CAPES 2002 – Deuxième composition (extrait)

NOTATIONS.

On note $\mathbf{P}$ l'ensemble des nombres premiers. Pour tout nombre premier p, on note $\mathbf{Z}_{(p)}$ l'ensemble des **rationnels** dont une représentation irréductible a un dénominateur non divisible par p et v_p la valuation p-adique étendue à $\mathbf{Z}$: $v_p(0) = +\infty$ et, pour n non nul, $|n| = \prod_{p\in\mathbf{P}} p^{v_p(n)}$. On convient $v_p(n) \leq v_p(0)$, pour tout n dans $\mathbf{Z}$.

Pour tout réel x, on appelle partie entière de x et on note $[x]$ l'unique entier k vérifiant $k \leq x < k+1$.

On note :

— $\mathbf{Q}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients rationnels,

— $\mathbf{R}[X]$ l'ensemble des polynômes en l'indéterminée X à coefficients réels et, pour tout entier naturel n, $\mathbf{R}_n[X]$ le sous-ensemble de $\mathbf{R}[X]$ formé des polynômes de degré inférieur ou égal à n.

Pour tous sous-ensembles E et F de $\mathbf{R}$, on note :

$$\mathcal{P}(E,F) = \{P \in \mathbf{R}[X] \,|\, P(E) \subset F\} \ ,$$

à savoir, l'ensemble des éléments de $\mathbf{R}[X]$ dont la valeur en chaque élément de E appartient à F.

PARTIE I - Étude de $\mathcal{P}(\mathbf{Z},\mathbf{Z})$

Pour tout entier naturel n, on note Γ_n le polynôme défini par :

$$\Gamma_0 = 1 \qquad \text{et, pour } n > 0\,, \quad \Gamma_n = \frac{X(X-1)\dots(X-n+1)}{n!} \ .$$

Dans cette partie, on fixe un entier naturel m.

I.1) a) Montrer que, pour tout n, le polynôme Γ_n appartient à $\mathcal{P}(\mathbf{Z},\mathbf{Z})$. (Pour k élément de $\mathbf{Z}$, on distinguera selon qu'on a $0 \leq k < n$, $k \geq n$ ou $k < 0$.)

b) Montrer que la famille $(\Gamma_n)_{0\leq n\leq m}$ forme une base de l'espace vectoriel réel $\mathbf{R}_m[X]$.

I.2) On considère l'application Δ de $\mathbf{R}[X]$ dans lui-même donnée par $\Delta(P) = P(X+1) - P$.

a) Justifier que Δ est linéaire et déterminer son noyau.

b) Démontrer, pour $n \neq 0$: $\Delta(\Gamma_n) = \Gamma_{n-1}$.

c) Démontrer, pour P dans $\mathbf{R}_m[X]$: $P = \sum_{n=0}^{m} \Delta^n(P)(0)\Gamma_n$, où Δ^n est défini par $\Delta^0 = \mathrm{Id}_{\mathbf{R}[X]}$ et $\Delta^{n+1} = \Delta \circ \Delta^n$.

I.3) Soit P un élément de $\mathbf{R}_m[X]$. Montrer que les quatre assertions suivantes sont équivalentes :

(i) $P = \sum_{n=0}^{m} d_n\Gamma_n$ avec d_0, d_1, …, d_m entiers

(ii) $P \in \mathcal{P}(\mathbf{Z},\mathbf{Z})$

(iii) $P(0)$, $P(1)$, …, $P(m)$ sont entiers

(iv) il existe $m+1$ entiers consécutifs en lesquels les valeurs de P sont des entiers.

I.4) Application. On cherche un polynôme P de degré inférieur ou égal à 4 vérifiant $P(0) = 7$, $P(1) = 87$, $P(2) = -143$, $P(3) = -2453$ et $P(4) = -9897$.

a) Montrer qu'un tel polynôme existe et est unique puis déterminer P en utilisant la table des différences finies suivante

x	$\Delta^0 P$	$\Delta^1 P$	$\Delta^2 P$	$\Delta^3 P$	$\Delta^4 P$
0					
1					
2					
3					
4					

b) Généralisation : écrire en Python un programme permettant de calculer les coordonnées d'un polynôme Q de $\mathbf{R}_n[X]$ dans la base $(\Gamma_k)_{0\leq k\leq n}$, connaissant $(Q(k))_{0\leq k\leq n}$.

PARTIE II - Étude de $\mathcal{P}(E, \mathbf{Z}_{(p)})$

Dans toute cette partie p désigne un nombre premier fixé et E une partie infinie de $\mathbf{Z}$.

II.1) a) Montrer que, pour (k, n) dans $\mathbf{N}^* \times \mathbf{N}^*$, le cardinal de l'ensemble $\{j \in [\![1; n]\!] \,|\, v_p(j) = k\}$ est égal à $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$.

b) Justifier la formule suivante due à Legendre : $\forall n \in \mathbf{N}$, $v_p(n!\,) = \sum_{k>0} \left[\frac{n}{p^k}\right]$.

II.2) *On dit qu'une suite $(u_n)_{n\in\mathbf{N}}$ d'éléments distincts de E est p-ordonnée dans E si elle vérifie :*

$$\forall n \in \mathbf{N}^* \quad v_p\left(\prod_{k=0}^{n-1}(u_n - u_k)\right) = \min_{x\in E} v_p\left(\prod_{k=0}^{n-1}(x - u_k)\right) .$$

a) Montrer que si $E = \mathbf{Z}$, la suite $(n)_{n\in\mathbf{N}}$ est p-ordonnée.

b) Montrer par récurrence que, pour tout a dans E, il existe au moins une suite $(u_n)_{n\in\mathbf{N}}$, p-ordonnée dans E et vérifiant $u_0 = a$. Y a-t-il en général unicité d'une telle suite ?

II.3) *Dans la suite de cette partie, on considère une suite $(u_n)_{n\in\mathbf{N}}$ p-ordonnée dans E.* On lui associe la suite de polynômes $(P_n)_{n\in\mathbf{N}}$ définie par :

$$P_0 = 1 \quad \text{et, pour } n \geq 1\,, \quad P_n = \prod_{k=0}^{n-1} \frac{X - u_k}{u_n - u_k} .$$

Soit m dans $\mathbf{N}$ et P dans $\mathbf{R}_m[X]$. Montrer que les assertions suivantes sont équivalentes :

(i) $P \in \mathbf{R}_m[X] \cap \mathcal{P}(E, \mathbf{Z}_{(p)})$,

(ii) $P = \sum_{n=0}^{m} c_n P_n$ avec c_0, c_1, …, c_m dans $\mathbf{Z}_{(p)}$,

(iii) $P(u_0)$, $P(u_1)$, …, $P(u_m)$ sont dans $\mathbf{Z}_{(p)}$.

II.4) On pose $\omega(0) = 0$ et, pour tout élément n de $\mathbf{N}^*$, on note $\omega(n)$ l'entier $v_p\left(\prod_{k=0}^{n-1}(u_n - u_k)\right)$. Montrer que si P appartient à $\mathbf{R}_m[X] \cap \mathcal{P}(E, \mathbf{Z}_{(p)})$, alors les coefficients de $p^{\omega(m)}P$ appartiennent à $\mathbf{Z}_{(p)}$.

PARTIE III - Caractérisation de $\mathcal{P}(\mathbf{N} \setminus p\mathbf{N}, \mathbf{Z}_{(p)})$

Dans toute cette partie, p désigne un nombre premier.
On note $p\mathbf{N}$ l'ensemble des entiers naturels multiples de p et $\mathbf{N} \setminus p\mathbf{N}$ l'ensemble des entiers naturels non multiples de p. Pour tout entier naturel n, on pose :

$$\varphi_p(n) = n + 1 + \left[\frac{n}{p-1}\right] \quad \text{et} \quad \omega_p(n) = \sum_{k\geq 0} \left[\frac{n}{(p-1)p^k}\right] .$$

III.1) À l'aide de la division euclidienne par $p-1$, montrer

$$\left[\frac{\varphi_p(n)}{p}\right] = \left[\frac{n}{p-1}\right] \quad \text{et} \quad \varphi_p(n) \in \mathbf{N} \setminus p\mathbf{N} .$$

III.2) En déduire que :
  a) φ_p n'est autre que l'unique bijection croissante de $\mathbf{N}$ sur $\mathbf{N} \setminus p\mathbf{N}$,
  b) pour tout entier naturel n, $v_p\left((\varphi_p(n))!\right) = \omega_p(n)$.

III.3) Vérifier que pour n entier naturel :
  a) $\omega_p(n) \leq 2n$,
  b) si $n < p-1$, alors $\omega_p(n) = 0$.

III.4) Montrer que, pour (r, s) dans $p\mathbf{N} \times \mathbf{N}$, $v_p(r - \varphi_p(s)) = 0$.

III.5) En déduire que la suite $(\varphi_p(n))_{n\in\mathbf{N}}$ est une suite p-ordonnée dans $\mathbf{N} \setminus p\mathbf{N}$.

III.6) Soit P un élément de $\mathbf{R}_m[X]$.
  a) Montrer que P appartient à $\mathcal{P}\left(\mathbf{N} \setminus p\mathbf{N}, \mathbf{Z}_{(p)}\right)$ si et seulement si $P\left(\varphi_p(k)\right)$ appartient à $\mathbf{Z}_{(p)}$ pour $k = 0, 1, \ldots, m$.
  b) Montrer que si P appartient à $\mathcal{P}(\mathbf{N} \setminus p\mathbf{N}, \mathbf{Z}_{(p)})$ alors les coefficients de $p^{\omega_p(m)}P$ sont dans $\mathbf{Z}_{(p)}$.

PARTIE IV - Un algorithme pour déterminer les éléments de $\mathcal{P}(\mathbf{P}, \mathbf{Z})$

IV.1) En considérant $\dfrac{(X-1)(X-2)(X-3)}{24}$, montrer $\mathcal{P}(\mathbf{Z}, \mathbf{Z}) \neq \mathcal{P}(\mathbf{P}, \mathbf{Z})$.
On admet *le théorème de* DIRICHLET *suivant (que l'on ne cherchera pas à démontrer) :*
Si a et b sont deux entiers naturels premiers entre eux, alors il existe au moins un entier naturel k tel que $a + bk$ soit un nombre premier.

IV.2) Soit p un nombre premier, on pose $E_p = \{p\} \cup (\mathbf{N} \setminus p\mathbf{N})$. Montrer
  a) $\mathcal{P}(\mathbf{P}, \mathbf{Z}_{(p)}) \subset \mathcal{P}(\mathbf{N} \setminus p\mathbf{N}, \mathbf{Z}_{(p)})$.
  b) $\mathcal{P}(\mathbf{P}, \mathbf{Z}_{(p)}) = \mathcal{P}(E_p, \mathbf{Z}_{(p)})$.

IV.3) Montrer $\mathcal{P}(\mathbf{P}, \mathbf{Z}) = \bigcap_{p\in\mathbf{P}} \mathcal{P}(E_p, \mathbf{Z}_{(p)})$.

IV.4) Soit m un entier naturel et Q un élément de $\mathbf{R}_m[X]$. Montrer que les deux assertions suivantes sont équivalentes :
  (i) Q appartient à $\mathcal{P}(\mathbf{P}, \mathbf{Z})$,
  (ii) Pour tout nombre premier $p \leq m+1$, $Q(p)$ appartient à $\mathbf{Z}$, et, pour tout entier naturel $k \leq 2m+1$, $k^{2m}Q(k)$ appartient à $\mathbf{Z}$.

IV.5) Appliquer la caractérisation précédente pour démontrer que, quel que soit le nombre premier p, on a la congruence suivante

$$(p+1)(p-1)(p-2)(p-3)(p-5)(p-7)(p-193) \equiv 0 \pmod{2903040} .$$

CAPESA 1997 ET 2002, CAPES 2002

PARTIE I - Étude de $\mathcal{P}(\mathbf{Z},\mathbf{Z})$

I.1) a) Soit k un entier relatif et n un entier naturel. Si k est supérieur à n, on a $\Gamma_n(x)=\binom{k}{n}$. Si k est strictement négatif, on a $\Gamma_n(k)=(-1)^n\binom{-k+n-1}{n}$. Enfin si k est compris entre 0 et $n-1$, $\Gamma_n(k)$ est nul. Par conséquent $\boxed{\Gamma_n\in\mathcal{P}(\mathbf{Z},\mathbf{Z}).}$

b) La famille $(\Gamma_n)_{0\leq n\leq m}$ étant échelonnée en degrés, de 0 à m, on a affaire à une famille de polynômes non nuls de $\mathbf{R}_m[X]$, donc libre et, par cardinalité, elle forme une $\boxed{\text{base de } \mathbf{R}_m[X].}$

I.2) a) L'opérateur de translation de 1 étant linéaire (comme toute composition à droite), Δ est différence de deux applications linéaires et est donc elle aussi une $\boxed{\text{application linéaire}}$.

Soit P un polynôme dans $\mathbf{R}[X]$ tel que $\Delta(P)=0$. En particulier le polynôme $P-P(0)$ s'annule sur $\mathbf{Z}$ et donc est identiquement nul. Il en résulte que P est constant. Réciproquement si P est un polynôme constant, il est dans le noyau de Δ. Par conséquent le noyau de Δ est formé des $\boxed{\text{polynômes constants.}}$

b) Soit n un entier naturel non nul. On a, même si $n=1$, en tenant compte de $\Gamma_0=1$,

$$\begin{aligned}\Gamma_n &= \Gamma_{n-1}\frac{X-n+1}{n}=\frac{X}{n}\Gamma_{n-1}(X-1)\\ \Delta(\Gamma_n) &= \frac{X+1}{n}\Gamma_{n-1}-\Gamma_{n-1}\frac{X-n+1}{n}=\frac{X+1-X+n-1}{n}\Gamma_{n-1}\end{aligned}$$

i.e. $\boxed{\Delta(\Gamma_n)=\Gamma_{n-1}.}$

c) Par linéarité, il suffit de vérifier la formule demandée sur une base de $\mathbf{R}_m[X]$ et donc sur les polynômes $(\Gamma_n)_{0\leq n\leq m}$. Or pour n et k dans $[\![0;m]\!]$, on a, d'après ce qui précède, $\Delta^k(\Gamma_n)=\Gamma_{n-k}$, si $k\leq n$, ou $\Delta^k(\Gamma_n)=0$ sinon car Γ_0 est dans le noyau de Δ d'après I.2.a). Comme 0 est racine de tous les polynômes Γ_n sauf Γ_0, il vient $\Delta^k(\Gamma_n)(0)=0$ sauf si $n=k$ auquel cas $\Delta^n(\Gamma_n)=1$. La formule en résulte dans ce cas et donc dans le cas général : $\boxed{P=\sum_{n=0}^{m}\Delta^n(P)(0)\Gamma_n.}$

I.3) Si (i) est vrai, (ii) l'est aussi d'après I.1.a et puisque $\mathbf{Z}$ est un anneau. Si (ii) est vrai, alors (iii) l'est car $[\![0;m]\!]\subset\mathbf{Z}$. Et si (iii) est vrai, alors (iv) aussi car 0, 1, …, m sont $m+1$ entiers consécutifs.

Si (iv) est vrai, soit x_0 tel que $P(x_0)$, $P(x_0+1)$, …, $P(x_0+n)$ soient tous entiers relatifs. On note T l'opérateur de translation $P\mapsto P(X+1)$, de sorte qu'on a $\Delta=T-\mathrm{Id}$. De plus T est inversible et commute avec Δ, donc T^{x_0} existe même si x_0 est négatif et commute avec Δ. Il vient, pour n dans $[\![0;m]\!]$:

$$\left(\Delta^n\circ T^{x_0}\right)(P)(0)=\left(T^{x_0}\circ\Delta^n\right)(P)(0)=\Delta^n(P)(x_0)$$

et donc, en utilisant I.2.c),

$$T^{x_0}(P)=\sum_{n=0}^{m}\Delta^n(P)(x_0)\Gamma_n$$

ce qui entraîne $T^{x_0}(P)\in\mathcal{P}(\mathbf{Z},\mathbf{Z})$, d'après I.1.a). Comme $z\mapsto z+1$ est une bijection de $\mathbf{Z}$ dans lui-même, T préserve $\mathcal{P}(\mathbf{Z},\mathbf{Z})$ et il en résulte que (i) est vrai.

Par conséquent les quatre conditions $\boxed{(i),\ (ii),\ (iii) \text{ et } (iv) \text{ sont équivalentes.}}$

I.4) a) On remplit successivement la table des différences finies

x	$\Delta^0 P$	$\Delta^1 P$	$\Delta^2 P$	$\Delta^3 P$	$\Delta^4 P$
0	7				
1	87				
2	-143				
3	-2453				
4	-9897				

x	$\Delta^0 P$	$\Delta^1 P$	$\Delta^2 P$	$\Delta^3 P$	$\Delta^4 P$
0	7	80			
1	87	-230			
2	-143	-2310			
3	-2453	-7444			
4	-9897				

en complétant une colonne grâce à la précédente

x	$\Delta^0 P$	$\Delta^1 P$	$\Delta^2 P$	$\Delta^3 P$	$\Delta^4 P$
0	7	80	-310		
1	87	-230	-2080		
2	-143	-2310	-5134		
3	-2453	-7444			
4	-9897				

x	$\Delta^0 P$	$\Delta^1 P$	$\Delta^2 P$	$\Delta^3 P$	$\Delta^4 P$
0	7	80	-310	-1770	
1	87	-230	-2080	-3054	
2	-143	-2310	-5134		
3	-2453	-7444			
4	-9897				

x	$\Delta^0 P$	$\Delta^1 P$	$\Delta^2 P$	$\Delta^3 P$	$\Delta^4 P$
0	7	80	-310	-1770	-1284
1	87	-230	-2080	-3054	
2	-143	-2310	-5134		
3	-2453	-7444			
4	-9897				

et donc, si P existe, il vérifie $(\Delta^k(P)(0))_{0\leq k\leq 4} = (7, 80, -310, -1770, -1284)$. Il résulte de I.2.c) que, s'il existe, P est unique. Réciproquement, en posant $P = 7 + 80\Gamma_1 - 310\Gamma_2 - 1770\Gamma_3 - 1284\Gamma_4$ et puisque $(\Gamma_n)_{0\leq n\leq 4}$ est une base de $\mathbf{R}_4[X]$ d'après I.1.b), P vérifie $(\Delta^k(P)(0))_{0\leq k\leq 4} = (7, 80, -310, -1770, -1284)$. En effectuant les calculs dans la dernière des tables précédentes à partir de la ligne du haut, on obtient $(P(k))_{0\leq k\leq 4} = (7, 87, -143, -2453, -9897)$. Il résulte que

$\boxed{P \text{ existe et est unique, égal à } 7 + 80\Gamma_1 - 310\Gamma_2 - 1770\Gamma_3 - 1284\Gamma_4.}$

b) On se donne une liste ℓ de taille $n+1$ et on construit une liste c grâce à l'algorithme suivant. On initialise c à [ ]. Puis, tant que ℓ est distincte de [ ], on augmente c de $\ell[0]$ et on affecte la liste des différences entre les termes successifs de ℓ à ℓ.

```
def differences(x):
 y=x[:]
 y.pop()
 return map(lambda u,v: u-v,x[1:],y)

def delta(x):
 c=[]
 while(len(x)>0):
  c.append(x[0])
  x=differences(x)
 c.append(x[0])
 return c
```

PARTIE II - Étude de $\mathcal{P}(E, \mathbf{Z}_{(p)})$

II.1) a) Soit (k, n) dans $\mathbf{N}^* \times \mathbf{N}^*$. On a $p^k\mathbf{N} = \{j \in \mathbf{N} \,|\, v_p(j) \geq k\}$ par définition de la valuation p-adique et donc

$$\{j \in \mathbf{N} \,|\, v_p(j) = k\} = p^k\mathbf{N} \setminus p^{k+1}\mathbf{N} \,.$$

En prenant l'intersection avec $[\![1; n]\!]$, il vient

$$\{j \in [\![1; n]\!] \,|\, v_p(j) = k\} = p^k \left[\!\left[1; \left\lfloor \frac{n}{p^k} \right\rfloor\right]\!\right] \setminus p^{k+1} \left[\!\left[1; \left\lfloor \frac{n}{p^{k+1}} \right\rfloor\right]\!\right] \,.$$

Dans le membre de droite, le second ensemble étant inclus dans le premier, il vient par cardinalité $\boxed{|\{j \in [\![1; n]\!] \,|\, v_p(j) = k\}| = \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor.}$

b) Si $n = 0$, la formule donne 0 comme somme de termes nuls. Soit n dans $\mathbf{N}^*$. Puisque v_p est à valeurs dans $\mathbf{N}$, on a

$$[\![1; n]\!] = \coprod_{k \geq 0} \{j \in [\![1; n]\!] \,|\, v_p(j) = k\} \,,$$

la réunion étant en fait finie puisqu'à partir de $k = 1 + \left\lfloor \log_p(n) \right\rfloor$ les ensembles considérés sont vides. De plus la valuation d'un produit étant la somme des valuations, il vient

$$v_p(n!) = \sum_{j=1}^{n} v_p(j) = \sum_{k \geq 0} \sum_{j \in [\![1;n]\!], v_p(j)=k} v_p(j) = \sum_{k \geq 0} k \cdot |\{j \in [\![1; n]\!] \,|\, v_p(j) = k\}| \,,$$

la somme étant également, en fait, finie. Donc, par transformation d'Abel,

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

ou encore $\boxed{v_p(n!) = \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor.}$

II.2) a) Soit n dans $\mathbf{N}^*$ et x dans $\mathbf{Z}$. On a $\Gamma_n(x) \in \mathbf{Z}$ et donc

$$v_p\left(\frac{\prod_{k=0}^{n-1}(x-k)}{\prod_{k=0}^{n-1}(n-k)}\right) \geq 0\ .$$

Puisque la valuation d'un produit est la somme des valuations, il vient

$$v_p\left(\prod_{k=0}^{n-1}(x-k)\right) \geq v_p\left(\prod_{k=0}^{n-1}(n-k)\right)\ ,$$

ce qui montre que $\boxed{(n)_{n\in\mathbf{N}} \text{ est } p\text{-ordonnée.}}$

b) On pose $u_0 = a$ et on construit la suite (u_n) par récurrence. Soit donc n dans $\mathbf{N}^*$ tel que les n premiers termes de la suite aient été définis. On note $F = E \setminus \{u_0, \ldots, u_{n-1}\}$. L'application $x \mapsto \prod_{k=0}^{n-1}(x-u_k)$, pour x dans F, est à valeurs dans $\mathbf{Z}$ et ne s'annule pas, par construction de F et puisque $E \subset \mathbf{Z}$. On note G son ensemble image. Puisque $v_p(G)$ est une partie non vide de $\mathbf{N}$ (puisque E est infini, donc F aussi), elle admet un plus petit élément. On dispose donc de u_n dans F tel que, pour tout x dans F,

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

ce qui permet de construire la suite (u_n) par récurrence, d'après la convention faite sur $v_p(0)$ en ce qui concerne les éléments x qui ne sont pas dans F.

$\boxed{\text{Il existe au moins une suite } (u_n)_{n\in\mathbf{N}},\ p\text{-ordonnée dans } E \text{ et vérifiant } u_0 = a.}$

Dans le cas étudié précédemment, avec $E = \mathbf{Z}$ et $u_0 = 0$, la propriété de u_1 est $v_p(u_1) = \min_{x\in\mathbf{Z}} v_p(x)$, i.e. $v_p(u_1) = 0$ ou encore u_1 premier à p. Par conséquent,

$\boxed{\text{en général il n'y a pas unicité d'une telle suite.}}$

II.3) Soit x et y dans $\mathbf{Z}_{(p)}$, on dispose donc de a et b premiers à p tels que ax et by soient entiers. Il en résulte que $(ab)(x \pm y)$ ainsi que $(ab)(xy)$ sont entiers et donc que $x \pm y$ et xy sont dans $\mathbf{Z}_{(p)}$. Par conséquent $\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$.

Par définition d'une suite p-ordonnée, pour n entier naturel, P_n prend, sur E, des valeurs dans $\mathbf{Z}_{(p)}$. Puisque $\mathbf{Z}_{(p)}$ est un anneau, il en résulte $(ii) \Longrightarrow (i)$.

L'assertion $(i) \Longrightarrow (iii)$ est immédiate en spécialisant à u_0, …, u_m.

Comme la suite (P_n) est échelonnée en degrés entre 0 et m, $(P_n)_{0\leq n\leq m}$ forme une base de $\mathbf{R}_m[X]$. Soit donc P dans $\mathbf{R}_m[X] \cap \mathcal{P}(E, \mathbf{Z}_{(p)})$, on dispose de c_0, c_1, …, c_m dans $\mathbf{R}$ tels que $P = \sum_{n=0}^{m} c_n P_n$. En spécialisant, il vient, pour n dans $[\![0; m]\!]$, $P(u_n) = c_n + \sum_{k=0}^{n-1} c_k P_k(u_n)$. Il en résulte que les coefficients $(c_n)_{0\leq n\leq m}$ sont solutions d'un système linéaire triangulaire à coefficients dans $\mathbf{Z}_{(p)}$ et de diagonale 1. Par récurrence immédiate, puisque $\mathbf{Z}_{(p)}$ est un anneau, il en résulte que c_0, c_1, …, c_m sont dans $\mathbf{Z}_{(p)}$, i.e. $(iii) \Longrightarrow (ii)$.

Ainsi $\boxed{\text{les trois conditions sont équivalentes.}}$

II.4) Par définition, pour n dans $\mathbf{N}^*$, $p^{-\omega(n)}\prod_{k=0}^{n-1}(u_n-u_k)$ est un rationnel qui peut s'écrire comme le quotient de deux entiers premiers à p et donc son inverse appartient à $\mathbf{Z}_{(p)}$. Il en résulte que $p^{\omega(n)}P_n$ est à coefficients dans $\mathbf{Z}_{(p)}$. A fortiori, puisqu'on a affaire à une suite p-ordonnée, pour $m \geq n$, $p^{\omega(m)}P_n$ est à coefficients dans $\mathbf{Z}_{(p)}$. Comme ce dernier est un anneau, il résulte de II.3) et de $P_0 = 1$ que, si P appartient à $\mathbf{R}_m[X] \cap \mathcal{P}(E, \mathbf{Z}_{(p)})$, alors

$\boxed{\text{les coefficients de } p^{\omega(m)}P \text{ appartiennent à } \mathbf{Z}_{(p)}.}$

PARTIE III - Caractérisation de $\mathcal{P}(\mathbf{N} \setminus p\mathbf{N}, \mathbf{Z}_{(p)})$

III.1) Puisque p est premier, $p-1$ est un entier naturel non nul et on peut donc effectuer la division euclidienne de n par $p-1$. On dispose donc de q et r, entiers, avec $0 \leq r < p-1$ et tels que $n = (p-1)q + r$. Il vient $\varphi_p(n) = (p-1)q + r + 1 + q = pq + r + 1$ et, comme $0 \leq r+1 < p$, on a affaire à la division euclidienne de $\varphi_p(n)$ par p et ainsi $\left[\dfrac{\varphi_p(n)}{p}\right] = q$. Autrement dit

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

D'après ce qui précède le reste de la division euclidienne de $\varphi(n)$ par p est $r+1$ et il n'est donc pas nul. Par conséquent $\boxed{\varphi_p(n) \in \mathbf{N} \setminus p\mathbf{N}.}$

III.2) a) Comme la fonction partie entière est croissante, φ_p est somme d'une fonction affine strictement croissante et d'une fonction croissante (en tant que composée de deux fonctions croissantes), donc φ_p est strictement croissante. C'est donc une bijection croissante sur son image, et cette image est incluse dans $\mathbf{N} \setminus p\mathbf{N}$ d'après ce qui précède.

Réciproquement si m appartient à $\mathbf{N} \setminus p\mathbf{N}$, on écrit sa division euclidienne par p sous la forme $m = pq + r$ avec $0 < r < p$. Les calculs précédents montrent que m est l'image de $(p-1)q + (r-1)$ par φ_p, puisque $0 \leq r-1 < p-1$.

Enfin $\mathbf{N} \setminus p\mathbf{N}$ est une partie infinie de $\mathbf{N}$ et donc il existe une unique bijection croissante de $\mathbf{N}$ sur $\mathbf{N} \setminus p\mathbf{N}$. Par conséquent $\boxed{\varphi_p \text{ est l'unique bijection croissante de } \mathbf{N} \text{ sur } \mathbf{N} \setminus p\mathbf{N}.}$

b) On reprend les notations de III.1) : $n = (p-1)q+r$ et $\varphi_p(n) = pq+r+1$ avec $0 \leq r < p-1$. Soit k dans $\mathbf{N}^*$. On effectue la division euclidienne de q par p^{k-1}. On dispose donc de a et b entiers, avec $0 \leq b < p^{k-1}$ et tels que $q = p^{k-1}a + b$. Il vient

$$\varphi_p(n) = p^k a + (pb + r + 1) \quad \text{et} \quad n = p^{k-1}(p-1)a + ((p-1)b + r)$$

avec $0 \leq pb + r + 1 < p(p^{k-1}-1) + p = p^k$ et $0 \leq (p-1)b + r < (p-1)(p^{k-1}-1) + p - 1 = (p-1)p^{k-1}$. Il en résulte $\left[\dfrac{\varphi_p(n)}{p^k}\right] = \left[\dfrac{n}{(p-1)p^{k-1}}\right]$. Par conséquent, en utilisant la formule de LEGENDRE et en translatant un indice, il vient

$$v_p\left((\varphi_p(n))!\right) = \sum_{k\geq 1}\left[\frac{\varphi_p(n)}{p^k}\right] = \sum_{k\geq 0}\left[\frac{n}{(p-1)p^k}\right],$$

i.e. $\boxed{v_p\left((\varphi_p(n))!\right) = \omega_p(n).}$

III.3) a) Soit n un entier naturel. Puisqu'on a affaire à des séries à termes positifs, et puisque la partie entière d'un nombre lui est inférieure, on a, en minorant p par 2,

$$\sum_{k\geq 0}\left[\frac{n}{(p-1)p^k}\right] \leq \sum_{k\geq 0}\frac{n}{(p-1)p^k} \leq \sum_{k\geq 0}\frac{n}{2^k} = 2n\,,$$

i.e. $\boxed{\omega_p(n) \leq 2n.}$

b) Soit n un entier naturel avec $n < p-1$, alors tous les termes de la série $\sum\left[\frac{n}{(p-1)p^k}\right]$ sont nuls et donc sa somme aussi, i.e. $\boxed{\omega_p(n) = 0.}$

III.4) Soit (r,s) dans $p\mathbf{N}\times\mathbf{N}$, alors p divise r mais pas $\varphi_p(s)$, donc il ne divise pas leur différence et ainsi $\boxed{v_p(r-\varphi_p(s)) = 0.}$

III.5) Soit x dans $\mathbf{N}\setminus p\mathbf{N}$, i.e. dans $\varphi_p(\mathbf{N})$ et n dans $\mathbf{N}^*$. On dispose de m dans $\mathbf{N}$ tel que $x = \varphi_p(m)$. Si $k < n$, alors $\prod_{k=0}^{n-1}(x-\varphi_p(k)) = 0$ et la valuation p-adique du membre de droite est donc $+\infty$. Sinon on a, en utilisant la question précédente pour la troisième égalité puisque $v_p(x-k) = v_p(\varphi_p(m)-k) = 0$ lorsque k appartient à $p\mathbf{N}$, ce qui est en particulier le cas si $\varphi_p(n-1) < k < \varphi_p(n)$ et permet d'écrire la quatrième égalité :

$$\begin{aligned}
v_p\left(\prod_{k=0}^{n-1}(x-\varphi_p(k))\right) &= \sum_{k=0}^{n-1} v_p(x-\varphi_p(k)) \\
&= \sum_{0\leq k\leq \varphi_p(n-1),\, k\notin p\mathbf{N}} v_p(x-k) \\
&= \sum_{0\leq k\leq \varphi_p(n-1)} v_p(x-k) \\
&= \sum_{0\leq k< \varphi_p(n)} v_p(x-k) \\
&= v_p\left(\frac{x!}{(x-\varphi_p(n))!}\right) \\
&= v_p((\varphi_p(n))!\,) + v_p\left(\binom{x}{\varphi_p(n)}\right) \\
&\geq v_p((\varphi_p(n))!\,)
\end{aligned}$$

et, de plus, il y a égalité lorsque $x = \varphi_p(n)$. On en déduit que

$\boxed{\text{la suite } (\varphi_p(n))_{n\in\mathbf{N}} \text{ est une suite } p\text{-ordonnée dans } \mathbf{N}\setminus p\mathbf{N}.}$

III.6) a) Soit P un élément de $\mathbf{R}_m[X]$. D'après la question précédente et l'équivalence entre (i) et (iii) dans II.3), P appartient à $\mathcal{P}\left(\mathbf{N}\setminus p\mathbf{N}, \mathbf{Z}_{(p)}\right)$ si et seulement si

$\boxed{P\,(\varphi_p(k)) \text{ appartient à } \mathbf{Z}_{(p)} \text{ pour } k = 0,\, 1,\, \ldots,\, m.}$

b) Soit P un élément de $\mathbf{R}_m[X]\cap\mathcal{P}(\mathbf{N}\setminus p\mathbf{N},\mathbf{Z}_{(p)})$. D'après la question précédente, en appliquant II.4) et en utilisant la formule III.2.b), il vient $\boxed{\text{les coefficients de } p^{\omega_p(m)}P \text{ sont dans } \mathbf{Z}_{(p)}.}$

PARTIE IV - Un algorithme pour déterminer les éléments de $\mathcal{P}(\mathbf{P},\mathbf{Z})$

IV.1) Soit $P=\dfrac{(X-1)(X-2)(X-3)}{24}$. On a $P(6)=\dfrac{5}{2}\notin\mathbf{Z}$ et donc P n'appartient pas à $\mathcal{P}(\mathbf{Z},\mathbf{Z})$. Par ailleurs pour p premier, avec $p>5$, on a $pP(p)=\Gamma_4(p)$ et on a $v_p(\Gamma_4(p))=v_p(24)+v_p(\Gamma_4(p))=v_p(p(p-1)(p-2)(p-3))=1$ puisque p est premier à 24, $p-1$, $p-2$ et $p-3$. On en déduit que $P(p)$ est entier. Enfin, $P(2)=P(3)=0$ et donc P appartient à $\mathcal{P}(\mathbf{P},\mathbf{Z})$. On en déduit $\boxed{\mathcal{P}(\mathbf{Z},\mathbf{Z})\neq\mathcal{P}(\mathbf{P},\mathbf{Z}).}$

IV.2) a) Soit P dans $\mathcal{P}(\mathbf{P},\mathbf{Z}_{(p)})$ et a dans $\mathbf{N}\setminus p\mathbf{N}$. On note m le degré de P et, puisque $\mathbf{P}$ est infini, on dispose de $m+1$ nombres premiers distincts $(p_i)_{0\leq i\leq m}$. Les équations $P(p_i-a)\in\mathbf{Z}$ fournissent un système linéaire de matrice associée une matrice de Vandermonde inversible, puisque les p_i sont distincts, et donc la solution est donnée par les coefficients de P relativement à la base $((X-a)^i)_{0\leq i\leq m}$. Ceux-ci sont donc obtenus par les formules de CRAMER et ainsi sont rationnels. Or P n'a qu'un nombre fini de coefficients non nuls, on dipose ainsi de ω entier et c_0, …, c_m dans $\mathbf{Z}_{(p)}$ tels que $p^\omega P=\sum_{i=0}^{m}c_i(X-a)^i$.

Puisque a n'appartient pas à $p\mathbf{N}$, il est premier à p et donc à p^ω. D'après le théorème de DIRICHLET, on dispose alors de k entier naturel tel que $a+kp^\omega$ soit premier et donc tel que $P(a+kp^\omega)$ soit dans $\mathbf{Z}_{(p)}$. Or

$$P(a+kp^\omega)-P(a)=\sum_{i=1}^{m}k^ip^{(i-1)\omega}c_i$$

et donc $P(a+kp^\omega)-P(a)$ appartient à $\mathbf{Z}_{(p)}$ puisque ce dernier est un anneau contenant $\mathbf{Z}$. Il en résulte que $P(a)$ appartient lui aussi à $\mathbf{Z}_{(p)}$ et donc $\boxed{\mathcal{P}(\mathbf{P},\mathbf{Z}_{(p)})\subset\mathcal{P}(\mathbf{N}\setminus p\mathbf{N},\mathbf{Z}_{(p)}).}$

b) L'inclusion résulte de la question précédente puisque $E_p\subset\mathbf{P}\cup(\mathbf{N}\setminus p\mathbf{N})$ et l'inclusion réciproque du fait que $\mathbf{P}$ est inclus dans E_p puisque tout nombre premier autre que p est premier à p et appartient donc à $\mathbf{N}\setminus p\mathbf{N}$. Il vient donc $\boxed{\mathcal{P}(\mathbf{P},\mathbf{Z}_{(p)})=\mathcal{P}(E_p,\mathbf{Z}_{(p)}).}$

IV.3) Un rationnel est entier si et seulement si son dénominateur n'est divisible par aucun nombre premier et donc $\mathbf{Z}=\bigcap_{p\in\mathbf{P}}\mathbf{Z}_{(p)}$. On en déduit

$$\mathcal{P}(\mathbf{P},\mathbf{Z})=\bigcap_{p\in\mathbf{P}}\mathcal{P}(\mathbf{P},\mathbf{Z}_{(p)})$$

et donc, en utilisant la question précédente $\boxed{\mathcal{P}(\mathbf{P},\mathbf{Z})=\bigcap_{p\in\mathbf{P}}\mathcal{P}(E_p,\mathbf{Z}_{(p)}).}$

IV.4) Si Q appartient à $\mathcal{P}(\mathbf{P},\mathbf{Z})$, alors pour tout nombre premier p, en particulier inférieur à $m+1$, $Q(p)$ est entier. De plus, en utilisant IV.2.a) on en déduit que Q appartient à $\mathcal{P}(\mathbf{N}\setminus p\mathbf{N},\mathbf{Z}_{(p)})$. On en déduit, grâce à III.6.b) que les coefficients de $p^{\omega_p(m)}Q$ sont dans $\mathbf{Z}_{(p)}$ et donc aussi ceux de $p^{2m}Q$, en vertu de III.3.a). Il en résulte que $X^{2m}Q$ prend des valeurs dans $\mathbf{Z}_{(p)}$ sur

$p\mathbf{N}$. Mais, d'après IV.3, il en va de même pour Q sur $\mathbf{N} \setminus p\mathbf{N}$ et donc a fortiori de $X^{2m}Q$. Par conséquent $X^{2m}Q$ appartient à $\bigcap_{p\in\mathbf{P}} \mathcal{P}(\mathbf{Z}, \mathbf{Z}_{(p)})$, et prend donc des valeurs entières sur $\mathbf{Z}$, donc en particulier sur $[\![1; 2m+1]\!]$.

Réciproquement si, pour tout entier naturel $k \leq 2m+1$, $k^{2m}Q(k)$ appartient à $\mathbf{Z}$ alors, pour j dans $[\![1; m]\!]$ et p dans $\mathbf{P}$, on a $\varphi_p(j) \leq \varphi_p(m) \leq m + 1 + \dfrac{m}{p-1} \leq 2m+1$ et donc $\varphi_p(k)^{2m}Q(\varphi_p(k))$ appartient à $\mathbf{Z}_{(p)}$ et donc aussi $Q(\varphi_p(k))$ puisque $\varphi_p(k)$ est premier à p. On en déduit, en utilisant III.6.a), que Q appartient à $\mathcal{P}(\mathbf{N} \setminus p\mathbf{N}, \mathbf{Z}_{(p)})$.

D'après III.6.b) cela entraîne que les coefficients de $p^{\omega_p(m)}Q$ sont dans $\mathbf{Z}_{(p)}$ et donc, pour $p > m+1$, en utilisant III.3.b), $Q(p)$ appartient à $\mathbf{Z}_{(p)}$, ce qui implique que Q appartient à $\mathcal{P}(E_p, \mathbf{Z}_{(p)})$.

Si, pour $p \leq m+1$, $Q(p)$ est entier, il est a fortiori dans $\mathbf{Z}_{(p)}$ et on conclut encore que Q appartient à $\mathcal{P}(E_p, \mathbf{Z}_{(p)})$. Et donc, grâce à IV.2.b), Q appartient à $\mathcal{P}(\mathbf{P}, \mathbf{Z})$. Au final

les deux propriétés sont équivalentes.

IV.5) On applique ce qui précède avec $m = 7$ et

$$Q = \frac{(X+1)(X-1)(X-2)(X-3)(X-5)(X-7)(X-193)}{2\ 903\ 040}.$$

Pour p premier inférieur à 8, on a $Q(p) = 0$ et donc la première propriété est vérifiée. On décompose 2 903 040 en facteurs premiers. On trouve successivement $2\ 903\ 040 = 40 \times 72\ 576$, $72\ 576 = 4 \times 18\ 144$, $18\ 144 = 4 \times 4\ 536$, $4\ 536 = 4 \times 1\ 134$, $1\ 134 = 2 \times 567$, $567 = 9 \times 63$ et donc $2\ 903\ 040 = 2^{10} \times 3^4 \times 5 \times 7$. Il s'agit donc de vérifier que, pour $1 \leq k \leq 15$, $k^{14}(k+1)(k-1)(k-2)(k-3)(k-5)(k-7)(k-193)$ est divisible par 2^{10}, par 3^4, par 5 et par 7. Or

- On a $-1 \equiv 6 \bmod 7$ et $193 \equiv 4 \bmod 7$, donc on a $(k+1)(k-1)(k-2)(k-3)(k-5)(k-7)(k-193) \equiv (k-1)(k-2)(k-3)(k-4)(k-5)(k-6)(k-7) \bmod 7$ et ce dernier produit est nul modulo 7.
- De même $-1 \equiv 4 \bmod 5$, donc on a $(k+1)(k-1)(k-2)(k-3)(k-5) \equiv (k-1)(k-2)(k-3)(k-4)(k-5) \bmod 5$ et ce dernier produit est nul modulo 5.
- Modulo 9, on a $-1 \equiv 8 \bmod 9$ et $193 \equiv 4 \bmod 9$, donc si $k \equiv 2 \bmod 3$, alors l'un des termes parmi $k+1$, $k-2$ et $k-5$ est divisible par 9 tandis que les deux autres sont divisibles par 3. Donc leur produit est divisible par 3^4. Si $k \equiv 1 \bmod 3$, alors la même propriété est vraie pour les termes $k-1$, $k-7$ et $k-193$. Enfin si $k \equiv 0 \bmod 3$, alors 3^4 divise k^{14}. Donc dans tous les cas le produit $k^{14}(k+1)(k-1)(k-2)(k-3)(k-5)(k-7)(k-193)$ est divisible par 3^4.
- Enfin si k est pair, 2^{10} divise k^{14}. Sinon on raisonne modulo 8 en remarquant que 193 est congru à 1 modulo 8. Les termes $k+1$, $k-1$, $k-3$, $k-5$, $k-7$ et $k-193$ forment donc modulo 8 une suite arithmétique de raison -2, de termes congrus à 0 modulo 2. Il en résulte que parmi eux se trouvent au moins un terme divisible par 8, deux autres divisibles par 4 et trois autres divisibles par 2. Le produit est donc divisible par 2 à la puissance $3 + 2 \times 2 + 3 \times 1$, i.e. 10.

On a donc, pour p premier,

$$(p+1)(p-1)(p-2)(p-3)(p-5)(p-7)(p-193) \equiv 0 \pmod{2\ 903\ 040}.$$