CORRIGÉ DU DM n°1 : CAPES externe 2002

Polynômes prenant des valeurs particulières sur certaines parties

Préambule :

En tant que tels, les polynômes à valeurs entières ont été considérés pour la première fois par G. Pôlya et A. Ostrowski dans un article de 1919 : étant donné un corps de nombres $\mathbb{K}$ d'anneau d'entiers A, il s'agissait de déterminer des bases du A-module $\{P \in \mathbb{K}[X], P(A) \subset A\}$. Depuis les années 1970, la structure d'algèbre de cet ensemble a été particulièrement étudiée. Il existe une monographie sur le sujet : *P.-J. Cahen et J.-L. Chabert, Integer-Valued Polynomials, American Mathematical Society Surveys and Monographs, t. 48, 1997.*

La notion fructueuse de suite p-ordonnée dont il est question ici a été introduite en 1997 par Manjul Bhargava, un élève d'Andrew Wiles. Bhargava a écrit un article de vulgarisation à ce propos : *The Factorial Function and Generalizations, The American Mathematical Monthly, t. 107 (2000), pp. 783-799.*

Enfin, l'algorithme donné dans ce problème, permettant de caractériser les polynômes prenant des valeurs entières sur les nombres premiers, est tiré d'un article de *J.-L. Chabert au Canadian Mathematical Bulletin [t. 39 (1996), pp. 402-407].*

Partie A :

1°) a) On a immédiatement : $L_j(X) = \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq j}} \dfrac{X - q_i}{q_j - q_i}$.

Plus précisément : L_j est un polynôme de degré m admettant les q_i $(i \neq j)$ pour racines, donc s'écrit sous la forme $\lambda \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq j}} (X - q_i)$, puis on détermine λ en écrivant $L_k(q_j) = 1$).

b) Si $P = \sum_{j=0}^{n} \lambda_j L_j$, alors $P(q_i) = \lambda_i$ pour tout i. Il en résulte que les $m+1$ polynômes L_j sont linéairement indépendants dans $\mathbb{R}[X]$, puisque si P=0, alors $\lambda_i = 0$ pour tout i.
Puisque $\dim(\mathbb{R}_m[X]) = m+1$, il s'agit bien d'une base de $\mathbb{R}_m[X]$.

c) Le calcul ci-dessus donne : $P = \sum_{j=01}^{n} P(q_j) L_j$.

d) Soit $P \in \mathcal{P}(\mathbb{Q},\mathbb{Q})$, non nul, et m le degré de P. Soient alors $q_0, q_1, \dots q_m$, $m+1$ *rationnels* distincts. On a alors $L_j \in \mathbb{Q}[X]$ et $P(q_j) \in \mathbb{Q}$ pour tout j, donc $P \in \mathbb{Q}[X]$.
Réciproquement, il est immédiat que, si $P \in \mathbb{Q}[X]$, alors $P \in \mathcal{P}(\mathbb{Q},\mathbb{Q})$.
Finalement : $\boxed{\mathcal{P}(\mathbb{Q},\mathbb{Q}) = \mathbb{Q}[X]}$.

2°) a) $(a^2+b^2)(c^2+d^2) = |(a+ib)(c+id)|^2 = |x+iy|^2$ où $x = ac - bd$ et $y = ad + bc.$, soit $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$.

b) L'identité obtenue $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$ (dite de Brahmagupta) reste valable dans tout anneau commutatif A : il suffit de développer les deux membres (en utilisant les règles de calcul dans un anneau commutatif) pour s'en convaincre. La stabilité de S pour la multiplication découle de la formule. Enfin, $0 = 0^2 + 0^2$ et $1 = 1^2 + 0^2$!

c) i. Si P était de degré impair, les limites de la fonction continue P en $+\infty$ et en $-\infty$ seraient infinies et de signes contraires et, d'après le théorème des valeurs intermédiaires, on aurait $P(\mathbb{R}) = \mathbb{R}$, ce qui est en contradiction avec l'hypothèse de l'énoncé.

ii. La décomposition de P en éléments irréductibles de $\mathbb{R}[X]$ s'écrit :

$$P = C(X-a_1)^{\alpha_1}...(X-a_r)^{\alpha_r}[(X-p_1)^2+q_1^2]^{\beta_1}...[(X-p_s)^2+q_s^2]^{\beta_s}$$

Puisque P est non nul et à valeurs positives, on a $C > 0$ (par ex. en considérant la limite en $+\infty$). Comme P ne doit pas changer de signe en a_i, les α_i sont nécessairement pairs.
Ainsi, $C = (\sqrt{C})^2 + 0^2$, $(X-a_i)^{\alpha_i} = [(X-a_i)^{\frac{\alpha_i}{2}}]^2 + 0^2$ et P est le produit de sommes de carrés dans $\mathbb{R}[X]$, donc est lui-même une somme de carrés dans $\mathbb{R}[X]$ d'après la question précédente.
Par suite, $\mathcal{P}(\mathbb{R},\mathbb{R}_+)$ est contenu dans l'ensemble des sommes de deux carrés de polynômes. Mais la réciproque est évidente et donc

$$\mathcal{P}(\mathbb{R},\mathbb{R}_+) = \{A^2 + B^2,\ A,B \in \mathbb{R}[X]\}$$

3°) a) Comme la fonction polynôme associée à $P \in \mathbb{R}[X]$ est continue, $P(\mathbb{Q}) \subset \mathbb{Q}_+$ implique $P(\mathbb{R}) \subset \mathbb{R}_+$, puisque tout réel est limite d'une suite de rationnels. (*donc P est somme de deux carrés de polynômes à coefficients réels, mais on ne peut pas toujours trouver deux tels polynômes à coefficients rationnels, comme le montre le contre-exemple ci-après.*)

b) i. $2X^2+4 = (\sqrt{2}X)^2 + 2^2 = (X-\sqrt{2})^2 + (X+\sqrt{2})^2$.

ii. L'égalité $2X^2+4 = (aX+b)^2 + (cX+d)^2$ donne facilement le système :

$$\begin{cases} \left(\dfrac{a}{\sqrt{2}}\right)^2 + \left(\dfrac{c}{\sqrt{2}}\right)^2 & = 1 \qquad (1) \\ \left(\dfrac{a}{\sqrt{2}}\right)\left(\dfrac{b}{2}\right) + \left(\dfrac{c}{\sqrt{2}}\right)\left(\dfrac{d}{2}\right) & = 0 \qquad (2) \\ \left(\dfrac{b}{\sqrt{2}}\right)^2 + \left(\dfrac{d}{\sqrt{2}}\right)^2 & = 1 \qquad (3) \end{cases}$$

D'après (1) et (3), on peut poser : $a = \sqrt{2}\cos\vartheta$, $c = \sqrt{2}\sin\vartheta$ et $b = 2\cos\vartheta'$, $d = 2\sin\vartheta'$; dans ce cas, la relation (2) implique $\sin(\vartheta+\vartheta') = 0$, d'où $\vartheta' = -\vartheta$ modulo π, ce qui donne les relations demandées.
La conclusion est immédiate : si a,b,c,d étaient quatre rationnels non nuls, $\sqrt{2}$ serait rationnel...

iii. Si on avait $2X^2+4 = A^2+B^2$, avec $A,B \in \mathbb{Q}[X]$, alors nécessairement $\deg A \leqslant 1$ et $\deg B \leqslant 1$; d'après ce qui précède, cela est impossible.

Partie B :

1°) a) Soit $k \in \mathbb{Z}$.
- Pour $0 \leqslant k < n$, $\Gamma_n(k) = 0$;

• Pour $k \geqslant n$, $\Gamma_n(k) = \binom{k}{n}$;

• Pour $k < 0$, $\Gamma_n(k) = (-1)^n \binom{n-k-1}{n}$.

Dans tous les cas, on a bien : $\Gamma_n(k) \in \mathbb{Z}$, donc $\underline{\Gamma_n \text{ appartient à } \mathcal{P}(\mathbb{Z},\mathbb{Z})}$.

b) $\deg(\Gamma_n) = n$ donc la famille $(\Gamma_n)_{0 \leqslant n \leqslant m}$ est une famille de polynômes de degrés échelonnés de 0 à m, c'est donc une base de $\mathbb{R}_m[X]$.

2°) Compte tenu des calculs précédents, on a facilement :

$$\left\{\begin{array}{lcl} P(0) & = & d_0 \\ P(1) & = & d_0 + d_1 \\ P(2) & = & d_0 + \binom{2}{1} d_1 + d_2 \\ P(3) & = & d_0 + \binom{3}{1} d_1 + \binom{3}{2} d_2 + d_3 \\ \ldots & = & \ldots \\ P(m) & = & d_0 + \binom{m}{1} d_1 + \binom{m}{2} d_2 + \ldots + \binom{m}{m-1} d_{m-1} + d_m \end{array}\right.$$

3°) • $(i) \Rightarrow (iii)$ est évident.

• $(iii) \Rightarrow (ii)$: Les d_j s'obtiennent à l'aide du système précédent. En remarquant que tous les coefficients diagonaux sont égaux à 1, il est facile de montrer par récurrence que, si $P(0),P(1),\ldots,P(m) \in \mathbb{Z}$, les d_j appartiennent aussi à $\mathbb{Z}$.

• $(ii) \Rightarrow (i)$: puisque $\Gamma_n \in \mathcal{P}(\mathbb{Z},\mathbb{Z})$ pour tout $n \in \mathbb{N}$, que $d_n \in \mathbb{Z}$ pour $0 \leqslant n \leqslant m$ et que $P = \displaystyle\sum_{0 \leqslant n \leqslant m} d_n \Gamma_n$, on a $P \in \mathcal{P}(\mathbb{Z},\mathbb{Z})$.

• $(iii) \Rightarrow (iv)$ est évident.

• $(iv) \Rightarrow (iii)$: Soit $a \in \mathbb{Z}$ tel que $P(a),P(a+1),\ldots,P(a+m) \in \mathbb{Z}$; alors le polynôme $Q(X) = P(a+X)$ vérifie $Q(0),Q(1),\ldots,Q(m) \in \mathbb{Z}$. D'après ce qui précède, $Q \in \mathcal{P}(\mathbb{Z},\mathbb{Z})$, et donc, pour tout $k \in \mathbb{Z}$, $P(k) = Q(k-a) \in \mathbb{Z}$.

4°) **a)** $P(0) = -120$; $P(1) = P(2) = P(3) = P(4) = P(5) = 0$; la résolution du système précédent donne $d_n = (-1)^n 120$ pour $n \in [\![1,5]\!]$; et, facilement :
$P = (X-1)(X-2)(X-3)(X-4)(X-5)$.

b) $P(n) = 0$ pour $1 \leqslant n \leqslant m$ (en remplaçant les d_j par leurs valeurs $(-1)^j$ dans le système précédent et compte tenu de la formule du binôme). De plus, $\deg(P) \leqslant m$ et le coefficient dominant de P est celui de $(-1)^m \Gamma_m$. On a donc :

$$P = \frac{(-1)^m}{m!}(X-1)(X-2)\ldots(X-m) \ = \ (-1)^m \Gamma_m(X-1)$$

Partie C :

1°) **a)** L'existence de k se déduit de la décomposition de a et b en facteurs premiers; l'unicité résulte du fait que : si $p^k \dfrac{a}{b} = p^{k'} \dfrac{a'}{b'}$ avec $a,a',b,b' \in \mathbb{Z} \setminus p\mathbb{Z}$ et $k \neq k'$ on a une contradiction : si par exemple $k > k'$, on a $p^{k-k'} ab' = a'b$ d'où p divise $a'b$ donc devrait apparaître dans la décomposition en facteurs premiers de a' ou de b...

b) (i) Pour tout $k \in \mathbb{Z}$, $v_p(p^k) = k$ donc tout $k \in \mathbb{Z}$ appartient à l'image de v_p.

(ii) Les cas $x = 0$ ou $y = 0$ sont triviaux. Si $xy \neq 0$, $x = p^k \dfrac{a}{b}$, $y = p^{k'} \dfrac{a'}{b'}$ avec $a,a',b,b' \in \mathbb{Z} \setminus p\mathbb{Z}$, alors $xy = p^{k+k'} \dfrac{aa'}{bb'}$ où aa' et bb' ne sont pas multiples de p (pour la même raison que ci-dessus).

(iii) Les cas $x = 0$ ou $y = 0$ sont triviaux (puisque l'on a posé $v_p(0) = +\infty$). Supposons $xy \neq 0$. Avec les mêmes notations que ci-dessus, supposons par exemple, $k \leqslant k'$. Alors : $x + y = p^k \dfrac{ab' + p^{k'-k}a'b}{bb'}$. bb' n'est pas divisible par p; si $k < k'$, $ab' + p^{k'-k}a'b$ n'est pas divisible par p (car sinon ab' le serait), donc, dans ce cas, $\mathrm{v}_p(x + y) = k$; si $k = k'$, $ab' + a'b$ *peut* être divisible par p; on a en tout cas $v_p(x + y) \geqslant k$.
Ainsi, on a toujours $v_p(x + y) \geqslant \min\{v_p(x),v_p(y)\}$ (avec égalité si $v_p(x) \neq v_p(y)$).

c) $v_p(1) = v_p(-1) = 0$. Si $y \neq 0$, $v_p(x) = v_p\left(\dfrac{x}{y}.y\right) = v_p\left(\dfrac{x}{y}\right) + v_p(y)$ d'après la question précédente, d'où : $v_p\left(\dfrac{x}{y}\right) = v_p(x) - v_p(y)$.

d) • Soit $x \in \mathbb{Q}^*$ et $\dfrac{c}{d}$ une représentation irréductible de x. Alors $v_p(x) = v_p(c) - v_p(d)$, où $v_p(c)$ et $v_p(d)$ sont des entiers naturels dont l'un au moins est nul (car, si p divise c, par exemple, il ne peut diviser d puisque c et d sont premiers entre eux). Il est alors immédiat que : $v_p(x) \geqslant 0 \Leftrightarrow v_p(d) = 0 \Leftrightarrow x \in \mathbb{Z}_{(p)}$.
• $1 \in \mathbb{Z}_{(p)}$; la question C.1.b.(ii) montre que $\mathbb{Z}_{(p)}$ est stable pour le produit; $-1 \in \mathbb{Z}_{(p)}$ et la question C.1.b.(iii) montrent que $\mathbb{Z}_{(p)}$ est stable pour la différence ; donc $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$.
• Si $x \in \mathbb{Z}_{(p)}$ est inversible, il existe $y \in \mathbb{Z}_{(p)}$ tel que $xy = 1$; alors $v_p(x)+v_p(y) = v_p(1) = 0$, et $v_p(x) \geqslant 0$, $v_p(y) \geqslant 0$ impliquent $v_p(x) = 0$.
Réciproquement, si $v_p(x) = 0$, $v_p\left(\dfrac{1}{x}\right) = v_p(1) - v_p(x) = 0$, donc $\dfrac{1}{x} \in \mathbb{Z}_{(p)}$ et x est inversible dans $\mathbb{Z}_{(p)}$.

e) Pour tout entier $q > 0$, $\left\lfloor \dfrac{n}{p} \right\rfloor$ compte les multiples de p compris entre 1 et n. Ainsi, $\left\lfloor \dfrac{n}{p^k} \right\rfloor - \left\lfloor \dfrac{n}{p^{k+1}} \right\rfloor$ compte le nombre d'entiers j compris entre 1 et n divisibles par p^k et non par p^{k+1}, c'est-à-dire tels que $v_p(j) = k$. Pour $n \geqslant 1$,

$$v_p(n!) = \sum_{j=1}^{n} v_p(j) = \sum_{k>0} k \left\{ \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right\} = \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor$$

(en regroupant dans la première somme les termes tels que $v_p(j) = k$)
(ces sommes étendues à tout $k > 0$ sont en fait finies...)

2°) a) Si $\dfrac{a}{b} \in \bigcap_{l \in \mathbb{P}} \mathbb{Z}_{(l)}$, alors, pour tout $l \in \mathbb{P}$, $v_l(a) - v_l(b) = v_l\left(\dfrac{a}{b}\right) \geqslant 0$; ainsi, la décomposition de a et b en facteurs premiers montre que b divise a dans $\mathbb{Z}$, et donc $\dfrac{a}{b} \in \mathbb{Z}$. La réciproque est claire.

b) Pour tout $l \in \mathbb{P}$, $\mathbb{Z} \subset \mathbb{Z}_{(l)}$, d'où $\mathcal{P}(E,\mathbb{Z}) \subset \mathcal{P}(E,\mathbb{Z}_l)$ puis $\mathcal{P}(E,\mathbb{Z}) \subset \bigcap_{l \in \mathbb{P}} \mathcal{P}(E,\mathbb{Z}_l)$.

Réciproquement, soit $P \in \bigcap_{l \in \mathbb{P}} \mathcal{P}(E,\mathbb{Z}_l)$. Si $x \in E$, alors $P(x) \in \bigcap_{l \in \mathbb{P}} \mathbb{Z}_{(l)} = \mathbb{Z}$, d'où

$P \in \mathcal{P}(E,\mathbb{Z})$.

3°) **a)** En prenant $n=1$ dans la définition d'une suite 3-ordonnée, on obtient $v_p(u_1) = \min_{x\in E} v_3(x) = 0$ d'où $u_1 = 1$; puis, en prenant $n=2$: $v_3(u_2(u_2-1)) = \min_{x\in E} v_3(x(x-1)) = 1$ d'où $v_3(u_2)+v_3(u_2-1) = 1$ d'où $u_2 = 3k$ avec $k \in \mathbb{N}\setminus 3\mathbb{N}$.

b) Soit $n\in\mathbb{N}^*$ et $x\in\mathbb{Z}$. $\prod_{k=0}^{n-1}(x-k) = n!\Gamma_n(x)$ d'où $v_p\left(\prod_{k=0}^{n-1}(x-k)\right) = v_p(n!)+v_p(\Gamma_n(x)) \geqslant v_p(n!)$ puisque $\Gamma_n(x)\in\mathbb{Z}$. Ainsi, pour tout $n\in\mathbb{N}^*$ et tout $x\in\mathbb{Z}$, on a bien
$v_p\left(\prod_{k=0}^{n-1}(n-k)\right) \leqslant v_p\left(\prod_{k=0}^{n-1}(x-k)\right)$; l'égalité étant réalisée pour $x=n$, on a bien:
$v_p\left(\prod_{k=0}^{n-1}(n-k)\right) = \min_{x\in\mathbb{Z}} v_p\left(\prod_{k=0}^{n-1}(x-k)\right)$, ce qui prouve ce qui était demandé.

c) On peut construire une suite (u_n)convenable par récurrence. En effet, posons $u_0 = a$ et supposons (hypothèse de récurrence $(\mathcal{H}_{n-1})$) que u_0,...,u_{n-1} soient des éléments distincts de E tels que:
$v_p\left(\prod_{j=0}^{k-1}(u_k-u_j)\right) = \min_{x\in E} v_p\left(\prod_{j=0}^{k-1}(x-u_j)\right)$ pour tout $k\in[\![1,n-1]\!]$.
Puisque E est infini, l'ensemble $E\setminus\{u_0,\ldots,u_{n-1}\}$ est non vide, donc l'ensemble
$\left\{v_p\left(\prod_{k=0}^{n-1}(x-u_k)\right), x\in E\setminus\{u_0,\ldots,u_{n-1}\}\right\}$ est un sous-ensemble non vide de $\mathbb{N}$; il admet donc un plus petit élément, obtenu pour un certain $x\in E\setminus\{u_0,\ldots,u_{n-1}\}$; on posera alors $u_n = x$, et $(\mathcal{H}_n)$ est bien vérifiée. La suite $(u_n)_{n\in\mathbb{N}}$ ainsi construite est bien p-ordonnée.
Il n'y pas unicité en général comme le montre C.3.a.

4°) **a)** i. La suite (u_n) étant p-ordonnée, on a:
$\forall x\in E$, $v_p(P_n(x)) = v_p\left(\prod_{k=0}^{n-1}(x-u_k)\right) - v_p\left(\prod_{k=0}^{n-1}(u_n-u_k)\right) \geqslant 0$. Ainsi, P_n appartient à $\mathcal{P}(E,\mathbb{Z}_{(p)})$.

ii. Il s'agit d'une famille de polynômes de degrés échelonnés de 0 à m...

iii. $P_n(u_k) = \delta_{k,n}$ pour $0\leqslant k\leqslant n$.

b) • $(ii) \Rightarrow (i)$ Soit $x\in E$. Alors, pour tout $k\in\mathbb{N}$, $P_k(x)\in\mathbb{Z}_{(p)}$. Or $c_k\in\mathbb{Z}_{(p)}$ donc $c_kP_k(x)\in\mathbb{Z}_{(p)}$ puis $\sum_{n=0}^{m} c_nP_n(x)\in\mathbb{Z}_{(p)}$, puisque $\mathbb{Z}_{(p)}$ est un anneau. Ainsi, $P\in\mathcal{P}(E,\mathbb{Z}_{(p)})$.

• $(i)\Rightarrow(iii)$ est facile, puisque les u_k sont dans E !
• $(iii)\Rightarrow(ii)$ Se démontre comme dans B.3: on écrit le système qui exprime les $P(u_j)$ $(0\leqslant j\leqslant m)$ en fonction des c_n et des $P_n(u_j)$. D'après ce qui précède, ce système est triangulaire, à coefficients dans $\mathbb{Z}_{(p)}$, et dont les coefficients diagonaux sont égaux à 1. Les c_n peuvent donc s'exprimer comme combinaisons linéaires à coefficients dans $\mathbb{Z}_{(p)}$ des $P(u_j)$ qui appartiennent aussi à $\mathbb{Z}_{(p)}$; puisque $\mathbb{Z}_{(p)}$ est un anneau, les c_n appartiennent aussi à $\mathbb{Z}_{(p)}$.

c) • On remarque que, pour $0 \leqslant n \leqslant m$,

$$\begin{aligned}
\omega(n) &= v_p\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) \\
&\leqslant v_p\left(\prod_{k=0}^{n-1}(u_m - u_k)\right) \\
&\leqslant v_p\left(\prod_{k=0}^{n-1}(u_m - u_k)\right) + v_p\left(\prod_{k=n}^{m-1}(u_m - u_k)\right) = \omega(m)
\end{aligned}$$

Par suite, $p^{\omega(m)}P_n(X) = p^{\omega(m)-\omega(n)}\dfrac{p^{\omega(n)}}{\prod_{k=0}^{n-1}(u_n - u_k)}\prod_{k=0}^{n-1}(X - u_k)$ est à coefficients dans $\mathbb{Z}_{(p)}$, car le facteur central est un élément inversible de $\mathbb{Z}_{(p)}$ (sa valuation p.r à p est nulle). Ainsi, si $P \in \mathcal{P}(E,\mathbb{Z}_{(p)})$, $p^{\omega(m)}P = \sum_{n=0}^{m} c_n p^{\omega(m)}P_n$ est aussi à coefficients dans $\mathbb{Z}_{(p)}$.

• Cela implique que les coefficients de P sont rationnels, donc $\mathcal{P}(E,\mathbb{Z}_{(p)}) \subset \mathbb{Q}[X]$. Le fait que $\mathcal{P}(E,\mathbb{Z}_{(p)})$ est un sous-anneau de $\mathbb{Q}[X]$ résulte facilement du fait que $\mathbb{Z}_{(p)}$ est un anneau.

Partie D :

1°) **a)** La division euclidienne de n par $p-1$ s'écrit $n = (p-1)q + r$ avec $0 \leqslant r < p-1$. Alors $q = \left\lfloor \dfrac{n}{p-1} \right\rfloor$, et, d'autre part, $\varphi_p(n) = n + 1 + q = qp + r + 1$ avec $0 < r+1 < p$, donc $\left\lfloor \dfrac{\varphi_p(n)}{p} \right\rfloor = q$ et $\varphi_p(n) \in \mathbb{N} \setminus p\mathbb{N}$.

b) (i) On vient de voir que : $\varphi_p(\mathbb{N}) \subset \mathbb{N} \setminus p\mathbb{N}$. De plus, φ_p est strictement croissante, car $n \mapsto n+1$ l'est et que $n \mapsto \left\lfloor \dfrac{n}{p-1} \right\rfloor$ est croissante. Donc φ_p est injective.
Il reste à vérifier que φ_p est surjective de $\mathbb{N}$ *sur* $\mathbb{N} \setminus p\mathbb{N}$. Si $m \in \mathbb{N} \setminus p\mathbb{N}$, la division euclidienne de m par p s'écrit $m = lp + s$ avec $0 < s < p$; si on pose $n = (p-1)l + s - 1$, on a bien alors $m = \varphi_p(n)$.

(ii) D'après C.1.e, on a $v_p(\varphi_p(n)!) = \sum_{k>0} \left\lfloor \dfrac{\varphi_p(n)}{p^k} \right\rfloor = \sum_{k>0} \left\lfloor \dfrac{\frac{\varphi_p(n)}{p}}{p^{k-1}} \right\rfloor$. Or, on vérifie facilement, en utilisant la division euclidienne, que, pour $x \in \mathbb{R}$ et $a,b \in \mathbb{N}^*$, on a $\left\lfloor \dfrac{x}{ab} \right\rfloor = \left\lfloor \dfrac{\lfloor \frac{x}{a} \rfloor}{b} \right\rfloor$.
D'où, à l'aide de D.1.a, $v_p(\varphi_p(n)!) = \sum_{k>0} \left\lfloor \dfrac{n}{(p-1)p^{k-1}} \right\rfloor = \omega_p(n)$.

c) (i) $\omega_p(n) = \sum_{k\geqslant 0} \left\lfloor \dfrac{n}{(p-1)p^k} \right\rfloor \leqslant \sum_{k=0}^{+\infty} \dfrac{n}{(p-1)p^k} = \dfrac{pn}{(p-1)^2}$ (somme des termes d'une série géométrique) d'où facilement $\omega_p(n) \leqslant 2n$.

(ii) La formule précédente montre immédiatement que si $n < p-1$, alors $\omega_p(n) = 0$.

2°) **a)** Pour $s \in \mathbb{N}$, $\varphi_p(s) \in \mathbb{N} \setminus p\mathbb{N}$, donc p ne divise pas $\varphi_p(s)$. Donc, si p divise r, il ne divise pas $(r - \varphi_p(s))$, i.e $v_p(r - \varphi_p(s)) = 0$.

b) Lorsque k varie de 0 à $n-1$, $\varphi_p(k)$ décrit l'ensemble des entiers non divisibles par p et compris entre 0 et $\varphi_p(n) - 1$, d'après D.1.a . Ainsi, les deux produits de l'énoncé diffèrent par des facteurs de la forme $\varphi_p(n) - r$ où r est multiple de p, ce qui ne change pas la valeur de v_p d'après la question précédente. D'où l'égalité demandée (la dernière des deux égalités étant évidente, puisque $\displaystyle\prod_{r=0}^{\varphi_p(n)-1} (\varphi_p(n) - r) = \varphi_p(n)!$).

c) La première égalité se justifie comme précédemment. La deuxième est là encore facile, puisque $\displaystyle\prod_{r=0}^{\varphi_p(n)-1} (\varphi_p(s) - r) = \frac{\varphi_p(s)!}{(\varphi_p(s) - \varphi_p(n))!}$.

d) D'après D.1.b, $\varphi_p(\mathbb{N}) = \mathbb{N} \setminus p\mathbb{N}$. La suite $(\varphi_p(n))_{n\in\mathbb{N}}$ vérifie bien la condition demandée : soit $s \in \mathbb{N}$;

- si $0 \leqslant s < n$, alors $v_p\left(\displaystyle\prod_{k=0}^{n-1} (\varphi_p(s) - \varphi_p(k))\right) = \infty \;\geqslant\; v_p\left(\displaystyle\prod_{k=0}^{n-1} (\varphi_p(n) - \varphi_p(k))\right)$
- si $s \geqslant n$,

$$\begin{aligned} v_p\left(\prod_{k=0}^{n-1} (\varphi_p(s) - \varphi_p(k))\right) &= v_p\left(\frac{\varphi_p(s)!}{(\varphi_p(s) - \varphi_p(n))!}\right) \\ &\geqslant v_p(\varphi_p(n)!) = v_p\left(\prod_{k=0}^{n-1} (\varphi_p(n) - \varphi_p(k))\right) \end{aligned}$$

3°) **a)** C'est une application de C.4.b dans le cas particulier où $E = \mathbb{N} \setminus p\mathbb{N}$ et $u_n = \varphi_p(n)$.

b) C'est une application de C.4.c dans le cas particulier précédent avec $\omega(n) = \omega_p(n)$ car, d'après D.2.b et D.1.b,

$$v_p\left(\prod_{k=0}^{n-1} (\varphi_p(n) - \varphi_p(k))\right) = v_p(\varphi_p(n)!) = \omega_p(n)$$

Partie E :

1°) • $\Gamma_4 \in \mathcal{P}(\mathbb{Z},\mathbb{Z}) \subset \mathcal{P}(\mathbb{P},\mathbb{Z})$

• Donc, pour tout $p \in \mathbb{P}$, $24 \big| p(p-1)(p-2)(p-3)$. Si $p \neq 2{,}3$, alors 24 est premier avec p donc $24 \big| (p-1)(p-2)(p-3)$. Et ce résultat subsiste pour $p = 2$ ou 3. Donc $\dfrac{(X-1)(X-2)(X-3)}{24}$ appartient à $\mathcal{P}(\mathbb{P},\mathbb{Z})$.

• Mais le polynôme ci-dessus n'appartient pas à $\mathcal{P}(\mathbb{Z},\mathbb{Z})$ (prendre par ex. sa valeur en 4).

2°) **a)** i. Posons $Q(X) = \displaystyle\sum_{n=0}^{m} b_n X^n$. On a :

$$Q(a + kp^\alpha) - Q(a) = \sum_{n=1}^{m} b_n[(a + kp^\alpha)^n - a^n] = \sum_{n=1}^{m} b_n k p^\alpha \sum_{i=0}^{n-1} -a + kp^\alpha)^i a^{n-i-1}.$$

Par hypothèse, $b_n p^\alpha \in \mathbb{Z}_{(p)}$, et, dans la somme ci-dessus, $b_n p^\alpha$ est multiplié par un entier. $\mathbb{Z}_{(p)}$ étant un anneau, on a donc bien que $Q(a + kp^\alpha) - Q(a)$ appartient à $\mathbb{Z}_{(p)}$.

ii. Soit a un élément de $\mathbb{N} \setminus p\mathbb{N}$. Alors a et p^α sont premiers entre eux, et, d'après le th. de Dirichlet, il existe $k \in \mathbb{N}^*$ tel que $a + kp^\alpha \in \mathbb{P}$, et donc tel que $Q(a + kp^\alpha) \in \mathbb{Z}_{(p)}$ (d'après l'hypothèse sur Q).

iii. Compte tenu de i. et ii., on a alors $Q(a) = [Q(a)-Q(a+kp^\alpha)]+Q(a+kp^\alpha) \ \in \mathbb{Z}_{(p)}$.Cela étant valable pour tout $a \in \mathbb{N} \setminus p\mathbb{N}$, on a bien $Q(\mathbb{N} \setminus p\mathbb{N}) \subset \mathbb{Z}_{(p)}$.

b) i. Si $q \in \mathbb{P} \setminus \{p\}$, alors $q \in \mathbb{N} \setminus p\mathbb{N}$ d'où $\mathbb{P} \subset E_p$.

ii. D'où l'inclusion :$\mathcal{P}(E_p,\mathbb{Z}_{(p)}) \subset \mathcal{P}(\mathbb{P},\mathbb{Z}_{(p)})$, et E.2.a donne l'inclusion inverse.

iii. D'après C.2.a, $\mathcal{P}(\mathbb{P},\mathbb{Z}) = \cap_{l\in\mathbb{P}}\mathcal{P}(\mathbb{P},\mathbb{Z}_{(l)}) = \cap_{l\in\mathbb{P}}\mathcal{P}(E_l,\mathbb{Z}_{(l)})$.

3°) Soit $Q \in \mathcal{P}(\mathbb{P},\mathbb{Z})$ de degré $\leqslant m$. Alors, pour tout $p \in \mathbb{P}$, on a $Q(p) \in \mathbb{Z}$, $Q(\mathbb{N} \setminus p\mathbb{N}) \subset \mathbb{Z}_{(p)}$ (d'après E.2.a) et les coefficients de $p^{2m}Q$ appartiennent à $\mathbb{Z}_{(p)}$ (d'après D.3.b et D.1.c.i).
Soit $x \in \mathbb{N}$, alors, ou bien $x \in \mathbb{N} \setminus p\mathbb{N}$ et alors $Q(x) \in \mathbb{Z}_{(p)}$, ou bien x multiple de p, et alors $x^{2m}Q(x) \in \mathbb{Z}_{(p)}$ (car x^{2m} est multiple de p^{2m}).
Ainsi, pour tout $x \in \mathbb{N} \setminus p\mathbb{N}$, $x^{2m}Q(x) \in \mathbb{Z}_{(p)}$; ceci ayant lieu pour tout $p \in \mathbb{P}$, $x^{2m}Q(x)$ appartient à $\mathbb{Z}$ d'après C.2.a. Ainsi, $X^{2m}Q(X) \in \mathcal{P}(\mathbb{N},\mathbb{Z})$; par suite, d'après B.3, $X^{2m}Q(X) \in \mathcal{P}(\mathbb{Z},\mathbb{Z})$.

4°) **a)** D'après D.3.a, il suffit de vérifier que, pour $p \in \mathbb{P}$ et $n \in [\![0,m]\!]$, on a : $Q(\varphi_p(n)) \ \in \ \mathbb{Z}_{(p)}$
Or, pour $0 \leqslant n \leqslant m$, $\varphi_p(n) \leqslant m+1+\dfrac{m}{p-1} \leqslant 2m+1$. L'hypothèse montre donc que, pour $0 \leqslant n \leqslant m$, $\varphi_p(n)^{2m}Q(\varphi_p(n)) \in \mathbb{Z}_{(p)}$, et comme $v_p(\varphi_p(n)) = 0$, on a bien $Q(\varphi_p(n)) \in \mathbb{Z}_{(p)}$.

b) Supposons $p > m+1$. D'après ce qui précède et D.3.b, $p^{\omega_p(m)}Q$ est à coefficients dans $\mathbb{Z}_{(p)}$. D'après D.1.c.i, $\omega_p(m) = 0$ donc, en particulier, $Q(p) \in \mathbb{Z}_{(p}$.

5°) Si $Q \in \mathcal{P}(\mathbb{P},\mathbb{Z})$, alors la 1ère condition est immédiate, et la seconde découle de E.3
Réciproquement, la seconde condition montre que, pour $p \in \mathbb{P}$, $Q(\mathbb{N} \setminus p\mathbb{N}) \in \mathbb{Z}_{(p}$ d'après E.4.a. De plus, $Q(p) \in \mathbb{Z}_{(p)}$ si $p \leqslant m+1$ et aussi, d'après E.4.b, si $p > m+1$. Dans tous les cas, $Q(E_p) \subset \mathbb{Z}_{(p)}$ et donc, d'après E.2.b, $Q \in \mathcal{P}(\mathbb{P},\mathbb{Z})$.

6°) Il s'agit de montrer que :

$$Q(X) \ = \ \frac{1}{2903040}(X+1)(X-1)(X-2)(X-3)(X-5)(X-7)(X-193)$$

appartient à $\mathcal{P}(\mathbb{P},\mathbb{Z})$. Il suffit d'appliquer la caractérisation précédente avec $m = 7$...
