FEUILLE DE TD 2, 4MA033 2025-2026

Exercice 1 (Le symbole de Legendre comme signature d'une permutation)**.** Soient p un nombre premier impair et a un entier qui n'est pas un multiple de p. Démontrer que le symbole de Legendre $\left(\frac{a}{p}\right)$ est égal à la signature de la permutation "multiplication par a" de $(\mathbb{Z}/p\mathbb{Z})^{\times}$.

Exercice 2. Soit $f \in \mathbb{Z}[\mathrm{T}]$ un polynôme non constant.

(a) Montrer qu'il existe des entiers n arbitrairement grands tels que $f(n)$ ne soit pas un nombre premier.

(b) Montrer que l'ensemble des nombres premiers qui divisent l'une des valeurs $f(n)$, pour $n \geqslant 1$, est infini.

Exercice 3 (Calcul du signe de la somme de Gauss)**.** Soit $n \geqslant 1$ un entier impair, et

$$\mathrm{G}_n = \sum_{k=0}^{n-1} \exp\left(2\pi i \frac{k^2}{n}\right).$$

On se propose de calculer la somme de Gauss G_n, incluant son signe, selon la méthode analytique inaugurée par P.L Dirichlet.

(a) On note pour $t \in [0, 1[$,

$$f(t) = \sum_{k=0}^{n-1} \exp\left(2\pi i \frac{(t+k)^2}{n}\right).$$

Démontrer que f se prolonge en une fonction 1-périodique sur $\mathbb{R}$, continue, et de classe C^1 par morceaux.

(b) Rappeler le théorème de convergence (de Dirichlet !) pour les séries de Fourier des fonctions continues et de classe C^1 par morceaux. L'appliquer au cas de f, avec $\mathrm{S_N}(f)(t) = \sum_{-\mathrm{N}}^{\mathrm{N}} c_m e^{2i\pi mt}$ la somme partielle symétrique de la série de Fourier de f.

(c) En effectuant le changement de variables $v = t + k - \frac{mn}{2}$, démontrer que

$$c_m = b_m(n) \int_{-\frac{mn}{2}}^{n-\frac{mn}{2}} e^{2i\pi v^2/n} dv,$$

avec $b_m(n) = e^{-i\pi nm^2/2}$.

(d) Calculer $b_m(n)$ en fonction de la parité de m.

(e) Pour tout entier q on pose

$$u_q = \int_{nq}^{n(q+1)} e^{2i\pi v^2/n dv} \quad \text{et} \quad v_q = \int_{n(q-\frac{1}{2})}^{n(q+\frac{1}{2})} e^{2i\pi v^2/n dv}.$$

Démontrer que $c_{2q} = u_{-q}$ et que $c_{2q+1} = (-i)^n v_{-q}$. En déduire que

$$f(0) = u_0 + \sum_{q \geqslant 1} (u_q + u_{-q}) + (-i)^n \sum_{q \geqslant 1} (v_q + v_{1-q}).$$

(f) Démontrer que $f(0) = \sqrt{n}(1 + (-i)^n)\mathrm{J}$, avec $\mathrm{J} = \int_{-\infty}^{+\infty} e^{2i\pi v^2} dv$ (on pourra justifier par une intégration par partie que l'intégrale qui définit J a du sens).

(g) Conclure, en calculant l'intégrale de Fresnel J (en cadeau bonus), que $G_n = \sqrt{n}$ si $n \equiv 1 \mod 4$, et $G_n = i\sqrt{n}$ si $n \equiv 3 \mod 4$.

Exercice 4 (Une démonstration de la loi de réciprocité quadratique)**.** (notations de l'exercice précédent).

(1) Démontrer l'égalité

$$G_{pq} = \sum_{x=0}^{p-1}\sum_{y=0}^{q-1} \exp\left(2\pi i \frac{(qx+py)^2}{pq}\right).$$

(2) Calculer $\sum_{x=0}^{p-1} \exp\left(2\pi i \frac{\ell x^2}{p}\right)$ selon que ℓ est un carré modulo p ou pas.

(3) En déduire l'égalité

$$G_{pq} = G_p G_q \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

(4) Démontrer la loi de réciprocité quadratique $(\frac{p}{q})(\frac{q}{p}) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$ en écrivant

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{G_{pq}}{\sqrt{pq}} \frac{\sqrt{p}}{G_p} \frac{\sqrt{q}}{G_q}.$$

Exercice 5 ($\varphi(n)$ tend vers l'infini)**.** On rappelle que, si $n = p_1^{k_1} \dots p_r^{k_r}$, alors l'indicatrice d'Euler satisfait l'identité $\varphi(n) = p_1^{k_1-1} \dots p_r^{k_r-1}(p_1-1)\cdots(p_r-1)$.

(a) Déterminer tous les entiers n tels que $\varphi(n) \leqslant 2$, puis $\varphi(n) \leqslant 3$.

(b) On note p_j le j-ème nombre premier. Démontrer par récurrence que $p_j > j$.

(c) En déduire que $\varphi(n) \geqslant An/\log_2(n)$ pour une constante absolue $A > 0$, et donc que $\varphi(n)$ tend vers l'infini.

Exercice 6 (Générateurs des groupes cycliques $(\mathbb{Z}/p\mathbb{Z})^\times$)**.**

(a) Trouver un générateur du groupe cyclique $(\mathbb{Z}/97\mathbb{Z})^\times$.

(b) Soit p un nombre premier de la forme $4\ell + 1$, où ℓ est un nombre premier. Démontrer que 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 7 (Valuation p-adique des factorielles)**.** Soit p un nombre premier. Écrivons n en base p, c'est-à-dire

$$n = a_0 + a_1 p + \cdots + a_r p^r \quad \text{avec } a_i \in \{0, \dots, p-1\} \text{ et } a_r \neq 0.$$

(a) Démontrer que la valuation p-adique de $n!$ est donnée par

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - (a_0 + \cdots - +a_n)}{p-1},$$

où $\lfloor x \rfloor$ désigne la partie entière d'un nombre réel x.

(b) Soit $n \geqslant 1$ un entier. Démontrer que tout nombre premier p satisfaisant à $n < p \leqslant 2n$ divise le coefficient binomial $\binom{2n}{n}$.

(c) Démontrer que le quotient de factorielles

$$\frac{n!(30n)!}{(6n)!(10n)!(15n)!}$$

est un nombre entier pour tout $n \geqslant 1$.

(d) Soient $a, b \geqslant 1$ des entiers. Démontrer que $\mathrm{ord}_p(\binom{a+b}{a})$ est le nombre de retenus dans l'addition de a et b en base p.

(e) Soit p un nombre premier. Démontrer que $\binom{p}{i}$ est divisible par p pour tout $1 \leqslant i \leqslant p-1$. En déduire que $n^p - n$ est divisible par p pour tout entier n et que l'application $x \mapsto x^p$ induit un morphisme d'anneaux $A \to A$ pour tout anneau A dans lequel p est nul.