Licence Pluridisciplinaire – Mathématiques
Examen partiel d'Algèbre – durée : 2 heures
Mercredi 27 octobre 2010
Sans documents

Question de Cours

Enoncer le petit théorème de Fermat (aussi connu sous le nom d'Euler-Fermat).

Problème

Soit $n \geq 2$ un entier. On dit que $x \in \mathbb{Z}$ est un *carré* modulo n s'il existe $y \in \mathbb{Z}$ tel que $x \equiv y^2 \bmod n$. Par exemple, $-1 \bmod 10$ est un carré modulo 10 car $-1 \equiv 3^2 \bmod 10$.

La propriété pour un entier x d'être un carré modulo n ne dépend que de la classe de congruence x modulo n. Par conséquent, on dit aussi que $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ est un *carré* de $\mathbb{Z}/n\mathbb{Z}$ si x est un carré modulo n.

Les quatre parties du problème sont indépendantes. Le choix des parties à traiter est libre (voir barême en fin de sujet).

Première Partie

Dans cette partie, n est un entier *premier* impair. On note $F_n = \mathbb{Z}/n\mathbb{Z}$ et $F_n^\times = F_n \setminus \{0\}$. On rappelle que $F_n^\times$ est un groupe pour la multiplication.

1. Donner la liste des carrés de $\mathbb{Z}/7\mathbb{Z}$. Combien y a-t-il de carrés modulo 7 non nuls dans $\mathbb{Z}/7\mathbb{Z}$?

2. Soit $x \bmod n$ un carré non nul. Montrer que $x^{\frac{n-1}{2}} \equiv 1 \bmod n$.

3. Montrer que le nombre de carrés non nuls dans $F_n^\times$ est $\frac{n-1}{2}$. (On pourra considérer l'application $f : F_n^\times \to F_n^\times$ définie par $f(x) = x^2$.)

4. soit $q \geq 1$ un entier. Combien de solutions l'équation $x^q = 1$ dans F_n a-t-elle *au plus* ?

5. Montrer que réciproquement, si $x^{\frac{n-1}{2}} \equiv 1 \bmod n$, alors x est un carré (non nul) de F_n. Calculer $x^{\frac{n-1}{2}} \bmod p$ pour un élément quelconque x non nul qui n'est pas un carré.

6. On note $C_n \subset F_n^\times$ l'ensemble des carrés non nuls de F_n. Montrer que C_n est un sous-groupe (pour la multiplication) de $F_n^\times$.

On définit

$$\left(\frac{x}{n}\right) = \begin{cases} +1 & \text{si } x \in C_n \\ -1 & \text{si } x \notin C_n. \end{cases}$$

7. Montrer que l'application

$$F_n^\times \to \{\pm 1\},\ x \mapsto \left(\frac{x}{n}\right)$$

est un morphisme de groupes (pour la multiplication).

Deuxième Partie

Dans cette partie, n est une puissance d'un nombre premier impair : $n = p^k$ avec p premier distinct de 2.

1. Décrire les carrés de $\mathbb{Z}/p^k\mathbb{Z}$ pour $p = 3$ et $k = 1, 2, 3$.

2. Soit a un entier premier avec p. Soit $x_1 \in \mathbb{Z}$ une solution de l'équation $x^2 \equiv a \bmod p$. Montrer qu'il existe $t_1 \in \mathbb{Z}$ tel que $x_2 = x_1 + pt_1$ est solution de l'équation $x^2 \equiv a \bmod p^2$. En déduire que $x^2 \equiv a \bmod p^2$ si et seulement si $x^2 \equiv a \bmod p$.

3(*). Montrer que x est un carré dans $\mathbb{Z}/p^k\mathbb{Z}$ si et seulement si x est un carré dans $\mathbb{Z}/p\mathbb{Z}$ (Faire une récurrence sur k.)

Troisième Partie

Dans cette partie, n est une puissance de 2 : $n = 2^k$, $k \geq 1$.

1. Décrire les carrés de $\mathbb{Z}/2^k\mathbb{Z}$ pour $k = 1, 2, 3$.

2. On suppose que $k \geq 4$. Soit x un carré impair modulo 2^k. Montrer que $x \equiv 1 \bmod 8$ (commencer par utiliser que $x \equiv 1 \bmod 2$.)

Quatrième partie

1. Résoudre l'équation

$$\begin{cases} x^2 & \equiv & 4 \bmod 5 \\ x^2 & \equiv & 1 \bmod 8 \end{cases}$$

où l'inconnue x est un entier.

2(*). Soit $m, n \geq 2$ deux entiers premiers entre eux. Si x est à la fois un carré modulo m et un carré modulo n, est-ce que x est un carré modulo mn ? (Démontrer ou donner un contre-exemple).

3. Soit $a, m, n \geq 2$ trois entiers deux à deux premiers entre eux. Si $x \equiv a^2 \bmod m$ et $x \equiv a^2 \bmod n$, est-ce que $x \equiv a^2 \bmod mn$? (Démontrer ou donner un contre-exemple).

barême indicatif –
question de cours : 3 pts. Pb : Partie 1 : 9 pts. Partie 2 : 8 pts. Partie 3 : 4 pts. Partie 4 : 8 pts.