldots, e_n)$ est une base de E.
En déduire que $\dim(E) = \dim(F) + \dim(G)$.

2°) Réciproquement, montrer que si $(e_1, \ldots, e_n)$ est une base de E et si $p \in \{0, \ldots, n\}$, en posant $F = \mathrm{Vect}(e_1, \ldots, e_p)$ et $G = \mathrm{Vect}(e_{p+1}, \ldots, e_n)$, alors $E = F \oplus G$.

3°) Soit $u \in L(E,F)$ et H un sous-espace vectoriel de E tel que $\mathrm{Ker}(u) \oplus H = E$.
Montrer que $u|_H^{\mathrm{Im}(u)}$ est un isomorphisme.
En déduire la formule du rang : $\dim(E) = \mathrm{rg}(u) + \dim(\mathrm{Ker}(u))$.

Soit $p \in L(E)$. On dit que p est un projecteur de E si et seulement si $p^2 = p$.

4°) Soit p un projecteur de E.
Montrer que $\mathrm{Im}(p) = \{x \in E \ / \ p(x) = x\}$.
Montrer que $\mathrm{Im}(p) \oplus \mathrm{Ker}(p) = E$.

Partie II : g-inverses

Lorsque $u \in L(E,F)$ et $v \in L(F,E)$, on dit que v est un inverse généralisé de u, ou bien que v est un g-inverse de u si et seulement si $uvu = u$.

5°) Soit $u \in L(E,F)$. Lorsque $u = 0$, quels sont les g-inverses de u ?
Lorsque u est un isomorphisme, quels sont les g-inverses de u ?

6°) Soit $u \in L(E,F)$ et $v \in L(F,E)$. On suppose que v est un g-inverse de u.
On pose $p = vu$ et $q = uv$.
a) Montrer que p et q sont des projecteurs.
b) Montrer que $\mathrm{Im}(q) = \mathrm{Im}(u)$ et $\mathrm{Ker}(p) = \mathrm{Ker}(u)$.
c) Montrer que $\mathrm{rg}(p) = \mathrm{rg}(q) = \mathrm{rg}(u) \leq \mathrm{rg}(v)$.

d) Montrer qu'il existe un sous-espace vectoriel E_1 de E tel que $\mathrm{Ker}(u) \oplus E_1 = E$ et tel que $v|_{\mathrm{Im}(u)}^{E_1} = \left(u|_{E_1}^{\mathrm{Im}(u)}\right)^{-1}$.

7°) Soit $u \in L(E,F)$.
Montrer que u possède au moins un g-inverse v.
Soit s un entier compris entre $\mathrm{rg}(u)$ et $\min(\dim(E), \dim(F))$. Montrer que u possède au moins un g-inverse v tel que $rg(v) = s$.

8°) Soit $u \in L(E,F)$. Notons v_0 un g-inverse de u.
a) Montrer que l'ensemble des g-inverses de u est $\{v_0 + a \ / \ a \in A\}$, où A est un sous-espace vectoriel de $L(F,E)$ que l'on précisera.

b) Pour tout $w \in A$, on pose $\varphi(w) = w|_{\mathrm{Im}(u)}^{\mathrm{Ker}(u)}$.
Montrer que φ est une application linéaire surjective de A sur $L(\mathrm{Im}(u), \mathrm{Ker}(u))$.

c) Calculer la dimension de A en fonction de u.

9°) Soit $u \in L(E,F)$ et soit v un g-inverse de u. Soit $b \in F$.
On note $(\mathcal{E})$ l'équation $u(x) = b$ en l'inconnue $x \in E$.
Montrer que $(\mathcal{E})$ possède au moins une solution si et seulement si $b = (uv)(b)$ et dans ce cas, montrer que l'ensemble des solutions est $\{v(b) + (\mathrm{Id}_E - vu)(z) \ / \ z \in E\}$.