DÉNOMBREMENT

Les trois parties de ce devoir sont indépendantes.

1 PARTAGES ÉQUITABLES

Soient $n, p \in \mathbb{N}^*$.

1) Combien existe-t-il de partitions de l'ensemble $[\![1, np]\!]$ en p parties de cardinal n ? Le résultat final est très simple !

2) Combien existe-t-il d'applications de $[\![1, np]\!]$ dans $[\![1, p]\!]$ dont tout élément de l'image possède exactement n antécédents ?

2 INVOLUTIONS

Pour tout $n \in \mathbb{N}^*$, on note i_n le nombre d'*involutions de* $[\![1, n]\!]$, i.e. de permutations σ de $[\![1, n]\!]$ pour lesquelles : $\sigma^2 = \mathrm{Id}_{[\![1,n]\!]}$.
On pose aussi par convention : $i_0 = 1$.

1) Déterminer i_1, i_2 et i_3.

2) Montrer que pour tout $n \in \mathbb{N}$: $i_{n+2} = i_{n+1} + (n+1)i_n$. On pourra s'intéresser, pour toute involution σ de $[\![1, n+2]\!]$, à l'image de $n+2$ par σ.

On pose à présent pour tout $n \in \mathbb{N}$: $a_n = \dfrac{i_n}{n!}$ et $P_n(X) = \displaystyle\sum_{k=0}^{n} a_k X^k$.

3) a) Déterminer une relation de récurrence simple entre a_n, a_{n+1} et a_{n+2} pour tout $n \in \mathbb{N}$.

b) En déduire que pour tout $n \in \mathbb{N}$: $P'_{n+2}(X) = XP_n(X) + P_{n+1}(X)$.

Si on avait la possibilité de poser sans précaution : $f(X) = \displaystyle\sum_{k=0}^{+\infty} a_k X^k$ et de faire tendre n vers $+\infty$ dans le résultat de la question **3)b)**, f serait aussitôt l'unique solution d'un problème de Cauchy : $f'(X) = (X+1)f(X)$ et $f(0) = 1$.

4) Déterminer l'unique fonction $\varphi \in \mathscr{C}^\infty(\mathbb{R}, \mathbb{R})$ pour laquelle : $\varphi(0) = 1$ et pour tout $x \in \mathbb{R}$: $\varphi'(x) = (x+1)\varphi(x)$.

On note alors $(b_k)_{k\in\mathbb{N}}$ la suite des coefficients des développements limités de φ au voisinage de 0 : $\varphi(x) \underset{x\to 0}{=} \displaystyle\sum_{k=0}^{n} b_k x^k + \mathrm{o}\big(x^n\big)$ pour tout $n \in \mathbb{N}$.

5) Montrer que pour tout $n \in \mathbb{N}$: $(n+2)b_{n+2} = b_n + b_{n+1}$, puis que : $a_n = b_n$.

6) En déduire que pour tout $n \in \mathbb{N}$: $i_n = \displaystyle\sum_{0\leqslant 2k\leqslant n} \binom{n}{2k} \frac{(2k)!}{2^k k!}$. On commencera par écrire φ comme le produit de deux fonctions.

3 Théorèmes de Lagrange et Sylow

Ce problème est facultatif.

Soit G un groupe fini fixé une fois pour toutes. Pour toute partie X de G et pour tout $g \in G$, on pose : $\quad gX = \{gx \mid \quad x \in X\}$.
On ADMET pour gagner du temps que pour toute partie X de G et pour tous $g, g' \in G$: $\quad g(g'X) = (gg')X$.

1) Soit H un sous-groupe de G. On définit une relation $\sim_H$ sur G de la façon suivante — pour tous $x, y \in G$:
$$x \sim_H y \quad \iff \quad x^{-1}y \in H.$$

a) Montrer que $\sim_H$ est une relation d'équivalence sur G et déterminer ses classes d'équivalence.

On apelle *indice de H dans G* et on note $|G : H|$ le nombre de classes d'équivalence de la relation $\sim_H$.

b) Montrer que : $\quad |G : H| = \dfrac{|G|}{|H|}$.

Le résultat de la question **1)b)** prouve en particulier l'important *théorème de Lagrange*.

Théorème **(Théorème de Lagrange)** Soient G un groupe fini et H un sous-groupe de G. Le cardinal de H divise celui de G.

Le théorème de Lagrange a-t-il une réciproque ? Plus précisément, si d est diviseur de $|G|$, existe-t-il forcément dans G un sous-groupe de cardinal d ? La réponse est non en général, mais oui comme on va le voir si d est une puissance de nombre premier.

Soient $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}$ fixés. On fait l'hypothèse que le cardinal de G est divisible par p^α. On peut donc l'écrire sous la forme : $|G| = p^\alpha m$ pour un certain $m \in \mathbb{N}^*$. On souhaite montrer que G possède un sous-groupe de cardinal p^α.

2) **a)** Montrer que pour tout $k \in [\![1, p^\alpha - 1]\!]$: $\quad v_p\big(p^\alpha m - k\big) = v_p(k)$.

b) En déduire que : $\quad v_p\left(\binom{p^\alpha m}{p^\alpha}\right) = v_p(m)$.

On note à présent $\mathscr{P}$ l'ensemble des parties de G de cardinal p^α.

3) Montrer que pour tous $A \in \mathscr{P}$ et $x \in G$: $\quad xA \in \mathscr{P}$.

4) On définit une relation $\approx$ sur $\mathscr{P}$ de la façon suivante — pour tous $A, B \in \mathscr{P}$:
$$A \approx B \quad \iff \quad \exists\, x \in G, \quad B = xA.$$

a) Montrer que $\approx$ est une relation d'équivalence sur $\mathscr{P}$.

b) Montrer que l'une au moins des classes d'équivalence de la relation $\approx$ n'est pas de cardinal divisible par $p^{v_p(m)+1}$. On note A_0 un élément quelconque d'une telle classe d'équivalence.

On pose alors : $\quad H_0 = \{x \in G \mid \quad xA_0 = A_0\}$.

c) Montrer que H_0 est un sous-groupe de G.

d) Montrer que : $\quad |H_0| \leqslant |A_0|$.

e) Montrer que pour tous $x, y \in G$: $\quad xA_0 = yA_0 \quad \iff \quad x \sim_{H_0} y$. En déduire le cardinal de la classe d'équivalence de A_0 pour la relation $\approx$.

f) Montrer l'égalité : $\quad |H_0| = p^\alpha$.

On a finalement prouvé le résultat suivant.

Théorème **(Théorème de Sylow)** Soient G un groupe fini, $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}$. Si le cardinal de G est divisible par p^α, alors G possède un sous-groupe de cardinal p^α.

Dans le cas où p^α est la plus grande puissance de p qui divise $|G|$, les sous-groupes de cardinal p^α de G sont appelés ses *p-sous-groupes de Sylow*. La théorie des groupes finis consiste en grande partie à étudier ces sous-groupes et la manière dont ils sont plongés dans leur groupe ambiant.