Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont interdits.

La qualité de la rédaction est un facteur important d'appréciation des copies. Les candidats sont donc invités à produire des raisonnements clairs, complets et concis.

Les candidats peuvent utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant dans ce cas à préciser la référence du résultat utilisé.

Notations, vocabulaire et rappels

— On désigne par $\mathbf{Z}$ l'anneau des entiers relatifs, $\mathbf{Q}$ le corps des nombres rationnels, $\mathcal{P}$ l'ensemble des nombres premiers.

— Soit A un anneau commutatif, unitaire (c'est-à-dire possédant un élément neutre pour la multiplication).

- $A^\times$ désigne le groupe des éléments inversibles de A.
- On note $A[X]$ l'anneau des polynômes à coefficients dans A et, pour tout entier naturel n, $A_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n à coefficients dans A.
- On dénote par $\mathcal{M}_n(A)$ l'anneau des matrices (n,n) à coefficients dans A et $\mathcal{T}_n(A)$ l'ensemble des matrices (n,n) triangulaires inférieures à coefficients dans A.
- Un polynôme de $A[X]$ est dit *unitaire* lorsque son coefficient dominant est 1.
- Une fonction f de A dans A est dite *polynomiale* s'il existe un polynôme P dans $A[X]$ tel que :
$$\forall a \in A,\ f(a) = P(a).$$
- Par convention, un produit d'éléments de A indexé sur l'ensemble vide est égal à 1.

— Soient k et n deux entiers naturels. On désigne par $\binom{n}{k}$ le coefficient binomial "k parmi n", c'est-à-dire le nombre de possibilités de choisir k éléments dans un ensemble à n éléments ; si $n = k = 0$, ce nombre vaut 1. Si $k > n$, cette quantité est nulle, par convention.

— Pour tout entier naturel k, on introduit le polynôme à coefficients rationnels
$$H_k(X) = \begin{cases} 1 & \text{si } k = 0 \\ \frac{X(X-1)\cdots(X-k+1)}{k!} & \text{sinon.} \end{cases}$$

— On définit l'anneau des *entiers de Gauss* de la manière suivante :
$$\mathbf{Z}[i] = \{a + ib\,;\ a, b \in \mathbf{Z}\}.$$
Si z est un entier de Gauss et a, b sont les entiers tels que $z = a + ib$, on note
$$N(z) = z\overline{z} = (a + ib)(a - ib).$$

— On introduit l'opération de *dérivation discrète* :

$$\begin{array}{rccc} \Delta : & \mathbf{Q}[X] & \to & \mathbf{Q}[X] \\ & P(X) & \mapsto & P(X+1) - P(X) \end{array}$$

On définit les itérées de cette opération par récurrence :

$$\forall P \in \mathbf{Q}[X]\,,\ \Delta^0(P) = P \text{ et } \forall k \in \mathbf{N}^*,\ \Delta^k(P) = \Delta(\Delta^{k-1}(P)).$$

— On rappelle la définition d'un *polynôme interpolateur de Lagrange*. Soit $n \in \mathbf{N}$. Soit $k \in \{0, \cdots, n\}$. Le polynôme $L_k^n(X)$ est l'unique polynôme de degré n de $\mathbf{Q}[X]$ tel que, pour tout $h \in \{0, \cdots, n\}$, $L_k^n(h) = \delta_{kh}$ où δ_{kh} est le symbole de Kronecker (il vaut 0 si $k \neq h$ et 1 si $k = h$). Plus précisément,

$$L_k^n(X) = \prod_{i=0,\ i\neq k}^{n} \frac{X-i}{k-i}.$$

Exercices Préliminaires

Exercice 1

1. Justifier que les polynômes H_0, H_1, H_2 et H_3 forment une famille libre dans $\mathbf{Q}[X]$.
2. Expliciter le sous-espace vectoriel $\mathcal{F}$ de $\mathbf{Q}[X]$ engendré par les polynômes H_0, H_1, H_2 et H_3.
3. Justifier que Δ induit un endomorphisme sur $\mathcal{F}$.

On note $\Delta_{\mathcal{F}}$ l'endomorphisme induit par Δ sur $\mathcal{F}$.

4. Déterminer le polynôme caractéristique de $\Delta_{\mathcal{F}}$.
5. Déterminer le polynôme minimal de $\Delta_{\mathcal{F}}$.
6. L'endomorphisme $\Delta_{\mathcal{F}}$ est-il diagonalisable ?

Exercice 2

Soit k un corps.

Soit n un entier naturel. Pour $n+1$ éléments de k, $x_0, ..., x_n$, on note $V(x_0, ..., x_n)$ la matrice dans $\mathcal{M}_{n+1}(k)$ définie par

$$V(x_0, ..., x_n) = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix}$$

1. Soient $a_0, a_1, ..., a_n$ dans k et soit P le polynôme $P = \sum_{j=0}^{n} a_j X^j$. Expliciter en fonction de P et $x_0, ..., x_n$ le vecteur :
$$V(x_0, ..., x_n) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}$$
2. Justifier qu'il existe une matrice T dans $\mathcal{M}_{n+1}(k)$, de déterminant 1, telle que
$$V(x_0, ..., x_n)T = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} & 0 \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} & 0 \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} & \prod_{i=0}^{n-1}(x_n - x_i) \end{pmatrix}$$
3. En déduire, par récurrence, une expression du déterminant de $V(x_0, ..., x_n)$ en fonction de $x_0, ..., x_n$.

Soit K un corps tel que $k \subset K$.

4. Soit P un polynôme dans $K[X]$ de degré n tel que $P(k) \subset k$. Soient $a_0, a_1, ..., a_n$ dans K tels que $P = \sum_{j=0}^{n} a_j X^j$. On suppose que k contient $n+1$ éléments distincts $x_0, ..., x_n$. Démontrer que $P \in k[X]$.

   Indication : On pourra utiliser $V(x_0, ..., x_n) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}$.

5. On note $\mathcal{E} = \{P \in K[X] \mid P(k) \subset k\}$.
   (a) On suppose que k est un corps infini. Démontrer que
   $$\mathcal{E} = k[X].$$
   (b) On suppose que k est un corps fini. On note q son cardinal. On note $\mathcal{I}$ l'idéal de $K[X]$ engendré par le polynôme $X^q - X$. Démontrer que
   $$\mathcal{E} = \{P + Q \ ; \ P \in \mathcal{I} \text{ et } Q \in k[X]\}$$

Exercice 3

On définit
$$\mathrm{Ent}(\mathcal{T}_2(\mathbf{Z})) = \{P \in \mathbf{Q}[X] \mid P(\mathcal{T}_2(\mathbf{Z})) \subseteq \mathcal{M}_2(\mathbf{Z})\}.$$
Pour deux entiers $x_0, x_1 \in \mathbf{Z}$, on pose
$$\phi(P)(x_0, x_1) = \begin{cases} \frac{P(x_1)-P(x_0)}{x_1-x_0}, & \text{si } x_1 \neq x_0; \\ P'(x_0), & \text{sinon.} \end{cases}$$

1. Soient $x_0, x_1 \in \mathbf{Z}$. Soit $P \in \mathbf{Q}[X]$. Exprimer le reste de la division euclidienne de P par $(X - x_0)(X - x_1)$ en fonction de x_0, $\phi(P)(x_0, x_1)$ et $P(x_0)$.
2. En déduire que
   $$\mathrm{Ent}(\mathcal{T}_2(\mathbf{Z})) = \{P \in \mathbf{Q}[X] \mid P(\mathbf{Z}) \subset \mathbf{Z} \text{ et } \phi(P)(\mathbf{Z}^2) \subseteq \mathbf{Z}.\}.$$
   Indication : Etant donné $P \in \mathbf{Q}[X]$, on pourra exprimer en fonction de y, $\phi(P)(x_0, x_1)$, $P(x_0)$ et $P(x_1)$ la matrice $P(T)$ pour toute matrice
   $$T = \begin{pmatrix} x_0 & 0 \\ y & x_1 \end{pmatrix}, x_0, x_1, y \text{ dans } \mathbf{Z}.$$

Exercice 4

Soit p un nombre premier.

1. Démontrer que toute fonction de $\mathbf{Z}/p\mathbf{Z}$ dans lui-même est polynomiale.
2. Déterminer le nombre de fonctions polynomiales de $\mathbf{Z}/p\mathbf{Z}$ dans lui-même.
3. Donner un exemple de fonction de $\mathbf{Z}/4\mathbf{Z}$ dans lui-même qui n'est pas polynomiale.

Problème

Notations et définitions.

— Soit A un anneau intègre ; on note $\mathbf{K}$ son corps de fractions.
Un polynôme P de $\mathbf{K}[X]$ est dit *à valeurs entières* sur A lorsque $P(A) \subseteq A$.

— Soit E un sous-ensemble de A.

— On définit

$$\mathrm{Ent}(E, A) = \{P \in \mathbf{K}[X] \mid P(E) \subseteq A\}$$

et, pour tout entier naturel n,

$$\mathrm{Ent}_n(E, A) = \{P \in \mathbf{K}_n[X] \mid P(E) \subseteq A\}.$$

On admettra **sans le vérifier** que $\mathrm{Ent}(A)$ est un anneau.
Lorsque $E = A$, on note plus simplement $\mathrm{Ent}(A)$ et $\mathrm{Ent}_n(A)$ pour $\mathrm{Ent}(A, A)$ et $\mathrm{Ent}_n(A, A)$ respectivement.

— Soit n un entier naturel. On dit qu'une famille $P_0, \cdots, P_n$ est une *base régulière de* $\mathrm{Ent}_n(E, A)$ si pour tout entier k compris entre 0 et n, P_k est un polynôme dans $\mathrm{Ent}(E, A)$ de degré k, et pour tout $P \in \mathrm{Ent}_n(E, A)$, il existe d'uniques $\lambda_0, \cdots, \lambda_n$ dans A, tels que

$$P(X) = \sum_{i=0}^{n} \lambda_i P_i(X).$$

— On dit qu'une famille $(P_n)_{n\in\mathbf{N}}$ est une *base régulière de* $\mathrm{Ent}(E, A)$ si pout tout entier naturel n, $P_0, \cdots, P_n$ est une base régulière de $\mathrm{Ent}_n(E, A)$.

Le problème est divisé en quatre parties.

I Polynômes à valeurs entières sur Z

Dans toute cette partie, n désigne un entier naturel.

1. Soit p un nombre premier. Démontrer que le polynôme

$$\frac{1}{p}(X^p - X)$$

est à valeurs entières sur $\mathbf{Z}$.

2. Soit k un entier naturel.
   (a) Quelles sont les racines du polynôme H_k ?
   (b) Démontrer que le polynôme H_k appartient à $\mathrm{Ent}(\mathbf{Z})$.
3. Démontrer que la famille $(H_k)_{k\in\{0,\ldots,n\}}$ est une $\mathbf{Q}$-base de $\mathbf{Q}_n[X]$.
4. Soit $P \in \mathbf{Q}[X]$ de degré n. Soit $(b_k)_{k\in\{0,\ldots,n\}}$ dans $\mathbf{Q}^{n+1}$ tel que

$$P(X) = \sum_{k=0}^{n} b_k H_k(X)$$

(a) Démontrer qu'il existe une matrice M dans $\mathcal{M}_{n+1}(\mathbf{Z})$ telle que

$$\begin{pmatrix} P(0) \\ \vdots \\ P(n) \end{pmatrix} = M \begin{pmatrix} b_0 \\ \vdots \\ b_n \end{pmatrix}$$

(b) Démontrer qu'il existe une matrice N dans $\mathcal{M}_{n+1}(\mathbf{Z})$ telle que

$$\begin{pmatrix} b_0 \\ \vdots \\ b_n \end{pmatrix} = N \begin{pmatrix} P(0) \\ \vdots \\ P(n) \end{pmatrix}$$

(c) En déduire que les assertions suivantes sont équivalentes :

(i) P est un polynôme à valeurs entières

(ii) $P(\{0, \ldots, n\}) \subseteq \mathbf{Z}$.

5. En déduire que la famille des $(H_k)_{k\in\mathbf{N}}$ forme une base régulière de $\mathrm{Ent}(\mathbf{Z})$.

6. (a) Démontrer que, pour tout P dans $\mathrm{Ent}(\mathbf{Z})$ de degré n, $n!P \in \mathbf{Z}[X]$.

(b) Démontrer que $n!$ est le plus petit entier naturel non nul k tel que $k\mathrm{Ent}_n(\mathbf{Z}) \subset \mathbf{Z}[X]$.

7. On rappelle qu'il est admis que $\mathrm{Ent}(\mathbf{Z})$ est un anneau.

(a) Démontrer que $\mathrm{Ent}(\mathbf{Z})$ est un anneau intègre.

(b) Déterminer $\mathrm{Ent}(\mathbf{Z})^\times$.

(c) Démontrer que, pour tout entier non nul k, le polynôme H_k est irréductible dans $\mathrm{Ent}(\mathbf{Z})$.

8. (a) Soit $k \in \{0, \ldots, n\}$. Démontrer que

$$L_k^n(X) = (-1)^{n-k} H_k(X) H_{n-k}(X - k - 1).$$

(b) En déduire que, pour P polynôme de $\mathbf{Q}[X]$ de degré n, P est un polynôme à valeurs entières si et seulement si P prend des valeurs entières sur $n+1$ entiers consécutifs.

9. Soit P un polynôme de $\mathbf{Q}[X]$ de degré n s'écrivant, par la question 3,

$$P(X) = \sum_{k=0}^{n} b_k H_k(X),$$

avec $b_0, \ldots, b_n$ dans $\mathbf{Q}$.

(a) Démontrer que, pour tout entier naturel non nul ℓ,

$$\sum_{i=0}^{\ell} (-1)^i \binom{\ell}{i} = 0.$$

(b) En déduire que, pour tout $k \in \{0, \cdots, n\}$,

$$b_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} P(i).$$

(c) Démontrer que

$$\Delta P(X) = \sum_{k=0}^{n-1} b_{k+1} H_k(X),$$

puis que, pour tout k dans $\{0, \ldots, n\}$, on a

$$b_k = \Delta^k(P)(0).$$

10. Pour tout polynôme unitaire $P \in \mathbf{Z}[X]$, on introduit

$$d(P) = \mathrm{pgcd}(P(z) \ ; \ z \in \mathbf{Z}).$$

(a) Calculer $d(X^5 + X)$.

(b) Démontrer que $d(P)$ divise $n!$ pour tout $P \in \mathbf{Z}[X]$ de degré n.

(c) Donner un polynôme P dans $\mathbf{Z}[X]$, unitaire et de degré n, tel que $d(P) = n!$.

II Généralisation des polynômes à valeurs entières sur un anneau A

Dans cette partie, A désigne un anneau infini commutatif, unitaire (c'est-à-dire possédant un élément neutre pour la multiplication), et **principal**. On note $\mathbf{K}$ le corps de fractions de A. Soit n un entier naturel. On introduit

$$I_n = \{0\} \cup \{\alpha \in \mathbf{K} \mid \exists P \in \mathrm{Ent}_n(A), \ P(X) = \alpha X^n + Q, \deg(Q) \leq n-1\}.$$

1. Soit P dans $\mathrm{Ent}(A)$ de degré n. Soient $a_0, \cdots, a_n \in A$. Soit

$$d = \prod_{0 \leq i < j \leq n} (a_j - a_i).$$

Démontrer que $dP \in A[X]$.
Indication : On pourra utiliser l'exercice 2.

2. En déduire qu'il existe α_n dans $A \setminus \{0\}$ tel que $\alpha_n I_n \subseteq A$.
3. En déduire qu'il existe β_n dans $\mathbf{K}^\times$ tel que $I_n = \beta_n A$.
4. Démontrer qu'il existe une base régulière de $\mathrm{Ent}(A)$.
5. On considère l'anneau $\mathbf{Z}[i]$.

(a) Propriétés de $\mathbf{Z}[i]$.

i. Soit N l'application qui envoie un élément z dans $\mathbf{Z}[i]$ sur $z\overline{z}$. Démontrer que N est à valeurs dans $\mathbf{N}$.

ii. Démontrer que

$$\mathbf{Z}[i]^\times = \{z \in \mathbf{Z}[i] \mid N(z) = 1\} = \{1, -1, i, -i\}.$$

iii. Démontrer que $\mathbf{Z}[i]$ est un anneau euclidien.

(b) Justifier que $\mathrm{Ent}(\mathbf{Z}[i])$ possède une base régulière.

(c) Soient

$$Q_0(X) = 1, \ Q_1(X) = X, \ Q_2(X) = \frac{1}{1+i}(X^2 - X).$$

Démontrer que la famille (Q_0, Q_1, Q_2) forme une base régulière de $\mathrm{Ent}_2(\mathbf{Z}[i])$.

III Polynômes à valeurs entières sur un sous-ensemble de Z

Notations et définitions.

Soit p un nombre premier.

— Soit $x \in \mathbf{Q}$. On définit la *valuation p-adique* de x, notée $v_p(x)$ de la façon suivante :

  — Si x est non nul, $v_p(x)$ est l'exposant de p dans la décomposition en facteurs premiers de x. En d'autres termes, si $x = p^\alpha \dfrac{a}{b}$, avec $\alpha \in \mathbf{Z}$, a, b entiers tous deux premiers avec p, alors $v_p(x) = \alpha$.

  — $v_p(0) = +\infty$.

  Ainsi par exemple, $v_p(p^2) = 2$ et $v_p(\frac{1}{p}) = -1$.

— Soit E un sous-ensemble non vide de $\mathbf{Z}$. On appelle *suite p-ordonnée* de E toute suite $\underline{a} = (a_n)_{n\in\mathbf{N}}$ telle que :

  — $a_0 \in E$,

  — $a_1 \in E$ et a_1 minimise la valuation p-adique de $a_1 - a_0$, c'est-à-dire

$$v_p(a_1 - a_0) = \min_{x\in E} v_p(x - a_0).$$

  — Pour tout entier $k \geq 2$, $a_k \in E$ et a_k minimise la valuation p-adique de $(a_k - a_{k-1}) \cdots (a_k - a_1)(a_k - a_0)$, c'est-à-dire

$$v_p(\prod_{i=0}^{k-1}(a_k - a_i)) = \min_{x\in E} v_p(\prod_{i=0}^{k-1}(x - a_i)).$$

1. Soit $\underline{a} = (a_n)_{n\in\mathbf{N}}$ une suite p-ordonnée de E. Démontrer que pour un entier naturel k strictement inférieur au cardinal de E, on a $\prod_{i=0}^{k-1}(a_k - a_i) \neq 0$.

On définit alors pour un entier k strictement inférieur au cardinal de E,

$$V_k(E, \underline{a}, p) = p^{v_p(\prod_{i=0}^{k-1}(a_k - a_i))}.$$

Dans le cas où E est un ensemble fini et k un entier supérieur ou égal au cardinal de E, on pose $V_k(E, \underline{a}, p) = 0$.

2. Démontrer que la suite des entiers naturels $\underline{\mathbf{N}} = (n)_{n\in\mathbf{N}}$, est une suite p-ordonnée de $\mathbf{Z}$.
3. En déduire que

$$k! = \prod_{p\in\mathcal{P}} V_k(\mathbf{Z}, \underline{\mathbf{N}}, p).$$

On introduit

$$\mathbf{Z}_{(p)} = \{\frac{a}{b}\ ;\ a \in \mathbf{Z}, b \in \mathbf{Z} \setminus \{0\} \mid \text{pgcd}(a, b) = \text{pgcd}(b, p) = 1\}.$$

On admet que $\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$.

4. Démontrer que $\mathbf{Z}_{(p)} = \{x \in \mathbf{Q} \mid v_p(x) \geq 0\}$. Caractériser de même $\mathbf{Z}_{(p)}^\times$ en utilisant v_p.

Soit E un sous-ensemble de $\mathbf{Z}$. On rappelle qu'on a défini au début du problème

$$\mathrm{Ent}(E,\mathbf{Z}_{(p)})=\{P\in\mathbf{Q}[X]\mid P(E)\subseteq\mathbf{Z}_{(p)}\}\text{ et }\mathrm{Ent}_n(E,\mathbf{Z}_{(p)})=\{P\in\mathbf{Q}_n[X]\mid P(E)\subseteq\mathbf{Z}_{(p)}\},$$

pour tout entier naturel n.

5. On suppose **dans cette question uniquement** que l'ensemble E est infini. Soit $\underline{a}=(a_n)_{n\in\mathbf{N}}$ une suite d'éléments distincts deux à deux de E. On introduit, pour tout $n\in\mathbf{N}^*$,
$$P_n(X)=\prod_{j=0}^{n-1}\frac{X-a_j}{a_n-a_j}.$$
On définit $P_0(X)=1$.
   (a) Démontrer que, si la suite $\underline{a}$ est p-ordonnée, alors $P_n\in\mathrm{Ent}(E,\mathbf{Z}_{(p)})$ pour tout $n\in\mathbf{N}$.
   (b) Démontrer que $\underline{a}$ est une suite p-ordonnée si et seulement si, la suite $(P_k(X))_{k\in\mathbf{N}}$ forme une base régulière de $\mathrm{Ent}(E,\mathbf{Z}_{(p)})$.
   (c) En déduire que la valeur $V_k(E,\underline{a},p)$ ne dépend pas de la suite $\underline{a}$, pour tout entier naturel k.
6. Expliquer comment généraliser ces résultats au cas où E est un ensemble fini.

Désormais, pour p un nombre premier et k un entier naturel, on note $V_k(E,p)=V_k(E,\underline{a},p)$, pour toute suite p-ordonnée $\underline{a}$ de E.

7. Soit P un polynôme de $\mathbf{Q}[X]$. On note d son degré. Soit p un nombre premier. Soit (a_n) une suite p-ordonnée de E. Démontrer que
$$P\in\mathrm{Ent}(E,\mathbf{Z}_{(p)})\text{ si et seulement si }\forall i\in\{0,\cdots,d\},\ P(a_i)\in\mathbf{Z}_{(p)}.$$
On pourra commencer par traiter le cas où E est infini.
8. Soit k un entier naturel.
   (a) Soient $b_0,...,b_k$ des éléments de E. Justifier que si p ne divise pas $\prod_{0\leq i<j\leq k}(b_j-b_i)$ alors $V_k(E,p)=1$.
   (b) En déduire qu'il n'y a qu'un nombre fini de nombres premiers p tels que $V_k(E,p)\notin\{0,1\}$.

A l'instar de la factorielle sur l'ensemble des entiers naturels, on peut donc définir la *factorielle généralisée* du nombre k sur un sous-ensemble E de $\mathbf{Z}$ par

$$k!_E=\prod_{p\in\mathcal{P}}V_k(E,p).$$

9. Démontrer que $\{m\in\mathbf{Z}\mid m\ \mathrm{Ent}_k(E,\mathbf{Z})\subseteq\mathbf{Z}[X]\}$ est un idéal de $\mathbf{Z}$.

On note alors $\overline{k!_E}$ le générateur positif ou nul de l'idéal $\{m\in\mathbf{Z}\mid m\ \mathrm{Ent}_k(E,\mathbf{Z})\subseteq\mathbf{Z}[X]\}$.

10. On se propose de démontrer que $k!_E=\overline{k!_E}$.
   (a) Traiter le cas où E est fini et k est supérieur ou égal au cardinal de E.
   (b) On suppose que k est strictement inférieur au cardinal de E.

i. On suppose qu'il existe une suite $\underline{a}$ de E qui est p-ordonnée pour tout nombre premier p. Démontrer que $k!_E = \overline{k!_E}$.

ii. Dans le cas général, on se donne, pour tout p diviseur premier de $k!_E$, une suite $\underline{a^{(p)}} = (a_n^{(p)})_{n\in\mathbf{N}}$ p-ordonnée de E. Justifier l'existence d'une suite d'entiers $\underline{u} = (u_n)_{n\in\mathbf{N}}$ telle que : u_n est congru à $a_n^{(p)}$, modulo $V_k(E,p)$, pour tout p diviseur premier de $k!_E$.

iii. En déduire que $k!_E = \overline{k!_E}$.

11. Soit $E = \{n^2 \ ; \ n \in \mathbf{N}\}$.

(a) Démontrer que, pour tout $n \in \mathbf{N}$,

$$\prod_{k=0}^{n-1} \frac{X-k^2}{n^2-k^2} \in \mathrm{Ent}(E, \mathbf{Z}).$$

(b) En déduire

$$\forall n \in \mathbf{N}, n!_E = \frac{1}{2}(2n)!.$$

12. Soit q un entier supérieur ou égal à 2. Soit $E = \{q^n \ ; \ n \in \mathbf{N}\}$.

(a) Soit $n \in \mathbf{N}^*$. Démontrer que, pour tout $m \in \mathbf{N}$,

$$\frac{(q^m-1)(q^m-q)\cdots(q^m-q^{n-1})}{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})} \in \mathbf{N}.$$

Indication : On pourra commencer par traiter le cas où q est une puissance d'un nombre premier.

(b) En déduire que $(q^n)_{n\in\mathbf{N}}$ est une suite p-ordonnée pour tout nombre premier p.

(c) En déduire que, pour tout $n \in \mathbf{N}$,

$$n!_E = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\cdots(q-1).$$

IV Conclusions

Dans toute la section, E désigne un sous-ensemble non vide de $\mathbf{Z}$.
On donne les notations suivantes pour $P \in \mathbf{Z}[X]$:

— $d(E,P) = \mathrm{pgcd}(P(z) \ ; \ z \in E)$,

— $C(P)$ désigne le pgcd des coefficients de P.

1. Soit $\underline{a} = (a_n)_{n\in\mathbf{N}}$ une suite de E. On définit les polynômes $P_0(X) = 1$ et pour tout $n \in \mathbf{N}^*$,

$$P_n(X) = (X-a_0)(X-a_1)\cdots(X-a_{n-1}).$$

Soit P un polynôme dans $\mathbf{Z}[X]$; on note k son degré.

(a) Démontrer qu'il existe des entiers $\lambda_0, \cdots, \lambda_k$ uniques tels que

$$P(X) = \sum_{i=0}^{k} \lambda_i P_i(X).$$

(b) Démontrer qu'on a alors $C(P) = \text{pgcd}(\lambda_0, \cdots, \lambda_k)$.

(c) Soit p un nombre premier tel que la suite $\underline{a}$ est p-ordonnée. Soit m un entier naturel non nul. Démontrer l'équivalence des assertions :

i. $\forall z \in E$, p^m divise $P(z)$.

ii. $\forall i \in \{0, 1, ..., k\}$, $\forall z \in E$, p^m divise $\lambda_i P_i(z)$.

2. Soit k un entier naturel.

(a) Démontrer que si P est un polynôme de $\mathbf{Z}[X]$ de degré k tel que $C(P) = 1$ alors $d(E, P)$ divise $k!_E$.

(b) Réciproquement, démontrer qu'il existe un polynôme U dans $\mathbf{Z}[X]$, de degré k, tel que $C(U) = 1$ et $d(E, U) = k!_E$. On pourra s'inspirer de la question 10(b)ii de la partie III.

3. En déduire que, pour tous $k, l \in \mathbf{Z}$ $k!_E l!_E$ divise $(k + l)!_E$.

4. Soit F un sous-ensemble de E. Soit $k \in \mathbf{N}$. Démontrer que $k!_E$ divise $k!_F$.

5. (a) Soit n un entier naturel au moins égal à 2 et soient $a_0, ..., a_n$ des éléments de E. Démontrer que

$$0!_E 1!_E \cdots n!_E \text{ divise } \prod_{0 \leq i < j \leq n} (a_j - a_i).$$

(b) En déduire que pour tous entiers $a_0, \cdots, a_n$,

$$\prod_{0 \leq i < j \leq n} (a_j - a_i) \text{ est divisible par } 1!2! \cdots n!.$$

6. (a) On reprend les notations de la question 1 de cette partie. Soit p un nombre premier tel que la suite $\underline{a}$ est p-ordonnée. Soit m un entier naturel non nul. Démontrer l'équivalence des assertions :

i. $\forall z \in E$, p^m divise $P(z)$.

ii. $\forall i \in \{0, 1, ..., k\}$, λ_i est un multiple de $\dfrac{p^m}{\text{pgcd}(p^m, k!_E)}$.

(b) Soit n un entier naturel non nul. On appelle fonction polynomiale de E dans $\mathbf{Z}/n\mathbf{Z}$ une fonction f de E dans $\mathbf{Z}/n\mathbf{Z}$ telle qu'il existe un polynôme P dans $\mathbf{Z}[X]$ tel que pour tout x dans E, $P(x)$ modulo n est égal à $f(x)$.

i. Démontrer que le nombre de fonctions polynomiales de E dans $\mathbf{Z}/n\mathbf{Z}$ est donné par la formule suivante :

$$\prod_{k=0}^{n-1} \frac{n}{\text{pgcd}(n, k!_E)}.$$

ii. En déduire que le nombre de fonctions polynomiales de $\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ est

$$\prod_{k=0}^{n-1} \frac{n}{\text{pgcd}(n, k!)}.$$