Examen du cours "Arithmétique et groupes" (Maths 209)

17 décembre 2008

Orsay, 2008/2009; durée : 2 heures. Aucun document autorisé.

Dans chaque exercice, la dernière question est nettement plus difficile. On peut admettre le résultat d'une question pour traiter une question ultérieure.

Exercice 1. (9 points)

Soient a et b des éléments non nuls de $\mathbf{Z}$. On considère l'équation d'inconnues x, y, z :

$$x^2 - ay^2 - bz^2 = 0 \qquad (1)$$

Dans toute la suite, on appellera *solution non triviale* de (1) un triplet (x, y, z) d'éléments de $\mathbf{Z}$ qui vérifient (1) avec $(x, y, z) \neq (0, 0, 0)$.

1. a) Soit (x, y, z) une solution non triviale de (1). Soit d un entier non nul. Que peut-on dire de (dx, dy, dz) ?

b) Montrer que si (1) possède une solution non triviale, alors elle possède une solution non triviale (x, y, z) telle que le p.g.c.d. de (x, y, z) soit 1.

2. Soit (x, y, z) une solution non triviale de (1). Soit p un nombre premier qui divise b et tel que p^2 ne divise pas b.

a) Montrer que si p divise y, alors il divise aussi x.

b) En déduire que si p divise y, il divise x, y, et z.

c) Montrer que si l'on suppose que le p.g.c.d. de (x, y, z) est 1, alors p ne peut pas diviser y.

d) On garde les hypothèses de 2c). Montrer qu'il existe $\bar{c}$ dans $\mathbf{Z}/p\mathbf{Z}$ tel que $\bar{a} = \bar{c}^2$, où $\bar{a}$ désigne la classe de a dans $\mathbf{Z}/p\mathbf{Z}$ (on montrera d'abord que p divise $x^2 - ay^2$).

Exercice 2. (7 points)

Soit p un nombre premier impair. On considère l'application f de $(\mathbf{Z}/p\mathbf{Z})^*$ dans $(\mathbf{Z}/p\mathbf{Z})^*$ définie par $f(x) = x^2$.

a) L'application f est-elle un morphisme de groupes multiplicatifs ?

b) Déterminer le noyau $\ker f$ de f (on justifiera soigneusement la réponse).

c) Montrer que si x appartient à l'image $\mathrm{Im}\, f$ de f, alors $x^{(p-1)/2} = \bar{1}$.

d) Soit u un générateur du groupe cyclique $((\mathbf{Z}/p\mathbf{Z})^*, \times)$. Soit x un élément de $(\mathbf{Z}/p\mathbf{Z})^*$ tel que $x^{(p-1)/2} = \bar{1}$. En écrivant x comme une puissance de u, montrer que x appartient à $\mathrm{Im}\, f$.

Exercice 3. (7 points)

On considère le groupe additif $G = \mathbf{Z}/18\mathbf{Z}$. On note H l'ensemble des éléments x de G tels que $6x = \bar{0}$.

a) Montrer que H est un sous-groupe de G.

b) Montrer que H est de cardinal 6.

c) Soit H' un sous-groupe de cardinal 6 de G. Montrer que $H' \subset H$, puis que $H = H'$.

d) Montrer que G possède exactement 2 éléments d'ordre 6.