Devoir à la maison n°5

La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées**.

Exercice 1 (n°259)

Pour tout entier n, on note $r(n) = \text{Card}\{(A, B) \in \mathbb{Z}^2 \mid A^2 + B^2 = n\}$.
On pose également $\chi(n) = (-1)^{(n-1)/2}$ si n est impair et $\chi(n) = 0$, sinon.

1. Montrer que $r(5) = 8$. Que vaut $r(2)$?
2. Montrer en raisonnant sur la parité de A et B que si $n \equiv 3[4]$, alors $r(n) = 0$.
3. Soit $p \in \mathcal{P}$, un nombre premier tel que $p \equiv 1[4]$. On écrit $p = 4k + 1$.
   (a) On rappelle le théorème de Wilson, démontré au DM précédent : $(p-1)! \equiv -1[p]$.
   En faisant un changement de variable $j = p - i$ dans une partie de produit, montrer que
   $$(p-1)! \equiv (-1)^{2k} \prod_{i=1}^{2k} i^2 \quad [p]$$
   (b) En déduire une racine carré de (-1) modulo p.

On note x, le reste de la division euclidienne de ce nombre par p.
Puis on applique l'algorithme d'Euclide à ces nombres p et x.
On note $r_0 = p$, $r_1 = x$ et r_{n+2} le reste de la division euclidienne de r_n par r_{n+1}.
La suite (r_n) est une suite d'entiers naturels strictement décroissante.
On note M l'indice tel que : $r_M > \sqrt{p} > r_{M+1}$.

   (c) Montrer que $p = r_{M+1}^2 + v_{M+1}^2$, où (v_n) est définie comme dans le cours.
   (d) Appliquer l'algorithme à $p = 37$.
   (e) Montrer que si $p = a^2 + b^2$, avec $a \geqslant b > 0$, alors nécessairement $a > b$.
   On admet que cette décomposition avec des nombres entiers positifs est unique.
   En déduire $r(p) = 8$.

On a montré : pour p premier, $r(p) = 0$ si $p \equiv 3[4]$ ou $p = 2$ et $r(p) = 8$ si $p \equiv 1[4]$.

4. Montrer que χ est complètement multiplicative.
5. On définit $\delta(n) = \sum_{d|n} \chi(d)$. Montrer que $\delta(n) = \sum_{\substack{d|n \\ d\equiv 1[4]}} 1 - \sum_{\substack{d|n \\ d\equiv 3[4]}} 1$.
6. (*) Montrer que $r(n) = 4\delta(n)$.
   On pourra commencer par montrer que
   — $\delta(2^\alpha q) = \delta(q)$ *pour* q *impair*
   — $\delta(q) = \begin{cases} 0 & \text{si } \exists\ s \in \mathcal{P}, s \equiv 3[4] \text{ tel que } v_s(q) \equiv 1[2] \\ \displaystyle\sum_{s\in\mathcal{P}, s\equiv 1[4]} (v_s(q)+1) & \text{sinon} \end{cases}$

Exercice 2 (n°230)

On dit qu'un groupe $(G, \star)$ opère sur un ensemble X, s'il existe une application $G \times X \to X$ $(s, x) \mapsto s \cdot x$ (ou une loi externe) vérifiant :

— $\forall\ s, t \in G,\ \forall\ x \in X,\ s \cdot (t \cdot x) = (s \star t) \cdot x$

— $\forall\ x \in X,\ e \cdot x = x$.

Enfin, pour tout $x \in X$, on note $O(x) = \{s \cdot x, s \in G\}$ (orbite ou trajectoire de x sous l'action de G).

1. Un exemple.
   On note S_n, l'ensemble des permutations (i.e. des applications bijectives) de $\mathbb{N}_n$.
   On admet que $(S_n, \circ)$ est un groupe (fini) d'élément neutre id.
   On considère l'application (loi externe) : $S_n \times \mathbb{N}_n$, $(\varphi, k) \mapsto \varphi(k)$.
   Montrer que $(S_n, \circ)$ opère (simplement = naturellement = canoniquement) sur $X = \mathbb{N}_n$
2. On note, pour tout $x \in X$, $S_x = \{s \in G \mid s \cdot x = x\}$ (stabilisateur de x).
   Montrer que, pour tout $x \in X$, S_x est un sous-groupe de G
3. On suppose que G est fini. Démontrer que pour tout $x \in X$,

$$\operatorname{card}(G) = \operatorname{card}\big(O(x)\big) \times \operatorname{card}(S_x)$$

   On pourra exploiter la relation sur G : $s \mathcal{R}_1 s' \iff s \cdot x = s' \cdot x$
4. On suppose que G et X sont finis.
   Déduire de la question précédente, que si Θ contient exactement un représentant de chacune des orbites, alors

$$\operatorname{card}(X) = \operatorname{card}(G) \sum_{x \in \Theta} \frac{1}{\operatorname{card}(S_x)}$$

   où Θ est un système de représentant des orbites.
   On pourra commencer par montrer que $X = \biguplus_{x \in \Theta} \mathcal{O}(x)$.
5. Application :
   On note $\varphi : G \times G$, $(g, x) \mapsto g \cdot x := g \star x \star g^{-1}$.
   Montrer que φ fait opérer G sur lui-même.
   Montrer qu'il existe une famille $(H_i)_{i \in I}$ finie de sous-groupe strict de G ($\neq \{e\}$ et $\neq G$) telle que

$$\operatorname{card}(G) = \operatorname{card}\big(Z(G)\big) + \sum_{i \in I} \frac{\operatorname{card}(G)}{\operatorname{card}(H_i)}$$

   On rappelle que $Z(G)$ est le sous-groupe de G, appelé le centre de G :

$$Z(G) = \{g \in G \mid \forall\ s \in G, g \star s = s \star g\}$$