Problème 1 – Petit théorème de Fermat et indicatrice d'Euler

A faire pour le 14 février 2025

L'objectif de ce problème est de démontrer le petit théorème de Fermat en arithmétique puis le théorème de Lagrange en théorie des groupes. Ce dernier permettra alors de généraliser le petit théorème de Fermat. La troisième partie propose ensuite une méthode de calcul de l'indicatrice d'Euler intervenant dans la généralisation du petit théorème de Fermat.

Petit théorème de Fermat : Soit p un nombre premier. Alors pour tout $a \in \mathbb{N}$ premier avec p, $a^{p-1} \equiv 1\,[p]$.

Théorème de Lagrange : Soit G un groupe de cardinal fini n et H un sous-groupe de G de cardinal k. Alors k divise n.

Enfin, la quatrième et dernière partie présente un cas particulier du théorème de progression arithmétique de Dirichlet. En toute généralité, ce théorème énonce que si a et b sont deux entiers premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$. Dans notre cas, on se limitera à montrer ce résultat lorsque $b = 1$.

Partie I – Petit théorème de Fermat

Dans toute cette partie, p désigne un nombre premier.

1. Montrer que pour tout entier k tel que $1 \leqslant k \leqslant p-1$, le coefficient binomial $\binom{p}{k}$ est divisible par p.

2. En déduire que pour tout $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p\,[p]$.

3. Montrer par récurrence que la propriété $\mathcal{P}(a)$: « $a^p \equiv a\,[p]$ » est vraie pour tout $a \in \mathbb{N}$.

4. Montrer que pour tout $a \in \mathbb{N}$ premier avec p, $a^{p-1} \equiv 1\,[p]$.

Partie II – Théorème de Lagrange et application

Dans cette partie, $(G, \cdot)$ désigne un groupe de cardinal n et d'élément neutre e. De plus, H désigne un sous-groupe de G de cardinal k. Pour tout $a \in G$, on note $aH = \{a \cdot h \mid h \in H\}$.

1. Exemple : Soit $G = \mathbb{Z}/6\mathbb{Z}$ qui est un groupe pour l'addition et soit $H = \{0, 2, 4\}$.

   (a) Montrer que H est un sous-groupe de G.
   (b) Si $a = 1$, quel est l'ensemble aH ? (Attention, l'opération $\cdot$ est ici l'addition dans $\mathbb{Z}/6\mathbb{Z}$).
   (c) En général, est-ce que aH est un sous-groupe de G ?

2. Montrer que pour tout $a \in G$, $\text{Card}(aH) = \text{Card}(H)$.
Indication : on pourra montrer que l'application $h \in H \longmapsto a \cdot h \in aH$ est une bijection.

3. Supposons que $H \neq G$ (sinon le théorème de Lagrange est évidemment vérifié).

   (a) On considère $a_1 \in G \setminus H$. Montrer que $a_1 H \cap H = \emptyset$.
   (b) On pose $H_1 = a_1 H \cup H$. Si $G = H_1$, montrer que $\text{Card}(G) = 2\text{Card}(H)$.
   (c) Si $G \neq H_1$, on construit par récurrence, pour tout $n \geqslant 1$, et tant que $G \neq H_n$ une suite $(a_n)_{n\in\mathbb{N}} \in G^{\mathbb{N}}$ de la manière suivante :
   $$\begin{cases} a_{n+1} \notin H_n \\ H_{n+1} = a_{n+1}H \cup H_n \end{cases}$$
   Montrer que pour tout $n \geqslant 1$, $a_{n+1}H$ et H_n sont deux à deux disjoints.
   (d) Justifier que la suite est en fait une suite finie, c'est-à-dire qu'il existe $s \geqslant 1$ tel que $G = H_s$.
   (e) En déduire que $\text{Card}(G) = (s+1)\text{Card}(H)$ et conclure la démonstration du théorème de Lagrange.

   on considère $a_2 \in G \setminus (a_1 H \cup H)$. En itérant ensuite le procédé, donner une preuve algorithmique du théorème de Lagrange.

4. Soit $a \in G$. On note $A = \{a^m \mid m \in \mathbb{Z}\}$.

   (a) Montrer que A est un sous-groupe de G.
   (b) Justifier succinctement que a est d'ordre fini dans G.
   (c) Montrer alors que, si k_0 est l'ordre de a, alors $A = \{e, a, a^2, \ldots, a^{k_0-1}\}$.
   (d) Déduire du théorème de Lagrange que $a^n = e$.

5. Application : Soit $n \geqslant 2$ et soit $G = (\mathbb{Z}/n\mathbb{Z})^*$. On note $\varphi(n)$ le cardinal de G. Montrer que pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$,
$$a^{\varphi(n)} \equiv 1\,[n].$$

Partie III – Calcul pratique de l'indicatrice d'Euler $\varphi(n)$

1. Justifier que $\varphi(n)$ (appelée « indicatrice d'Euler ») désigne le nombre d'entiers premiers entre 1 et n qui sont premiers avec n.

2. Si p est premier, exprimer $\varphi(p)$ en fonction de p.

3. Si p est premier et $k \in \mathbb{N}^*$, montrer que :
$$\varphi(p^k) = p^k - p^{k-1}.$$

4. L'objectif de cette question est de montrer que φ est une fonction multiplicative, c'est-à-dire que si a et b sont premiers entre eux, on a :
$$\varphi(a \times b) = \varphi(a) \times \varphi(b).$$

Dans toute la suite, a et b désignent donc deux entiers strictement positifs et premiers entre eux.

(a) On définit l'application suivante :

$$\mathrm{F} : \left\{ \begin{array}{ccc} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b \\ k & \longmapsto & (k \bmod a \,; k \bmod b) \end{array} \right.$$

Montrer que F est un morphisme de groupes.

(b) Montrer que F est surjective.
Indication : on pourra commencer par montrer que les systèmes suivant admettent une solution dans $\mathbb{Z}$ *:* $\begin{cases} x \equiv 1\,[a] \\ x \equiv 0\,[b] \end{cases}$ *et* $\begin{cases} x \equiv 0\,[a] \\ x \equiv 1\,[b] \end{cases}$

(c) En déduire que F est un isomorphisme.

(d) Montrer que pour tout $k \in \mathbb{Z}/ab\mathbb{Z}$, $k \in (\mathbb{Z}/ab\mathbb{Z})^*$ si, et seulement si, $\mathrm{F}(k) \in (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$.

(e) En déduire que :

$$\mathrm{Card}\left((\mathbb{Z}/ab\mathbb{Z})^*\right) = \mathrm{Card}\left((\mathbb{Z}/a\mathbb{Z})^*\right) \times \mathrm{Card}\left((\mathbb{Z}/b\mathbb{Z})^*\right)$$

puis que la fonction φ est multiplicative.

5. Exemple d'application : Calculer le nombre d'entiers entre 1 et 3096 qui sont premiers avec 3 096.

Partie IV – Version faible de Dirichlet

On note $\Phi_1 = X - 1$ et pour $n \geqslant 2$, $\Phi_n = \prod_{\substack{1 \leqslant k \leqslant n \\ PGCD(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$.

1. Montrer que pour tout $n \geqslant 1$, $X^n - 1 = \prod_{d|n} \Phi_d$ et en déduire que $n = \sum_{d|n} \varphi(d)$.

2. Soient A et B deux polynômes à coefficients entiers avec B non nul et unitaire. Si Q et R sont le quotient et le reste de la division euclidienne de A par B dans $\mathbb{C}[X]$, montrer que Q et R sont aussi à coefficients entiers.

3. Montrer par récurrence sur n que, pour tout $n \geqslant 1$ Φ_n est à coefficients entiers.

4. Soit p un nombre premier, $k \in \mathbb{Z}$ et $n \geqslant 1$ un entier. Montrer que si p divise $\Phi_n(k)$ mais ne divise aucun $\Phi_d(k)$ pour d diviseur strict de n, alors p est de la forme $an + 1$ (avec $a \in \mathbb{N}$).

5. En déduire que pour $n \geqslant 1$ fixé, il existe un infinité de nombres premiers de la forme $an + 1$ avec $a \in \mathbb{N}$.