# Cinquième composition de mathématiques

***Durée :*** *4 heures (aucune sortie ne sera autorisée pendant les dix dernières minutes).*

*Sauf mention explicite du contraire, tout doit toujours être parfaitement justifié.*

*La présentation de la copie est prise en compte dans l'évaluation.*

- *Ne composez pas sur la première page, ce qui me permettra d'écrire mes commentaires.*
- *Merci* $\boxed{\text{d'encadrer}}$ *ou de* $\underline{\text{souligner}}$ *vos résultats.*
- *Numérotez vos copies doubles, et rendez-les dans l'ordre.*

*Les documents, calculatrices, etc. sont* ***interdits****, même quand la question met en jeu le nombre* 13 271 040*.*

## Problème. Polynômes à valeurs entières et factorielles de Bhargava.

- On note $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients entiers.
- On définit
$$\mathscr{G} = \left\{ P \in \mathbb{R}[X] \;\middle|\; \forall z \in \mathbb{Z}, P(z) \in \mathbb{Z} \right\},$$
qui contient manifestement $\mathbb{Z}[X]$.
- Dans le sujet, on rencontrera des produits de $k$ polynômes comme $(X-a_0)(X-a_1)\cdots(X-a_{k-1})$. Il est entendu que, quand $k = 0$, ce polynôme vaut 1.
- Pour tout $k \in \mathbb{N}$, on définit le polynôme
$$H_k = \frac{X(X-1)\cdots(X-k+1)}{k!}.$$
Conformément à la convention ci-dessus, on a $H_0 = 1$.
- Pour tous entiers $0 \leqslant k < n$, on considère le *polynôme interpolateur de Lagrange*
$$L_{n,k} = \prod_{\substack{j \in [\![0,n-1]\!] \\ j \neq k}} \frac{X-j}{k-j}.$$
- On étend légèrement le cours : toute partie $E \subseteq \mathbb{Z}$ qui contient au moins un entier non nul possède un PGCD, noté $\operatorname{pgcd} E$, c'est-à-dire un entier $d \in \mathbb{N}^*$ divisant tous les éléments de $E$ et maximal pour cette propriété.
Notamment, pour tout polynôme $P$ tel que $\exists z \in S : P(z) \neq 0$, on notera
$$\delta_S(P) = \operatorname{pgcd}\left\{ P(z) \;\middle|\; z \in S \right\}$$
le PGCD des valeurs prises par le polynôme $P$ sur $S$.

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

1. (a) Montrer que $\mathscr{G}$ est un sous-anneau de $\mathbb{R}[X]$.
   (b) L'anneau $\mathscr{G}$ est-il intègre ?
   (c) Déterminer le groupe des inversibles $\mathscr{G}^\times$.
2. Soit $p$ un nombre premier.
   (a) Montrer que $\frac{1}{p}(X^p - X) \in \mathscr{G}$.
   (b) En déduire que l'inclusion $\mathbb{Z}[X] \subseteq \mathscr{G}$ est stricte.
3. (a) Soit $P \in \mathscr{G}$ et $n > \deg P$ un entier. Exprimer $P$ en fonction des polynômes $L_{n,0}, \dots, L_{n,n-1}$.
   (b) En déduire $\mathscr{G} \subseteq \mathbb{Q}[X]$.

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

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

4. **Unicité.** Soit $b_0, b_1, \dots, b_n, c_0, c_1, \dots, c_n \in \mathbb{R}$.
   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 $b_0 = c_0$.
   (b) Plus généralement, montrer $\forall j \in [\![0, n]\!], b_j = c_j$.
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 $X^k = (X-a)Q_k + a^k$.
   (b) Montrer l'existence d'un polynôme $Q \in \mathbb{Z}[X]$ tel que $P - P(a) = (X-a)Q$.
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

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

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

7. Soit $k \in \mathbb{N}$.
   (a) Déterminer le degré et le coefficient dominant du polynôme $H_k$.
   (b) Montrer $H_k \circ (k-1-X) = (-1)^k H_k$.
   (c) Montrer $H_k \in \mathscr{G}$.
8. Soit $P \in \mathbb{Q}_n[X]$.
   (a) En utilisant ce qui précède, montrer qu'il existe un unique $(n+1)$-uplet $(b_0, \dots, b_n) \in \mathbb{Q}^{n+1}$ tel que $P = \sum_{k=0}^{n} b_k H_k$.
   (b) On suppose en outre $P \in \mathscr{G}$. Montrer $\forall k \in [\![0, n]\!], b_k \in \mathbb{Z}$.

## Partie IV. Théorème de Pólya (1915).

9. Déterminer $\delta_{\mathbb{Z}}(X^7 - X)$.
10. Soit $P \in \mathbb{Z}[X]$ unitaire, de degré $n \in \mathbb{N}$. Montrer $\delta_{\mathbb{Z}}(P) \mid n!$.
11. Réciproquement, montrer qu'il existe $P \in \mathbb{Z}[X]$ unitaire, de degré $n \in \mathbb{N}$, tel que $\delta_{\mathbb{Z}}(P) = n!$.

## Partie V. Factorielles de Bhargava (1997).

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

- Pour tout nombre premier $p$ et tout entier $x \in \mathbb{Z}$, on note $v_p(x) \in \mathbb{N} \cup \{+\infty\}$ la valuation $p$-adique de $x$ et $w_p(x) = p^{v_p(x)}$ (avec la convention $p^{+\infty} = 0$, si bien que $w_p(0) = 0$).
- Étant donné un nombre premier $p$,
  - on choisit arbitrairement un élément $a_0 \in S$ ;
  - ensuite, on choisit un élément $a_1 \in S$ minimisant la valuation $p$-adique $v_p(a_1 - a_0)$, c'est-à-dire tel que
  $$v_p(a_1 - a_0) = \min\left\{ v_p(x - a_0) \;\middle|\; x \in S \right\},$$
  ce qui entraîne $a_1 \neq a_0$ ;
  - de manière générale, pour $n \in \mathbb{N}^*$, on choisit $a_n$ tel que
  $$v_p\big((a_n - a_0)(a_n - a_1)\cdots(a_n - a_{n-1})\big) = \min\left\{ v_p\big((x - a_0)(x - a_1)\cdots(x - a_{n-1})\big) \;\middle|\; x \in S \right\},$$
  ce qui entraîne $a_n \notin \{a_0, a_1, \ldots, a_{n-1}\}$.

  On obtient ainsi une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments distincts de $S$. On dira qu'une telle suite est une *suite $p$-ordonnée d'éléments de $S$*.
  En résumé, une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments d'élements de $S$ est $p$-ordonnée si et seulement si,
  $$\forall n \in \mathbb{N}^*, \forall x \in S, v_p\big((a_n - a_0)(a_n - a_1)\cdots(a_n - a_{n-1})\big) \leqslant v_p\big((x - a_0)(x - a_1)\cdots(x - a_{n-1})\big).$$
  Notons qu'une telle suite n'est pas unique.
- On définit enfin, pour tout nombre premier $p$ et tout entier $n \in \mathbb{N}$, le nombre
  $$\omega_p(n, S) = w_p\big((a_n - a_0)(a_n - a_1)\cdots(a_n - a_{n-1})\big),$$
  c'est-à-dire la puissance de $p$ qui a été minimisée lors de la $n$-ième étape de la construction.
  Notons qu'*a priori*, cette quantité dépend du choix de la suite $p$-ordonnée, même si la notation ne la mentionne pas.

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 $p$.
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 $\omega_p(n, S) = 1$.

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

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

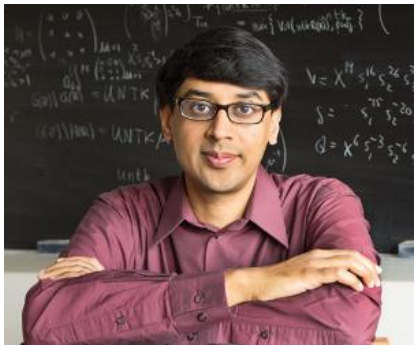
où le produit court sur l'ensemble des nombres premiers tels que $\omega_p(n, S) > 1$, qui est fini d'après la question précédente.
Là encore, le nombre $n!_S$ dépend *a priori* du choix de la suite p-ordonnée, même si la notation ne la mentionne pas.

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).
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 $b_0, b_1, \ldots, b_n \in \mathbb{Z}$ et $P = \sum_{k=0}^{n} b_k(X - a_0)(X - a_1)\cdots(X - a_{k-1})$.
    Montrer l'équivalence
    $$\big(\forall z \in S, p^r \mid P(z)\big) \Leftrightarrow \big(\forall k \in [\![0, n]\!], \forall z \in S, p^r \mid b_k(z - a_0)(z - a_1)\cdots(z - a_{k-1})\big).$$
    (b) Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $n$.
    En utilisant la question précédente, montrer que $\delta_S(P)$ divise $n!_S$.
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 $p$.
    (b) Construire un tel polynôme, sans l'hypothèse supplémentaire.

**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 $\forall n \in \mathbb{N}, n!_S \mid n!_T$.
18. Soit $a_0, a_1, \ldots, a_n$ des éléments de S.
    (a) Montrer que $0!_S\, 1!_S \cdots n!_S \mid \prod_{0\leqslant i<j\leqslant n} (a_i - a_j)$.
    ***Indication.*** *On pourra commencer par considérer le cas où il existe une partie infinie* $T \subseteq S$ *admettant une suite* p*-ordonnée, pour tout nombre premier* $p$*, commençant par* $a_0, \ldots, a_n$.
    (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.

George Pólya
(1887-1985)



Manjul Bhargava (1974–, médaillé Fields en 2014)