Cinquième composition de mathématiques [corrigé]

Problème. Polynômes à valeurs entières et factorielles de Bhargava.

Partie I. Généralités sur $\mathscr{G}$.

1. (a) Montrer que $\mathscr{G}$ est un sous-anneau de $\mathbb{R}[X]$.

   - *Le polynôme* 1 *est clairement à valeurs entières :* $1 \in \mathscr{G}$.
   - *Soit* $P, Q \in \mathscr{G}$.
     Pour tout $z \in \mathbb{Z}$, *on a* $(P-Q)(z) = \underbrace{P(z)}_{\in\mathbb{Z}} - \underbrace{Q(z)}_{\in\mathbb{Z}} \in \mathbb{Z}$ *et* $(PQ)(z) = \underbrace{P(z)}_{\in\mathbb{Z}}\underbrace{Q(z)}_{\in\mathbb{Z}} \in \mathbb{Z}$.
     Cela montre $P - Q \in \mathscr{G}$ *et* $PQ \in \mathscr{G}$, *et conclut.*

   (b) L'anneau $\mathscr{G}$ est-il intègre ?

   Oui.

   - *Il est déjà commutatif et non nul.*
   - *Ensuite, soit* $P, Q \in \mathscr{G}$ *tels que* $PQ = 0$.
     Par intégrité de $\mathbb{R}[X]$, *on a* $P = 0$ *ou* $Q = 0$, *ce qui conclut.*

   Remarque. *On a en fait montré que tout sous-anneau d'un anneau intègre est intègre.*

   (c) Déterminer le groupe des inversibles $\mathscr{G}^\times$.

   Soit $P \in \mathscr{G}^\times$. *On peut donc trouver* $Q \in \mathscr{G}$ *tel que* $PQ = 1$.
   En particulier, on a $\deg P + \deg Q = 0$, *ce qui montre que* P *et* Q *sont des polynômes constants non nuls.*
   On a en particulier $\underbrace{P(0)}_{\in\mathbb{Z}}\underbrace{Q(0)}_{\in\mathbb{Z}} = 1$, *d'où l'on tire* $P(0) = \pm 1$ *et, par constance,* $P = \pm 1$.
   La réciproque étant immédiate, on a donc $\mathscr{G}^\times = \{\pm 1\}$.

2. Soit p un nombre premier.

   (a) Montrer que $\dfrac{1}{p}(X^p - X) \in \mathscr{G}$.

   C'est une reformulation directe du petit théorème de Fermat.

   (b) En déduire que l'inclusion $\mathbb{Z}[X] \subseteq \mathscr{G}$ est stricte.

   La question précédente montre notamment que $\dfrac{1}{2}X^2 - \dfrac{1}{2}X \in \mathscr{G}$.
   Comme $\dfrac{1}{2} \notin \mathbb{Z}$, *on a* $\dfrac{1}{2}X^2 - \dfrac{1}{2}X \notin \mathbb{Z}[X]$, *ce qui montre* $\mathscr{G} \not\subseteq \mathbb{Z}[X]$, *et conclut.*

3. (a) Soit $P \in \mathscr{G}$ et $n > \deg P$ un entier. Exprimer P en fonction des polynômes $L_{n,0}, \dots, L_{n,n-1}$.

   D'après la formule d'interpolation de Lagrange (comme $P \in \mathbb{R}_{n-1}[X]$*), on a*

   $$P = \sum_{k=0}^{n-1} P(k)\, L_{n,k}.$$

(b) En déduire $\mathscr{G} \subseteq \mathbb{Q}[X]$.

Il est clair que chaque polynôme $\dfrac{X-j}{k-j}$ *est élément de* $\mathbb{Q}[X]$. *Par stabilité par produit, il en va de même des polynômes* $L_{n,k}$.

Soit maintenant $P \in \mathscr{G}$. *La formule* $P = \sum_{k=0}^{n-1} \underbrace{P(k)}_{\in\mathbb{Z}} L_{n,k}$ *montre alors que* $P \in \mathbb{Q}[X]$, *ce qui conclut.*

Partie II. Interpolation de Newton dans $\mathbb{Z}[X]$.

Dans toute cette partie, on fixe n réels $a_0, a_1, \ldots, a_{n-1} \in \mathbb{R}$.

4. **Unicité.** Soit $b_0, b_1, \ldots, b_n, c_0, c_1, \ldots, c_n \in \mathbb{R}$.
On suppose $\sum_{k=0}^{n} b_k(X-a_0)(X-a_1)\cdots(X-a_{k-1}) = \sum_{k=0}^{n} c_k(X-a_0)(X-a_1)\cdots(X-a_{k-1})$.

(a) Montrer $b_0 = c_0$.

Pour tout $k \geqslant 1$, *on a* $\big((X-a_0)(X-a_1)\cdots(X-a_{k-1})\big)(a_0) = 0$.
En évaluant en 0 *l'égalité de l'énoncé, les sommes s'effondrent donc et l'on obtient* $b_0 = c_0$.

(b) Plus généralement, montrer $\forall j \in [\![0,n]\!], b_j = c_j$.

Pour tout $j \in [\![0,n]\!]$, *on note* $A(j)$ *l'assertion* $b_j = c_j$.
Montrons $\forall j \in [\![0,n]\!]$ *par récurrence forte finie ascendante.*

Initialisation. *L'assertion* $A(0)$ *a été montrée à la question précédente.*

Hérédité. *Soit* $j \in [\![0,n-1]\!]$ *tel que* $A(0)$ *et* $A(1)$ *et* $\cdots$ *et* $A(j)$.
On a donc, après simplification,

$$\sum_{k=j+1}^{n} b_k(X-a_0)(X-a_1)\cdots(X-a_{k-1}) = \sum_{k=j+1}^{n} c_k(X-a_0)(X-a_1)\cdots(X-a_{k-1}),$$

ce qui donne après factorisation

$$(X-a_0)(X-a_1)\cdots(X-a_j)\left[\sum_{k=j+1}^{n}(b_k-c_k)(X-a_{j+1})\cdots(X-a_{k-1})\right] = 0.$$

Par intégrité, on en déduit $\sum_{k=j+1}^{n}(b_k-c_k)(X-a_{j+1})\cdots(X-a_{k-1}) = 0$, *puis* $b_{j+1}-c_{j+1}=0$ *en évaluant en* a_{j+1}.
Cela montre $A(j+1)$ *et clôt la récurrence.*

5. Soit $P \in \mathbb{Z}[X]$ et $a \in \mathbb{Z}$.

(a) Soit $k \in \mathbb{N}$. Montrer l'existence d'un polynôme $Q_k \in \mathbb{Z}[X]$ tel que $X^k = (X-a)Q_k + a^k$.

- *Si* $k = 0$, $Q_k = 0$ *convient trivialement.*
- *Supposons* $k \in \mathbb{N}^*$. *On a alors*

$$X^k - a^k = (X-a)\sum_{j=0}^{k-1} a^{k-1-j}X^j,$$

ce qui conclut, en posant $Q_k = \sum_{j=0}^{k-1} a^{k-1-j}X^j$.

(b) Montrer l'existence d'un polynôme $Q \in \mathbb{Z}[X]$ tel que $P - P(a) = (X - a)Q$.

On utilise les notations de la question précédente.

On peut par ailleurs trouver $a_0, \dots, a_n \in \mathbb{Z}$ *tels que* $P = \sum_{k=0}^{n} a_k X^k$.

On a alors

$$P - P(a) = \sum_{k=0}^{n} a_k (X^k - a^k) = (X - a) \sum_{k=0}^{n} a_k Q_k,$$

ce qui conclut, car $\sum_{k=0}^{n} a_k Q_k \in \mathbb{Z}[X]$.

6. **Interpolation de Newton dans** $\mathbb{Z}[X]$**.** Soit $P \in \mathbb{Z}[X]$ et $n \geqslant \deg P$ un entier.
On suppose $a_0, \dots, a_{n-1} \in \mathbb{Z}$.
Montrer qu'il existe un unique $(n+1)$-uplet $(b_0, b_1, \dots, b_{n-1}, b_n) \in \mathbb{Z}^n$ tel que

$$P = \sum_{k=0}^{n} b_k (X - a_0)(X - a_1) \cdots (X - a_{k-1}).$$

Pour tout $n \in \mathbb{N}$*, on note* $A(n)$ *l'assertion*

« pour tout polynôme $P \in \mathbb{Z}[X]$ *de degré* $\leqslant n$ *et tout* n*-uplet* $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{Z}^n$*, il existe un* $(n+1)$*-uplet* $(b_0, b_1, \dots, b_n) \in \mathbb{Z}^n$ *tel que* $P = \sum_{k=0}^{n} b_k (X - a_0) \cdots (X - a_{k-1})$. »

Montrons $\forall n \in \mathbb{N}, A(n)$ *par récurrence.*

Initialisation. *L'assertion* $A(0)$ *est essentiellement triviale : un polynôme de degré* $\leqslant 0$ *est constant, et il suffit de prendre* $b_0 = P(0)$.

Hérédité. *Soit* $n \in \mathbb{N}$ *tel que* $A(n)$*. Montrons* $A(n+1)$.

Soit $P \in \mathbb{Z}[X]$ *de degré* $\leqslant n+1$ *et* $a_0, \dots, a_n \in \mathbb{Z}$.

En appliquant ce qui précède à $a_0 \in \mathbb{Z}$*, on obtient* $Q \in \mathbb{Z}[X]$ *tel que* $P = P(a_0) + (X - a_0)Q$.

Par stabilité par combinaison linéaire, la différence $(X - a_0)Q = P - P(a_0)$ *est de degré* $\leqslant n+1$*, donc l'égalité* $\deg\big((X - a_0)Q\big) = \deg Q + 1$ *montre que* $\deg Q \leqslant n$.

On peut alors appliquer $A(n)$ *au polynôme* Q *et au* n*-uplet* $(a_1, \dots, a_n)$ *: on obtient ainsi un* $(n+1)$*-uplet* $\widetilde{b}_0, \dots, \widetilde{b}_n$ *tel que* $Q = \sum_{k=0}^{n} \widetilde{b}_k (X - a_1) \cdots (X - a_{k-1})$.

On en déduit

$$P = P(a_0) + (X - a_0) \sum_{k=0}^{n} \widetilde{b}_k (X - a_1) \cdots (X - a_{k-1}) = \sum_{\ell=0}^{n+1} b_\ell (X - a_0) \cdots (X - a_{\ell-1}),$$

en posant $b_0 = P(a_0)$ *et, pour tout* $\ell \in [\![1, n+1]\!]$, $b_\ell = \widetilde{b}_{\ell-1}$.

Cela démontre $A(n+1)$ *et clôt la récurrence.*

On a ainsi montré l'existence d'une telle décomposition, et la question 4 assure l'unicité.

Partie III. Structure additive de $\mathscr{G}$.

7. Soit $k \in \mathbb{N}$.

   (a) Déterminer le degré et le coefficient dominant du polynôme H_k.

   - *Le polynôme* H_k *est le produit de* k *polynômes de degré* 1, *donc* $\deg H_k = k$.
   - *Le polynôme* $X(X-1)\cdots(X-k+1)$ *est clairement unitaire, donc le coefficient dominant de* H_k *est* $\dfrac{1}{k!}$.

   (b) Montrer $H_k \circ (k-1-X) = (-1)^k H_k$.

   C'est un calcul : en faisant notamment le changement d'indices $[\lambda = k-1-\ell, \ell = k-1-\lambda]$, *on a*

$$H_k \circ (k-1-X) = \frac{1}{k!}\prod_{\ell=0}^{k-1}(k-1-X-\ell) = \frac{1}{k!}\prod_{\lambda=0}^{k-1}(\lambda - X) = \frac{(-1)^k}{k!}\prod_{\lambda=0}^{k-1}(X-\lambda) = (-1)^k H_k.$$

   (c) Montrer $H_k \in \mathscr{G}$.

   Soit $z \in \mathbb{Z}$.

   - *Si* $z \geqslant k$, *on a* $H_k(z) = \dfrac{z(z-1)\cdots(z-k+1)}{k!} = \dbinom{z}{k} \in \mathbb{Z}$.
   - *Si* $z \in [\![0, k-1]\!]$, *on a immédiatement* $H_k(z) = 0 \in \mathbb{Z}$.
   - *Si* $z < 0$, *on a* $k-1-z \geqslant k$, *donc* $H_k(z) = (-1)^k H_k(k-1-z) \in \mathbb{Z}$ *en utilisant la question précédente, et en se ramenant au premier cas.*

   Cela montre $H_k \in \mathscr{G}$.

8. Soit $P \in \mathbb{Q}_n[X]$.

   (a) En utilisant ce qui précède, montrer qu'il existe un unique $(n+1)$-uplet $(b_0, \ldots, b_n) \in \mathbb{Q}^{n+1}$ tel que $P = \displaystyle\sum_{k=0}^{n} b_k H_k$.

   Si m *est (par exemple) le produit des dénominateurs des coefficients de* P, *on a* $mP \in \mathbb{Z}[X]$.
   D'après la question 6, appliquée à $mP \in \mathbb{Z}[X]$, $n+1 \in \mathbb{N}$ *et* $(a_0, \ldots, a_n) = (0, \ldots, n)$, *on peut trouver des entiers* $\widetilde{b}_0, \ldots, \widetilde{b}_n \in \mathbb{Z}$ *tels que* $mP = \displaystyle\sum_{k=0}^{n} \widetilde{b}_k X(X-1)\cdots(X-k+1)$.

   On en déduit

$$P = \sum_{k=0}^{n} \underbrace{\frac{k!\,\widetilde{b}_k}{m}}_{\in\mathbb{Q}} H_k,$$

   ce qui montre déjà l'existence.
   L'unicité provient directement de la question 4.

   (b) On suppose en outre $P \in \mathscr{G}$. Montrer $\forall k \in [\![0, n]\!], b_k \in \mathbb{Z}$.

   Pour tout $j \in [\![0, n]\!]$, *on note* $A(j)$ *l'assertion* $b_j \in \mathbb{Z}$.
   Montrons $\forall j \in [\![0, n]\!], A(j)$ *par récurrence finie forte.*

   Initialisation. *On a* $H_0 = 1$ *et* $\forall j \in \mathbb{N}^*, H_j(0) = 0$.
   En évaluant en 0 *l'expression de* P, *les sommes s'effondrent donc et il reste* $P(0) = b_0$, *ce qui montre* $b_0 \in \mathbb{Z}$, *c'est-à-dire* $A(0)$.

Hérédité. *Soit* $j \in [\![0, n-1]\!]$ *tel que* $A(0)$ *et* $\cdots$ *et* $A(j)$.

En particulier, comme les polynômes H_k *appartiennent à* $\mathscr{G}$*, on a que*

$$P_0 = \sum_{k=0}^{j} \underbrace{b_k}_{\in\mathbb{Z}} H_k \in \mathscr{G},$$

car $\mathscr{G}$ *est un sous-anneau (et donc en particulier un sous-groupe additif) de* $\mathbb{R}[X]$.

On a alors $P - P_0 = \sum_{k=j+1}^{n} b_k H_k \in \mathscr{G}$.

Or, on a $H_{j+1}(j+1) = \dfrac{(j+1)j\cdots 1}{(j+1)!} = 1$ *et* $\forall k \geqslant j+2, H_k(j+1) = 0$.

En évaluant en $j+1$*, la somme s'effondre donc et l'on obtient* $b_{j+1} = (P - P_0)(j+1) \in \mathbb{Z}$.

Cela montre $A(j+1)$*, et clôt la récurrence.*

Partie IV. Théorème de Pólya (1915).

9. Déterminer $\delta_{\mathbb{Z}}(X^7 - X)$.

   - *On a*
     - $2^7 - 2 = 2(2^6 - 1) = 2 \times 63 = 2 \times 3^2 \times 7$;
     - $3^7 - 3 = 3(3^6 - 1) = 2 \times 3 \times 728 = 2^3 \times 3 \times 7 \times 13$,

     donc $(2^7 - 2) \wedge (3^7 - 3) = 2 \times 3 \times 7 = 42$.

     Cela montre déjà $\delta_{\mathbb{Z}}(X^7 - X) \mid 42$.
   - *Soit* $n \in \mathbb{Z}$.
     - *Comme* $0^7 = 0$ *et* $1^7 = 1$*, on a nécessairement* $n^7 \equiv n \pmod 2$;
     - *De même, comme* $0^7 = 0$, $1^7 = 1$ *et* $(-1)^7 = -1$*, on a nécessairement* $n^7 \equiv n \pmod 3$;
     - *enfin, d'après le petit théorème de Fermat (pour le premier 7), on a* $n^7 \equiv n \pmod 7$.

     Cela montre que $n^7 - n$ *est divisible par les nombres premiers 2, 3 et 7.*

     D'après le lemme de Gauss, on en déduit que $42 = 2 \times 3 \times 7 \mid n^7 - n$.

   In fine, *on a obtenu* $\delta_{\mathbb{Z}}(X^7 - X) = 42$.

10. Soit $P \in \mathbb{Z}[X]$ unitaire, de degré $n \in \mathbb{N}$. Montrer $\delta_{\mathbb{Z}}(P) \mid n!$.

    Le polynôme n'étant pas nul, le critère radical de nullité entraîne qu'il ne s'annule pas sur $\mathbb{Z}$ *tout entier, si bien que le PGCD* $\delta_{\mathbb{Z}}(P) \in \mathbb{N}^*$ *est bien défini.*

    Par construction, on a $\dfrac{P}{\delta_{\mathbb{Z}}(P)} \in \mathscr{G}$*, donc on peut trouver, d'après la question 6,* $b_0, \ldots, b_n \in \mathbb{Z}$ *tels que*

    $$\frac{P}{\delta_{\mathbb{Z}}(P)} = \sum_{k=0}^{n} b_k H_k.$$

    Comme P *est unitaire, la comparaison des coefficients dominants donne*

    $$\frac{1}{\delta_{\mathbb{Z}}(P)} = \frac{b_n}{n!},$$

    ce qui donne $n! = b_n\, \delta_{\mathbb{Z}}(P)$*, et montre que* $\delta_{\mathbb{Z}}(P) \mid n!$.

11. Réciproquement, montrer qu'il existe $P \in \mathbb{Z}[X]$ unitaire, de degré $n \in \mathbb{N}$, tel que $\delta_{\mathbb{Z}}(P) = n!$.

On a $P = X(X-1)\cdots(X-n+1) = n!\,H_n$, *qui est clairement unitaire et de degré* n.
Comme $H_n \in \mathscr{G}$, *on voit que, pour tout* $z \in \mathbb{Z}$, $n! \mid n!\,H_n(z) = P(z)$, *ce qui montre que* $n! \mid \delta_{\mathbb{Z}}(P)$.
La question précédente donne la divisibilité dans l'autre sens, ce qui conclut : $\delta_{\mathbb{Z}}(P) = n!$.

Partie V. Factorielles de Bhargava (1997).

Dans toute cette partie, on fixe $S \subseteq \mathbb{Z}$ infini.

12. Dans cette question, on prend $S = \mathbb{Z}$.
Montrer que la suite $(n)_{n\in\mathbb{N}}$ est p-ordonnée, pour tout nombre premier p.

Soit $n \in \mathbb{N}$ *et* p *un nombre premier. Soit* $x \in \mathbb{Z}$. *Il s'agit donc de montrer*

$$v_p(n!) = v_p\big((n-0)(n-1)\cdots(n-(n-1))\big) \leqslant v_p\big((x-0)(x-1)\cdots(x-(n-1))\big).$$

Or, le produit $x(x-0)\cdots(x-n+1)$ *apparaissant à droite est le produit de* n *entiers consécutifs. Il est donc divisible par* $n!$ *comme on l'a montré à la question 7c : on dit simplement que* $H_n(x) \in \mathbb{Z}$.
En passant à la valuation p*-adique, on a donc l'inégalité demandée.*

13. Soit $n \in \mathbb{N}$. Soit p un nombre premier et $(a_n)_{n\in\mathbb{N}}$ une suite p-ordonnée d'éléments de S.
Montrer que si p est suffisamment grand, alors $\omega_p(n, S) = 1$.

Il suffit par exemple de remarquer que si p *est strictement supérieur à tous les distances de la famille* $\big(|a_i - a_j|\big)_{0\leqslant i<j\leqslant n}$, *alors il ne divise aucune différence* $a_i - a_j$ *(car les éléments sont distincts, donc ces différences ne sont pas nulles), donc on a* $\omega_p(n, S) = w_p\big((a_n - a_0)\cdots(a_n - a_{n-1})\big) = 1$.

Grâce à la question précédente, on définit, pour tout entier n, la *factorielle de Bhargava* associée à l'ensemble S :

$$n!_S = \prod_p \omega_p(n, S),$$

où le produit court sur l'ensemble des nombres premiers tels que $\omega_p(n, S) > 1$, qui est fini d'après la question précédente.
Là encore, le nombre $n!_S$ dépend *a priori* du choix de la suite p-ordonnée, même si la notation ne la mentionne pas.

14. Pour tout $n \in \mathbb{N}$, calculer $n!_{\mathbb{Z}}$ et $n!_{2\mathbb{Z}}$ (à l'aide de suites p-ordonnées bien choisies).

- *Commençons par le cas* $S = \mathbb{Z}$.
Soit p *un nombre premier. Comme* $(n)_{n\in\mathbb{N}}$ *est* p*-ordonnée, on aura, pour tout* p *premier et tout* $n \in \mathbb{N}$,

$$\omega_p(\mathbb{Z}, p) = w_p\big((n-0)\cdots(n-(n-1))\big) = w_p(n!),$$

donc $n!_{\mathbb{Z}} = \prod_p w_p(n!) = n!$.

- *Dans le cas* $S = 2\mathbb{Z}$, *on voit directement que, quels que soient* $a_0 = 2b_0, \ldots, a_n = 2b_n$,

$$v_p\big((a_n - a_0)\cdots(a_n - a_{n-1})\big) = \begin{cases} p + v_p\big((b_n - b_0)\cdots(b_n - b_{n-1})\big) & \text{si } p = 2 \\ v_p\big((b_n - b_0)\cdots(b_n - b_{n-1})\big) & \text{sinon,} \end{cases}$$

donc, pour tout entier n,

$$n!_{2\mathbb{Z}} = \omega_2(2\mathbb{Z}, n) \prod_{p>2} \omega_p(2\mathbb{Z}, n) = 2^n\,\omega_2(\mathbb{Z}, n) \prod_{p\geqslant 3} \omega_p(\mathbb{Z}, n) = 2^n\,n!.$$

15. On va montrer dans les deux questions suivantes une généralisation du théorème de Pólya.
    (a) Soit p un nombre premier, $(a_n)_{n\in\mathbb{N}}$ une suite p-ordonnée d'éléments de S et $r \in \mathbb{N}$.

    Soit $b_0, b_1, \dots, b_n \in \mathbb{Z}$ et $P = \sum_{k=0}^{n} b_k(X-a_0)(X-a_1)\cdots(X-a_{k-1})$.

    Montrer l'équivalence

    $$\big(\forall z \in S, p^r \mid P(z)\big) \Leftrightarrow \big(\forall k \in [\![0,n]\!], \forall z \in S, p^r \mid b_k(z-a_0)(z-a_1)\cdots(z-a_{k-1})\big).$$

    - *L'implication réciproque est triviale, par somme.*
    - *Montrons l'implication directe par contraposée : on suppose qu'il existe au moins un indice* $k \in [\![0,n]\!]$ *tel que* $\exists z \in S : p^r \nmid b_k(z-a_0)(z-a_1)\cdots(z-a_{k-1})$.
      Choisissons alors un tel indice $j \in [\![0,n]\!]$*, minimal pour cette propriété, et un* $z \in S$ *pour lequel* $p^r \nmid b_k(z-a_0)(z-a_1)\cdots(z-a_{k-1})$.
      Comme la suite $(a_n)_{n\in\mathbb{N}}$ *est* p*-ordonnée, on a*

      $$\nu_p\big((a_j-a_0)(a_j-a_1)\cdots(a_j-a_{j-1})\big) \leqslant \nu_p\big((z-a_0)(z-a_1)\cdots(z-a_{j-1})\big)$$
      donc $\quad \nu_p\big(b_j\,(a_j-a_0)(a_j-a_1)\cdots(a_j-a_{j-1})\big) \leqslant \nu_p\big(b_j\,(z-a_0)(z-a_1)\cdots(z-a_{j-1})\big) < r.$

      En évaluant P *en* a_j*, une partie des termes disparaît et on obtient*

      $$P(a_j) = \sum_{k=0}^{j-1} b_k(z-a_0)(z-a_1)\cdots(z-a_{k-1}) + b_j\,(a_j-a_0)(a_j-a_1)\cdots(a_j-a_{j-1}).$$

      Par minimalité de j*, les termes apparaissant dans la somme sont tous multiples de* p^r*, alors que le terme sorti de la somme ne l'est pas, d'après ce qui précède.*
      On en déduit $p^r \nmid P(a_j)$*, ce qui montre notamment non*$(\exists z \in S : p^r \mid P(z))$*, et conclut.*

    (b) Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré n.
    En utilisant la question précédente, montrer que $\delta_S(P)$ divise $n!_S$.

    On écrit $P = \sum_{k=0}^{n} b_k(X-a_0)(X-a_1)\cdots(X-a_{k-1})$*, comme dans la question précédente. Comme* P *est unitaire, on a* $b_n = 1$ *en examinant les coefficients dominants.*
    Soit p *un nombre premier. Notons* $r = \nu_p(\delta_S(P))$.
    Par construction, on a $\forall z \in S, p^r \mid P(z)$*, donc la question précédente nous apprend notamment que*

    $$\forall z \in S, p^r \mid (z-a_0)(z-a_1)\cdots(z-a_{k-1}).$$

    En appliquant cela à $z = a_n$*, on a donc* $\nu_p\big((a_n-a_0)(a_n-a_1)\cdots(a_n-a_{n-1})\big) \geqslant r$*, ce qui donne*

    $$\nu_p(\delta_S(p)) \leqslant \nu_p\big((a_n-a_0)(a_n-a_1)\cdots(a_n-a_{n-1})\big) = \nu_p(n!_S).$$

    Cette inégalité étant vraie pour tout nombre premier p*, on a* $\delta_S(p) \mid n!_S$.

16. Soit $n \in \mathbb{N}$. On veut construire un polynôme $P \in \mathbb{Z}[X]$, unitaire et de degré n tel que $\delta_S(P) = n!_S$.
    (a) Construire un tel polynôme, sous l'hypothèse supplémentaire qu'il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de S qui est p-ordonnée, pour tout nombre premier p.

    Supposons donc qu'on puisse trouver une suite $(a_n)_{n\in\mathbb{N}}$ *d'éléments de* S *qui soit* p*-ordonnée, pour tout* p.
    Considérons alors le polynôme $P = (X-a_0)(X-a_1)\cdots-(X-a_{n-1})$*, qui est bien unitaire et de degré* n*. Pour tout nombre premier* p *et tout* $z \in \mathbb{Z}$*, on a, en utilisant l'hypothèse :*

    $$\underbrace{\nu_p\big((a_n-a_0)(a_n-a_1)\cdots-(a_n-a_{n-1})\big)}_{=\nu_p(n!_S)} \leqslant \underbrace{\nu_p\big((z-a_0)(z-a_1)\cdots-(z-a_{n-1})\big)}_{=\nu_p(P(z))}.$$

    Cette inégalité étant valable pour tout p*, on obtient* $n!_S \mid P(z)$.

(b) Construire un tel polynôme, sans l'hypothèse supplémentaire.

Notons Π *l'ensemble des nombres premiers divisant* $n!_S$*, qui est un ensemble fini.*
On a notamment $n!_S = \prod_{p \in \Pi} w_p(n!_S)$.

Pour tout $p \in \Pi$ *divisant* $n!_S$*, on considère la suite* p*-ordonnée* $(a_n^{\langle p \rangle})_{n \in \mathbb{N}}$ *qui a été choisie.*
D'après le lemme chinois, on peut trouver une liste $\alpha_0, \alpha_1, \ldots, \alpha_n$ *d'entiers telle que*

$$\forall p \in \Pi, \forall k \in [\![0, n]\!], \alpha_k \equiv a_k^{\langle p \rangle} \pmod{w_p(n!_S)}.$$

En particulier, pour tout $z \in S$*, on a*

$$(z-\alpha_0)(z-\alpha_1)\cdots-(z-\alpha_{n-1}) \equiv (z-a_0^{\langle p \rangle})(z-a_1^{\langle p \rangle})\cdots-(z-a_{n-1}^{\langle p \rangle}) \equiv 0 \pmod{w_p(n!_S)},$$

ce qui montre $v_p(n!_S) \leqslant v_p\big((z-\alpha_0)(z-\alpha_1)\cdots-(z-\alpha_{n-1})\big)$.
Cela démontre, comme à la question précédente, que le polynôme unitaire $(X-\alpha_0)\cdots(X-\alpha_n)$ *convient.*

Remarque. Cette généralisation du théorème de Pólya donne une caractérisation de la factorielle de Bhargava ne faisant pas intervenir les suites p-ordonnées. Notamment, elle démontre que la factorielle $n!_S$, et les nombres $\omega_p(n, S)$ intervenant dans sa définition, ne dépendent en fait pas du choix de ces suites.

17. Soit $T \subseteq S$ une partie infinie. Montrer $\forall n \in \mathbb{N}, n!_S \mid n!_T$.

Soit $n \in \mathbb{N}$.
On peut trouver un polynôme $P \in \mathbb{Z}[X]$ *unitaire, de degré* n*, tel que* $\delta_S(P) = n!_S$.
Comme $T \subseteq S$*, on a* $\{P(z) \mid z \in T\} \subseteq \{P(z) \mid z \in S\}$*, donc* $\delta_S(P)$ *divise* a fortiori *tous les éléments de* $\{P(z) \mid z \in T\}$*, ce qui montre* $\delta_S(P) \mid \delta_T(P)$.
Enfin, on a $\delta_T(P) \mid n!_T$.
In fine, $n!_S = \delta_S(P) \mid \delta_T(P) \mid n!_T$*, ce qui conclut.*

18. Soit $a_0, a_1, \ldots, a_n$ des éléments de S.
(a) Montrer que $0!_S\, 1!_S \cdots n!_S \mid \prod_{0 \leqslant i < j \leqslant n} (a_i - a_j)$.

► *Commençons par traiter la question sous l'hypothèse (plus faible que dans l'indication) qu'il existe une partie infinie* $T \subseteq S$ *telle que, pour tout* p *premier, une suite* p*-ordonnée d'éléments de* T *commence par une permutation* $b_0^{\langle p \rangle}, \ldots, b_n^{\langle p \rangle}$ *de* $a_0, \ldots, a_n$.
Si tel est le cas, on a que $\forall j \in [\![0, n]\!], j!_S \mid j!_T$*, d'après la question précédente et on en déduit*

$$\begin{aligned}
\prod_{j=0}^{n} j!_S \mid \prod_{j=0}^{n} j!_T &= \prod_{j=0}^{n} \prod_{p} w_p(j!_T) \\
&= \prod_{j=0}^{n} \prod_{p} w_p\big((b_j^{\langle p \rangle} - b_0^{\langle p \rangle}) \cdots (b_j^{\langle p \rangle} - b_{j-1}^{\langle p \rangle})\big) \\
&= \prod_{p} w_p\left(\prod_{j=0}^{n} (b_j^{\langle p \rangle} - b_0^{\langle p \rangle}) \cdots (b_j^{\langle p \rangle} - b_{j-1}^{\langle p \rangle})\right) \\
&= \prod_{p} w_p\left(\pm \prod_{0 \leqslant i < j \leqslant n} (b_i^{\langle p \rangle} - b_j^{\langle p \rangle})\right)
\end{aligned}$$

$$= \prod_p w_p \left(\pm \prod_{0 \leqslant i < j \leqslant n} (a_i - a_j) \right)$$
$$= \left| \prod_{0 \leqslant i < j \leqslant n} (a_i - a_j) \right|.$$

où les produits indexés par p courent sur l'ensemble des nombres premiers divisant l'une des factorielles $0!_T, 1!_T, \ldots, n!_T$.
La valeur absolue ne changeant rien aux questions de divisibilité, on a bien montré dans ce cas

$$0!_S \, 1!_S \cdots n!_S \mid \prod_{0 \leqslant i < j \leqslant n} (a_i - a_j).$$

► *Le clef pour le cas général est d'appliquer ce que l'on vient de faire à $T = \{a_0, \ldots, a_n\}$. Les définitions du sujet n'ont plus de sens car T est fini, mais on voit qu'on peut :*

- *définir la notion de suite (finie) p-ordonnée $(b_i)_{i=0}^n$ pour tout premier p ;*
- *définir les quantités $\omega_p(i, S)$ et $i!_S$, tant que $i \leqslant n$;*
- *la quantité $\delta_T(P)$ reste bien définie, tant que le degré du polynôme P est $\leqslant n$, d'après le critère radical ;*
- *la question 15b et les suivantes s'adaptent tout à fait dans ce nouveau cadre, avec la même démonstration,*

si bien que l'on dispose de la relation de divisibilité

$$\forall i \in [\![0, n]\!], i!_S \mid i!_T,$$

ce qui permet à la démonstration que nous venons de donner de s'adapter dans ce contexte.

(b) **Application numérique.** Soit $p_0, p_1, \ldots, p_5$ six nombres premiers.
Montrer que $\prod_{0 \leqslant i < j \leqslant n} (p_i - p_j)$ est un multiple de 13 271 040.

► *Expliquons dans le détail comment trouver le début d'une suite 2-ordonnée $(a_n)_{n \in \mathbb{N}}$ pour l'ensemble $\mathscr{P}$ des nombres premiers.*

- *On choisit $a_0 = 2$.*
- *Quel que soit $x \in \mathscr{P}$ différent de 2 (sans quoi la valuation de la différence serait infinie, ce qui n'est pas vraiment minimal), la valuation $v_2(x-2)$ est toujours la même, à savoir 0.*
  On peut donc prendre n'importe quel nombre premier impair pour a_1, par exemple $a_1 = 3$.
- *Maintenant, quel que soit $x \in \mathscr{P}$ différent des deux premiers, on aura x impair, donc $v_2(x-2) = 0$ et $v_2(x-3) \geqslant 1$.*
  Pour garder une suite 2-ordonnée, il faut simplement éviter que la valuation $v_2(x-3)$ ne vaille au moins 2, c'est-à-dire qu'il faut choisir un nombre premier (différent des précédents et) non congru à 3 modulo 4. Le premier $a_2 = 5$ convient alors.
- *Comme il n'y a que deux classes de congruence possibles, modulo 4, pour un premier impair, on voit qu'il est ici inévitable d'avoir $v_2(x-5) \geqslant 2$ ou $v_2(x-3) \geqslant 2$ (et que l'autre sera égale à 1).*
  On minimise alors $v_2\big((x-2)(x-3)(x-5)\big)$ en choisissant x congru à 3 modulo 4, mais pas modulo 8. Le premier $a_3 = 7$ convient alors.
- *Par le même argument, on voit que la valuation minimale va maintenant être atteinte si a_4 est congru à 5 modulo 4 mais pas modulo 8 : $a_4 = 17$ convient.*

- *Les quatre classes modulo 8 d'entiers impairs étant maintenant occupées, il est inévitable d'avoir l'une des valuations $v_2(x - a_i)$ supérieure ou égale à 3, une valuation égale à 2, et les autres valuations $v_3(x - a_j)$, pour $j \neq 0$, égales à 1. Le nombre premier $a_5 = 29$ convient alors, puisque $v_3(29 - 5) = 3$.*

► *On procède alors de même pour les autres facteurs premiers (c'est plutôt de plus en plus facile) : on remarque par exemple que*

- *2, 3, 7, 5, 13, 19 est le début d'une suite 3-ordonnée ;*
- *2, 3, 5, 11, 19, 7 est le début d'une suite 5-ordonnée.*
- *pour $p \geqslant 7$, on trouve facilement six nombres premiers occupant six classes de congruence modulo p différentes, ce qui donne des valuations toutes nulles. Pour $p \geqslant 17$ il suffit d'ailleurs de considérer les six premiers nombres premiers, dans l'ordre.*

On obtient alors le tableau récapitulatif suivant.

n	0	1	2	3	4	5
$\omega_2(\mathscr{P}, n)$	0	0	1	3	4	7
$\omega_3(\mathscr{P}, n)$	0	0	0	1	1	2
$\omega_5(\mathscr{P}, n)$	0	0	0	0	0	1
$\omega_p(\mathscr{P}, n)$ $(p \geqslant 7)$	0	0	0	0	0	0

On obtient ainsi

$$0!_{\mathscr{P}} = 2^0\,3^0\,5^0 = 1, \qquad 1!_{\mathscr{P}} = 2^0\,3^0\,5^0 = 1, \qquad 2!_{\mathscr{P}} = 2^1\,3^0\,5^0 = 2,$$
$$3!_{\mathscr{P}} = 2^3\,3^1\,5^0 = 24, \qquad 4!_{\mathscr{P}} = 2^4\,3^1\,5^0 = 48, \qquad 5!_{\mathscr{P}} = 2^7\,3^2\,5^1 = 5760,$$

et l'on a le résultat demandé, avec

$$13\,271\,040 = 0!_{\mathscr{P}}\ 1!_{\mathscr{P}}\ 2!_{\mathscr{P}}\ 3!_{\mathscr{P}}\ 4!_{\mathscr{P}}\ 5!_{\mathscr{P}}.$$