Capes 2002 - Deuxième épreuve

Cette correction a été rédigée par Frédéric Bayart. Si vous avez des remarques à faire, ou pour signaler des erreurs, n'hésitez pas à écrire à : mathweb@free.fr

Mots-clés : polynômes de Lagrange,arithmétique,formules de Cramer,partie entière

Commentaires : Problème d'arithmétique pas trop difficile, mais où il faut savoir rester lucide

Partie A

A.I.1. D'abord, il n'est peut-être pas inutile de préciser qu'un tel polynôme est unique. En effet, puisqu'il est de degré au plus m, et qu'il admet m racines, à savoir les q_i, pour $j \neq i$, il s'écrit nécessairement :

$$L_j(X) = \lambda \prod_{i \neq j} (X - q_i).$$

La condition $L_j(q_j) = 1$ entraîne

$$L_j(X) = \frac{\prod_{i \neq j}(X - q_i)}{\prod_{i \neq j}(q_j - q_i)}.$$

A.I.2. Puisqu'il s'agit d'une famille de $m+1$ vecteurs dans un espace vectoriel de dimension $m+1$, il suffit de montrer que la famille est libre. En effet, si on a une égalité

$$\alpha_0 L_0 + \cdots + \alpha_m L_m = 0,$$

l'évaluation des polynômes en q_i prouve que $\alpha_i = 0$.

A.I.3. On a :

$$P = \sum_{j=0}^{m} P(q_j) L_j.$$

En effet, le polynôme à droite de cette égalité est de degré au plus m, et il coïncide avec P sur un ensemble de $m+1$ éléments. Il lui est donc égal.

A.I.4. D'où d'abord, comme $\mathbb{Q}$ est un corps, il est clair que $\mathbb{Q}[X] \subset \mathcal{P}(\mathbb{Q},\mathbb{Q})$. Réciproquement, si $P \in \mathcal{P}(\mathbb{Q},\mathbb{Q})$ est de degré m, on pose $q_0 = 1, \ldots, q_m = m$. Les polynômes de Lagrange L_j associés à cette famille sont alors dans $\mathbb{Q}[X]$. L'égalité obtenue à la question précédente implique que P appartient lui-même à $\mathbb{Q}[X]$. En conclusion :

$$\mathbb{Q}[X] = \mathcal{P}(\mathbb{Q},\mathbb{Q}).$$

A.II.1. On a, en posant $w_1 = a + ib$ et $w_2 = c + id$:

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= |w_1|^2 |w_2|^2 \\ &= |w_1 w_2|^2 \\ &= (ac-bd)^2 + (ad+bc)^2.\end{aligned}$$

A.II.2. Comme tout commute, les identités remarquables sont vérifiées dans A et la formule précédente reste valable. En particulier, S est stable pour la multiplication. Remarquons que $0 = 0^2 + 0^2$ et que $1 = 1^2 + 0^2$: $0,1 \in S$.

A.II.3.i. Si P n'est pas de degré pair, ou bien P tend vers $-\infty$ en $-\infty$, ou bien P tend vers $-\infty$ en $+\infty$ (suivant le signe du coefficient dominant). C'est impossible. P est donc de degré pair, et la constante intervenant dans sa décomposition en produit de facteurs premiers est positive. En outre, les entiers α sont pairs, car si l'un d'eux était impair, alors P s'annulerait en changeant de signe en a, et ne pourrait être toujours positif.

A.II.3.ii Nous posons pour cette question $S = \mathbb{R}[X]$. D'après la question précédente, il suffit de prouver que chaque $(X-a)^{2\gamma}$ et chaque $(X^2+bX+c)^{\beta}$ s'écrit comme somme des carrés de deux polynômes de $\mathbb{R}[X]$. Réappliquant encore A.II.2., il suffit en fait de le faire pour $(X-a)^2$ et X^2+bX+c :

- Pour $(X-a)^2$, il suffit d'écrire :

$$(X-a)^2 = (X-a)^2 + 0^2.$$

- Pour X^2+bX+c, la mise sous forme canonique convient!

A.II.3.iii Nous venons de prouver que :

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

L'inclusion réciproque est évidente.

A.III.1. Soit $P \in \mathcal{P}(\mathbb{Q},\mathbb{Q}_+)$, et $x \in \mathbb{R}$. Puisque $\mathbb{Q}$ est dense dans $\mathbb{R}$, il existe une suite (x_n) d'éléments de $\mathbb{Q}$ qui converge vers x. On a alors $P(x_n) \geq 0$, et par continuité de P, $P(x) \geq 0$. En particulier, on a $P \in \mathcal{P}(\mathbb{R},\mathbb{R}_+)$.

A.III.2.i. On a par exemple :

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

A.III.2.ii Cette matrice est orthogonale. En effet :

1. $(a/\sqrt{2})^2 + (c/\sqrt{2})^2 = 1$ et $(b/2)^2 + (d/2)^2 = 1$.
2. $ab/2\sqrt{2} + cd/2\sqrt{2} = 0$.

En particulier, le déterminant de cette matrice vaut ± 1. Mais si a,b,c et d étaient tous dans $\mathbb{Q}$, on obtiendrait en calculant le déterminant de façon directe que $\sqrt{2}$ serait dans $\mathbb{Q}$, ce qui n'est pas.

A.III.2.iii Non, comme on vient de le prouver!

Partie B

B.I.1.

- Si $0 \leq k < n$, on a $\Gamma_n(k) = 0$.
- Si $k \geq n$, on a :

$$\Gamma_n(k) = \frac{k(k-1)\dots(k-n+1)}{n!} = C_n^k$$

qui est un coefficient binômial et est donc entier.

- Si $k < 0$, on pose $m = -k$ et on a :

$$\begin{aligned}\Gamma_n(k) &= (-1)^n \frac{m(m+1)\dots(m+n-1)}{n!} \\ &= (-1)^n \frac{(n+m-1)!}{n!(m-1)!} = (-1)^n C_{n+m-1}^n \in \mathbb{Z}.\end{aligned}$$

B.I.2. $(\Gamma_n)_{0\leq n\leq m}$ est une famille de polynômes à degrés étagés (i.e. tous distincts). C'est donc une famille libre. Comme le nombre d'éléments de la famille vaut la dimension de l'espace, elle forme une base de $\mathbb{R}_m[X]$.

B.II. On a $P(k)=\sum_{k\geq n} d_n\Gamma_n(k)$. $(d_n)_{0\leq n\leq m}$ est donc solution du système linéaire triangulaire suivant :

$$\left\{\begin{array}{ccccccccc} P(m) & = & d_m\Gamma_m(m) & + & d_{m-1}\Gamma_{m-1}(m) & + & \dots & + & d_0\Gamma_0(m)\\ P(m-1) & = & & & d_{m-1}\Gamma_{m-1}(m-1) & + & \dots & + & d_0\Gamma_0(m-1)\\ & \vdots & & \vdots & & & & & \\ P(0) & = & & & & & & & d_0\Gamma_0(0) \end{array}\right.$$

Puisque $\Gamma_k(k)=1$, les coefficients sur la diagonale valent 1, et le déterminant de ce système triangulaire vaut 1.

B.III. – $i) \implies ii)$: Soit A la matrice du système précédent. Alors les formules de Cramer montrent que :

$$\begin{aligned}\begin{pmatrix} d_0\\ \vdots\\ d_m\end{pmatrix} &= \frac{1}{\det A}({}^t comat A)\begin{pmatrix} P(0)\\ \vdots\\ P(m)\end{pmatrix}\\ &= ({}^t comat A)\begin{pmatrix} P(0)\\ \vdots\\ P(m)\end{pmatrix}.\end{aligned}$$

Maintenant, A est à coefficients entiers, et le calcul des cofacteurs de A ne fait intervenir que des produits et des sommes d'éléments de A. En particulier, la comatrice de A est à coefficients entiers, et si $P(0),\dots,P(m)$ sont des entiers, $d_0,\dots,d_m$ sont entiers.

– $ii) \implies iii)$: C'est évident en considérant l'écriture de P.

– $iii) \implies iv)$: C'est évident!

– $iv) \implies i)$: Soient $k,\dots,k+m$ ces $m+1$ entiers consécutifs. Posons $Q(X)=P(X-k)$. Alors $Q(0),\dots,Q(m)$ sont des entiers, et comme dans $i) \implies ii)$, on prouve que $Q=\sum d_n\Gamma_n$, où les d_n sont des entiers. On en déduit que $Q\in\mathcal{P}(\mathbb{Z},\mathbb{Z})$, et il en est de même pour P.

B.IV.1. Remarquons pour commencer que $P(1)=P(2)=P(3)=P(4)=P(5)=0$. On a alors le système suivant (on utilise le triangle de Pascal pour l'écrire facilement) :

$$\left\{\begin{array}{rcl} d_0 & = & -120\\ d_0+d_1 & = & 0\\ d_0+2d_1+d_2 & = & 0\\ d_0+3d_1+3d_2+d_3 & = & 0\\ d_0+4d_1+6d_2+4d_3+d_4 & = & 0\\ d_0+5d_1+10d_2+10d_3+5d_4+d_5 & = & 0. \end{array}\right.$$

La résolution donne donc :

$$d_0=-120,\ d_1=-120, d_2=120,\ d_3=-120,\ d_4=120,\ d_5=-120.$$

En outre, les racines que nous avons trouvées de P impliquent la factorisation suivante :

$$P(X)=(X-1)(X-2)\dots(X-5).$$

En particulier, P est scindé sur $\mathbb{Q}$.

B.IV.2. Inspirés par le résultat de la question précédente, on remarque que, pour $1 \leq k \leq m$, on a :

$$\begin{aligned} P(k) &= \sum_{n=0}^{m} (-1)^n \Gamma_n(k) \\ &= \sum_{n=0}^{k} (-1)^n C_k^n \\ &= (1-1)^k = 0. \end{aligned}$$

On a donc $P(X) = c(X-1)\dots(X-m)$. Le coefficient dominant de $P(X)$ vaut $c = \frac{(-1)^m}{m!}$. On en déduit que

$$P(X) = (-1)^m \Gamma_m(X-1).$$

Partie C

C.I.1. Si $x = c/d$, on écrit $c = p^{k_1}a$ où $a \wedge p = 1$ et $d = p^l b$, avec $b \wedge p = 1$. On a donc $x = p^{k_1-k_2}\frac{a}{b}$. Réciproquement, si l'on a $x = p^k \frac{a}{b} = p^l \frac{a'}{b'}$, alors $p^k ab' = p^l a'b$, et donc $p^k | p^l a'b$. Mais $p \wedge a'b = 1$, et le théorème de Gauss assure que $p^k | p^l$, ou encore que $k \leq l$. De même, on peut prouver que $l \leq k$, et donc $k = l$.

C.I.2. i. On a $\nu_p(p^k) = k$, et $\nu_p(0) = +\infty$. Ceci garantit que ν_p est surjective.

ii. Si $x = p^k \frac{a}{b}$, $y = p^l \frac{c}{d}$, on a :

$$\nu_p(xy) = \nu_p\left(p^{k+l}\frac{ac}{bd}\right) = k + l,$$

puisque ac et bd sont premiers avec p. Cette relation reste vérifiée si x et/ou y est nul.

iii. Ecrivons $x = p^k \frac{a}{b}$, $y = p^l \frac{c}{d}$, avec par exemple $k \geq l$. On a :

$$x + y = p^l \left(\frac{p^{k-l}ad + cb}{bd}\right).$$

Maintenant, comme $bd \wedge p = 1$, on a

$$\nu_p\left(\frac{1}{bd}\right) = 0.$$

Puisque $k \geq l$, on a $p^{k-l}ad + cb \in \mathbb{Z}$ et $\nu_p(p^{k-l}ad + cb) \geq 0$. On en déduit que

$$\nu_p(x + y) \geq l.$$

C.I.3. On a $\nu_p(1) = \nu_p(-1) = 0$ et

$$\nu_p(x/y) = \nu_p\left(\frac{x}{1} \times \frac{1}{y}\right) = \nu_p(x) + \nu_p(1/y) = \nu_p(x) - \nu_p(y).$$

C.I.4. Si $x \in \mathbb{Z}_{(p)}$, $x = \alpha/\beta$ où $\beta \wedge p = 1$. En particulier, $\nu_p(\beta) = 0$, et $\nu_p(x) \geq 0$. Réciproquement, si $\nu_p(x) \geq 0$, on sait que x s'écrit $x = p^k \frac{a}{b}$, où $k \geq 0$, $a \wedge p = 1$ et $b \wedge p = 1$. Quitte à simplifier la fraction a/b, on en déduit que $x \in \mathbb{Z}_{(p)}$.

On déduit par exemple de C.I.2.(ii) et (iii) que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$. Puisque $\nu_p(1/x) = -\nu_p(x)$, les éléments inversibles de $\mathbb{Z}_{(p)}$ sont ceux pour lesquels $\nu_p(x) = 1$ (c'est-à-dire les fractions a/b où les entiers a,b et p sont premiers entre eux deux à deux).

C.I.5.i. Notons $F_k = \{1 \leq j \leq n;\ \nu_p(j) \geq k\}$. Si $j \in F_k$, alors $j = p^k a$ où a est un entier. Maintenant, puisque $1 \leq j \leq n$, on déduit que $1 \leq a \leq \frac{n}{p^k}$. Ceci signifie encore que $\operatorname{card} F_k = \left[\frac{n}{p^k}\right]$.Maintenant, on a :

$$\{j \in \mathbb{N};\ \nu_p(j) = k\} = F_k - F_{k+1},$$

et comme F_{k+1} est inclus dans F_k, le cardinal de cet ensemble vaut $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$.

C.I.5.ii. On a $\nu_p(n!) = \nu_p(1) + \cdots + \nu_p(n)$, que l'on réécrit en regroupant les termes qui ont même valuation p-addique.

$$\begin{aligned}
\nu_p(n!) &= \sum_{k>0} k \operatorname{card}\{1 \leq j \leq n;\ \nu_p(j) = k\} \\
&= \sum_{k>0} k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right) \\
&= \sum_{k>0} \left[\frac{n}{p^k}\right],
\end{aligned}$$

où la dernière égalité s'obtient en barrant les termes "en diagonale".

C.II.1. Soit $x \in \mathbb{Z}$. Alors, clairement, $x \in \mathbb{Z}_{(l)}$ pour tout l premier (voir par exemple la caractérisation C.I.4.). Réciproquement, si $x \in \mathbb{Q}$, $x \notin \mathbb{Z}$, x s'écrit $x = a/b$, avec $a \wedge b = 1$, et $b > 1$. Soit l un facteur premier de b, qui n'intervient donc pas dans a. Alors $x \notin \mathbb{Z}_{(l)}$.

C.II.2. L'inclusion $\mathcal{P}(E,\mathbb{Z}) \subset \mathcal{P}(E,\mathbb{Z}_{(l)})$ est évidente. Réciproquement, si $P \notin \mathcal{P}(E,\mathbb{Z})$, il existe $k \in E$ et $l \in \mathbb{P}$ tel que $P(k) \notin \mathbb{Z}_{(l)}$. Et donc P n'appartient pas à $\mathcal{P}(E,\mathbb{Z}_{(l)})$.

C.III.1. Choisissons d'abord u_1. u_1 satisfait la condition de minimisation

$$\nu_3(1) = \min_{x \in E} \nu_3(x).$$

Maintenant, $\nu_3(1) = 0$, et $\nu_3(3k) = 1 + \nu_3(k) \geq 1$. On a donc nécessairement $u_1 = 1$. Choisissons maintenant u_2, qui doit satisfaire :

$$\nu_3(u_2(u_2 - 1)) = \min_{x \in E} \nu_3(x(x-1)).$$

Maintenant, si $x = 3k$, on a :

$$\nu_3(x(x-1)) = \nu_3(3k) + \nu_3(3k-1) = 1 + \nu_3(k) + 0.$$

On peut choisir pour u_2 n'importe quel $3k$, pourvu que $k \wedge 3 = 1$.

C.III.2. Montrons que la propriété est vérifiée pour chaque $n \in \mathbb{N}^*$. Si $x \in \mathbb{Z}$, on sait depuis la question B.I.1. que

$$x(x-1)\ldots(x-n+1) = Cn!,$$

où C est un entier. En particulier,

$$\nu_p(x\ldots(x-n+1)) \geq \nu_p(n!) = \nu_p\left(\prod_{k=0}^{n-1}(n-k)\right).$$

C.III.3. Supposons qu'on a construit des éléments $u_0, \ldots, u_n$ pour lesquels la condition de minimalité est vérifiée. Il suffit de choisir pour u_{n+1} un entier x de E tel que la condition de minimalité, au rang $n+1$, est réalisée en ce x. Ceci est possible, puisque $\{\nu_p\left(\prod_{k=0}^{n}(x-u_k)\right);\ x \in E\}$ est une partie non-vide de $\mathbb{N}$. L'exemple de la question C.III.1., où plusieurs choix sont possibles pour u_2, prouve qu'il n'y a pas en général unicité de la suite.

C.IV.1.i. Si $x \in E$,

$$\nu_p(P_n(x)) = \nu_p\left(\prod_{k=0}^{n-1}(x-u_k)\right) - \nu_p\left(\prod_{k=0}^{n-1}(u_n-u_k)\right) \geq 0,$$

puisque (u_n) est p-ordonnée. En particulier, d'après C.I.4., $P \in \mathcal{P}(E,\mathbb{Z}_{(p)})$.

C.IV.1.ii. Les degrés des polynômes de cette famille sont étagés. On raisonne alors comme dans la partie B.

C.IV.1.iii. On a $P_n(u_k) = 0$ si $0 \leq k \leq n-1$, et $P_n(u_n) = 1$.

C.IV.2. Comme dans la partie B. un système linéaire (triangulaire) de déterminant 1 à coefficients dans $\mathbb{Z}_{(p)}$ relie $P(0),\ldots,P(u_m)$ à $c_0,\ldots,c_m$. On démontre l'équivalence en recopiant mot pour mot ce qui a été effectué auparavant.

C.IV.3. Il suffit, en vertu de la décomposition $P(X) = \sum_{n=0}^{m} c_n P_n(X)$ et du point ii) de C.IV.2., de prouver que $p^{\omega(m)}P_n$ a ses coefficients dans $\mathbb{Z}_{(p)}$ pour $0 \leq n \leq m$. Mais,

$$p^{\omega(m)}P_n = \frac{p^{\omega(m)}}{\prod_{k=0}^{n-1}(u_n-u_k)}\prod_{k=0}^{n-1}(X-u_k).$$

Comme

$$\nu_p\left(\frac{p^{\omega(m)}}{\prod_{k=0}^{n-1}(u_n-u_k)}\right) \geq \nu_p\left(\frac{p^{\omega(n)}}{\prod_{k=0}^{n-1}(u_n-u_k)}\right) \geq 0$$

(car (u_n) est p-ordonnée), les coefficients de $p^{\omega(m)}P_n$ sont bien dans $\mathbb{Z}_{(p)}$.
Le fait que $\mathcal{P}(E,\mathbb{Z}_{(p)})$ est un sous-anneau de $\mathbb{Q}[X]$ se déduit immédiatement du fait que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$.

Partie D

D.I.1. On effectue la division euclidienne de n par $p-1$:

$$n = a(p-1)+b,\ 0 \leq b < p-1.$$

On en déduit que :

$$\begin{aligned}\varphi_p(n) &= a(p-1)+b+1+a\\ &= ap-a+b+1+a\\ &= ap+b+1.\end{aligned}$$

Ainsi,

$$\frac{\varphi_p(n)}{p} = a + \frac{b+1}{p}.$$

Comme $0 \leq \frac{b+1}{p} < 1$, on obtient effectivement

$$\left[\frac{\varphi_p(n)}{p}\right] = \left[\frac{n}{p-1}\right].$$

D.I.2. i. D'abord (c'est le plus simple), nous remarquons que φ_p est croissante. Ensuite, prouvons que φ_p est à valeurs dans $\mathbb{N}\backslash p\mathbb{N}$: en écrivant comme ci-dessus $n = a(p-1)+b$, $0 \leq b < p-1$,

$$\begin{aligned}\varphi_p(n) = kp &\iff n+1+\left[\frac{n}{p-1}\right] = kp\\ &\iff a(p-1)+b+1+a = kp\\ &\iff b+1 = (k-a)p.\end{aligned}$$

Mais si $k \leq a$, on a $b \leq -1$ ce qui est impossible, et si $k > a$, on a $b \geq p-1$ ce qui est tout aussi impossible.
Il reste à étudier les sauts de la fonction φ_p. Précisément, il suffit de montrer que :

- Si $\varphi_p(n) = kp - 1$, alors $\varphi_p(n+1) = kp + 1$.
- Si $\varphi_p(n) \neq kp - 1$, alors $\varphi_p(n+1) = \varphi_p(n) + 1$.

Mais,

$$\begin{aligned}\varphi_p(n+1) - \varphi_p(n) &= 1 + \left[\frac{n+1}{p-1}\right] - \left[\frac{n}{p-1}\right] \\ &< \frac{n+1}{p-1} + 1 - \frac{n}{p-1} + 1 \\ &< 2 + \frac{1}{p-1} \\ &< 3.\end{aligned}$$

Le saut n'est donc que de 1 ou 2. Cherchons pour quelles valeurs de $\varphi_p(n)$ le saut vaut 2 :

$$\varphi_p(n+1) - \varphi_p(n) = 2 \iff \left[\frac{n+1}{p-1}\right] - \left[\frac{n}{p-1}\right] = 1$$

On a donc

$$\frac{n}{p-1} < l \leq \frac{n+1}{p-1} < l+1,$$

où l est un entier. A fortiori, on obtient

$$n < l(p-1) \leq n+1,$$

ce qui donne

$$n = l(p-1) - 1.$$

Réintroduisant cela dans $\varphi_p(n)$, on trouve :

$$\begin{aligned}\varphi_p(n) &= l(p-1) - 1 + 1 + l - 1 \\ &= lp - 1.\end{aligned}$$

Résumons : φ_p est croissante de $\mathbb{N}$ dans $\mathbb{N}\backslash p\mathbb{N}$, vérifie $\varphi_p(0) = 0$, ne réalise que des sauts de 1 sauf si $\varphi_p(n)$ est de la forme $lp-1$, où le saut pour atteindre $\varphi_p(n+1)$ vaut 2. φ_p est bien la bijection croissante de $\mathbb{N}$ dans $\mathbb{N}\backslash p\mathbb{N}$.

ii. On admet pour le moment que $\left[\frac{x}{ab}\right] = \left[\frac{\left[\frac{x}{a}\right]}{b}\right]$. Alors, d'après la question C.I.5.ii.,

$$\begin{aligned}\nu_p(\varphi_p(n)!) &= \sum_{k\geq 0}\left[\frac{\varphi_p(n)}{p^k}\right] \\ &= \sum_{k\geq 0}\left[\frac{\left[\frac{\varphi_p(n)}{p}\right]}{p^{k-1}}\right] \\ &= \sum_{k\geq 0}\left[\frac{\left[\frac{n}{p-1}\right]}{p^{k-1}}\right] \\ &= \sum_{k\geq 0}\left[\frac{n}{p^{k-1}(p-1)}\right] \\ &= \omega_p(n).\end{aligned}$$

Reste à prouver le fait admis. On écrit que $x = kab + r$, avec $0 \leq r < ab$. On écrit encore $r = r_1 a + r_2$, avec $0 \leq r_1 < b$ et $0 \leq r_2 < a$. On en déduit alors que :

$$\left[\frac{x}{ab}\right] = k,$$

et aussi

$$\left[\frac{x}{a}\right] = kb + r_1 \implies \left[\frac{\left[\frac{x}{a}\right]}{b}\right] = k.$$

D.I.3. i. On a :

$$\begin{aligned}
\omega_p(n) &\leq \sum_{k\geq 0} \frac{n}{(p-1)p^k} \\
&\leq \frac{n}{p-1}\frac{1}{1-1/p} \\
&\leq \frac{n}{p-1}\frac{p}{p-1} \\
&\leq 2n
\end{aligned}$$

(la fonction $x \mapsto x/(x-1)^2$ est décroissante sur $[2, +\infty[$, et vaut 2 si $x = 2$).

ii. Si $n < p-1$, alors pour tout $k \geq 0$, $\left[\frac{n}{(p-1)p^k}\right] = 0$, ce qui donne $\omega_p(n) = 0$.

D.II.1. Puisque $\varphi_p(s) \notin p\mathbb{N}$ et que $r \in p\mathbb{N}$, on a $r - \varphi_p(s) \in \mathbb{Z}\backslash p\mathbb{Z}$, et donc $\nu_p(r - \varphi_p(s)) = 0$.

D.II.2. On a :

$$\begin{aligned}
\nu_p\left(\prod_{r=0}^{\varphi_p(n)-1} (\varphi_p(n) - r)\right) &= \sum_{r=0}^{\varphi_p(n)-1} \nu_p\left(\varphi_p(n) - r\right) \\
&= \sum_{\substack{r=0 \\ r\in p\mathbb{Z}}}^{\varphi_p(n)-1} \nu_p\left(\varphi_p(n) - r\right) + \sum_{\substack{r=0 \\ r\notin p\mathbb{Z}}}^{\varphi_p(n)-1} \nu_p\left(\varphi_p(n) - r\right) \\
&= \sum_{\substack{r=0 \\ r\notin p\mathbb{Z}}}^{\varphi_p(n)-1} \nu_p\left(\varphi_p(n) - r\right).
\end{aligned}$$

On finit de prouver la première égalité en utilisant que φ_p est une bijection croissante de $\mathbb{N}$ dans $\mathbb{N} - p\mathbb{N}$, ce qui légitime le changement d'indice $r = \varphi_p(k)$. La seconde égalité est évidente pourvu que l'on ne se perde pas dans les notations. On a en effet :

$$\prod_{r=0}^{\varphi_p(n)-1} (\varphi_p(n) - r) = \varphi_p(n)!$$

D.II.3. La première égalité se démontre exactement de la même façon. Pour la seconde, il suffit de remarquer que

$$\prod_{r=0}^{n-1} (\varphi_p(s) - r) = \frac{\varphi_p(s)!}{(\varphi_p(s) - \varphi_p(n))!}.$$

D.II.4. On fixe $n \in \mathbb{N}^*$. Tout élément de $\mathbb{N}\backslash p\mathbb{N}$ différent de $\varphi_p(0), \ldots, \varphi_p(n-1)$ s'écrit $\varphi_p(s)$ pour $s \geq n$. Pour prouver le résultat, il suffit donc de démontrer que

$$\nu_p\left(\frac{\varphi_p(s)!}{(\varphi_p(s) - \varphi_p(n))!}\right) \geq \nu_p(\varphi_p(n)!)$$

si $s \geq n$. Mais ,

$$-\nu_p(\varphi_p(n)!) + \nu_p\left(\frac{\varphi_p(s)!}{(\varphi_p(s)-\varphi_p(n))!}\right) = \nu_p\left(\frac{\varphi_p(s)!}{(\varphi_p(s)-\varphi_p(n))!\varphi_p(n)!}\right) \geq 0,$$

car $\frac{\varphi_p(s)!}{(\varphi_p(s)-\varphi_p(n))!\varphi_p(n)!}$ est un entier.

D.III.1. On applique la question C.IV.2. avec $E = \mathbb{N}\backslash p\mathbb{N}$.

D.III.2. Il s'agit d'une application directe de C.IV.3.

Partie E

E.I. i. Ce polynôme est P_4 avec les notations de la partie C. Il est dans $\mathcal{P}(\mathbb{Z},\mathbb{Z})$ et a fortiori dans $\mathcal{P}(\mathbb{P},\mathbb{Z})$.

ii. Si p est un nombre premier, et $p = 2$ ou $p = 3$, on a $\frac{(p-1)(p-2)(p-3)}{24} = 0 \in \mathbb{Z}$. Sinon, $p \geq 5$ et

$$\frac{(p-1)(p-2)(p-3)}{3!} = C_{p-1}^3 \in \mathbb{Z}.$$

iii. Le polynôme $\frac{(X-1)(X-2)(X-3)}{24}$ est dans $\mathcal{P}(\mathbb{P},\mathbb{Z})$, mais pas dans $\mathcal{P}(\mathbb{Z},\mathbb{Z})$ (il suffit de l'évaluer en 0).

E.II.1. i. On écrit $Q(X) = \sum_{n=0}^m c_n X^n$, où c_n est tel que $p^\alpha c_n \in \mathbb{Z}_{(p)}$, $0 \leq n \leq m$. On a alors :

$$\begin{aligned} Q(a+kp^\alpha) - Q(a) &= \sum_{n=0}^m c_n\left[(a+kp^\alpha)^n - a^n\right] \\ &= \sum_{n=0}^m \sum_{j=1}^n C_n^j k^j a^{n-j} p^{\alpha j} c_m \\ &\in \mathbb{Z}_{(p)}. \end{aligned}$$

ii. En effet, il existe un entier naturel k tel que $a+kp^\alpha$ est premier. Mais alors $Q(a+kp^\alpha) \in \mathbb{Z}_{(p)}$.

iii. Si $a \in \mathbb{N} - p\mathbb{N}$, on choisit k comme à la question précédente. Utilisant i., on en déduit que $Q(a) \in \mathbb{Z}_{(p)}$, et donc $Q \in \mathcal{P}(\mathbb{N}\backslash p\mathbb{N},\mathbb{Z}_{(p)})$.

E.II.2. i. Si $q \in \mathbb{P}$, ou bien $q = p$ ou bien $q \wedge p = 1$ et $q \in \mathbb{N}\backslash p\mathbb{N}$.

ii. D'après ce qui a été prouvé auparavant, $\mathcal{P}(\mathbb{P},\mathbb{Z}_{(p)}) \subset \mathcal{P}(\mathbb{N}\backslash p\mathbb{N},\mathbb{Z}_{(p)})$. D'autre part, si $P \in \mathcal{P}(\mathbb{P},\mathbb{Z}_{(p)})$, on a $P(p) \in \mathbb{Z}_{(p)}$, ce qui achève de prouver que

$$\mathcal{P}(\mathbb{P},\mathbb{Z}_{(p)}) \subset \mathcal{P}(E_p,\mathbb{Z}_{(p)}).$$

D'autre part, l'inclusion $\mathbb{P} \subset E_p$ donne immédiatement

$$\mathcal{P}(E_p,\mathbb{Z}_{(p)}) \subset \mathcal{P}(\mathbb{P},\mathbb{Z}_{(p)}).$$

iii. Il s'agit d'une application immédiate de la question précédente et de C.II.2.

E.III. On a :

$$\begin{aligned} Q \in \mathcal{P}(\mathbb{P},\mathbb{Z}) &\implies Q \in \mathcal{P}(\mathbb{N}\backslash p\mathbb{N},\mathbb{Z}_{(p)}) \ (E.II.1.iii.) \\ &\implies p^{\omega_p(m)}Q \text{ est à coefficients dans } \mathbb{Z}_{(p)} \ (D.III.2.) \\ &\implies p^{2m}Q \text{ est à coefficients dans } \mathbb{Z}_{(p)} \ (D.I.3.) \end{aligned}$$

En particulier, si $R = X^{2m}Q$, $R \in \mathcal{P}(\mathbb{Z},\mathbb{Z}_{(p)})$ et ceci pour tout p. C.II.2 entraîne que $R \in \mathcal{P}(\mathbb{Z},\mathbb{Z})$ (ce n'est pas tout à fait le chemin indiqué).

E.IV.1. Pour k allant de 0 à m, on a

$$1 \leq \varphi_p(k) \leq 2m+1 \implies \varphi_p(k)^{2m} Q(\varphi_p(k)) \in \mathbb{Z}.$$

Mais comme $\varphi_p(k)^{2m} \wedge p = 1$, on en déduit que

$$Q(\varphi_p(k)) \in \mathbb{Z}_{(p)}.$$

D.III.1. donne le résultat.

E.IV.2. D'après D.III.2., on a

$$p^{\omega_p(m)} Q(p) \in \mathbb{Z}_{(p)}.$$

Mais, puisque $p > m+1$, on a $\omega_p(m) = 0$ et donc $Q(p) \in \mathbb{Z}_{(p)}$.

E.V. $(a) \implies (b)$: La première partie de (b) est évidente, et la deuxième est donnée par E.III.
$(b) \implies (a)$: Soit p un nombre premier, et $x \in E_p$. Si $x = p$, la première partie de b) ou E.IV.2. (suivant que $p \leq m+1$ ou non) entraîne que $Q(x) \in \mathbb{Z}_{(p)}$. Si $x \neq p$, alors $x \in \mathbb{N} \backslash p\mathbb{N}$, et E.IV.1. entraîne que $Q(x) \in \mathbb{Z}_{(p)}$. Il suffit d'appliquer E.II.2.iii. pour obtenir que Q est élément de $\mathcal{P}(\mathbb{P},\mathbb{Z})$.

E.VI. On pose

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

On vérifie la caractérisation de la question précédente à l'aide d'une calculatrice, et on a donc $Q \in \mathcal{P}(\mathbb{P},\mathbb{Z})$. Ceci donne le résultat.