UNIVERSITE Denis DIDEROT — Année universitaire 1999-2000.
UFR de Mathématiques — MT 282.
Premier cycle — Groupes et arithmétique.

EXAMEN PARTIEL du 4 décembre 1999

Durée : 3 h

L'usage de calculatrice, de téléphone, ainsi que de tout document est interdit.

Dans le problème, les questions 5) et 6) sont indépendantes des questions 7), 8), 9) et 10).

Exercice 1

Un pharmacien doit empaqueter toutes ses pilules vertes à l'aide de petites boîtes et de grandes boîtes. Il se propose de mettre autant de pilules dans chaque boîte utilisée sans nécessairement utiliser toutes les boîtes. Il constate que s'il n'utilise que les petites boîtes et s'il veut mettre sept pilules par boîte il lui manque deux pilules. En revanche, s'il n'utilise que les grandes boîtes et s'il en met neuf par boîte il ne lui en manque qu'une seule. Les pilules sont fournies par plaquettes de huit mais une plaquette est abîmée et la moitié de cette plaquette est à jeter.
Trouver combien de pilules doivent être rangées, sachant qu'il y en a moins de cinq cents.

Exercice 2

1) Trouver les éléments inversibles de l'anneau $\mathbf{Z}/8\mathbf{Z}$.

2) Trouver les éléments inversibles de l'anneau $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

3) Les anneaux $\mathbf{Z}/8\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ sont-ils isomorphes ?

Problème

Soit p un nombre premier impair. On note $\bar{n}$ la classe d'un entier n dans $\mathbf{Z}/p\mathbf{Z}$. On rappelle que dans $\mathbf{Z}/p\mathbf{Z}$ tout polynôme de degré n a au plus n racines et le petit théorème de Fermat : si a est un entier premier à p, alors $a^{p-1} \equiv 1$ modulo p.

1) Vérifier que l'application $\phi : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow (\mathbf{Z}/p\mathbf{Z})^*$ qui à x associe x^2 est un homomorphisme de groupes.

2) Déterminer le noyau de ϕ. En déduire que l'ordre de l'image de ϕ est $\frac{p-1}{2}$.

3) Montrer qu'un élément x de $(\mathbf{Z}/p\mathbf{Z})^*$ est dans l'image de ϕ si et seulement si $x^{\frac{p-1}{2}} = \bar{1}$ (on pourra considérer le polynôme $X^{\frac{p-1}{2}} - \bar{1}$).

Un critère important :

4) En déduire que $-\bar{1}$ est un carré dans $(\mathbf{Z}/p\mathbf{Z})^*$ si et seulement si $p \equiv 1$ modulo 4.

Application aux nombres premiers :

5) Montrer que tout facteur premier de $(n!)^2 + 1$ est congru à 1 modulo 4.

6) En déduire qu'il y a une infinité de nombres premiers congrus à 1 modulo 4.

Application à la courbe elliptique $y^2 = x^3 - 12$:

Soient x_0 et y_0 deux entiers qui vérifient $y_0^2 = x_0^3 - 12$.

7) Supposons que x_0 soit pair. Montrer que y_0 est pair, puis que $y_0/2$ est impair, puis que $x_0/2$ est pair. En posant $y_0/2 = 2c + 1$ et $x_0/2 = 2d$, trouver une contradiction.

8.a) Montrer que y_0 est impair.
8.b) Montrer alors que $x_0^3 \equiv 1$ modulo 4.
8.c) En déduire que $x_0 - 2 \equiv 3$ modulo 4.

9) On suppose que p est un diviseur premier de $x_0 - 2$.
9.a) Etablir l'égalité $y_0^2 + 4 = (x_0 - 2)(x_0^2 + 2x_0 + 4)$.
9.b) En déduire que $y_0^2 + 4 \equiv 0$ modulo p puis que -1 est un carré modulo p.
9.c) En conclure que $x_0 - 2 \equiv 1$ modulo 4.

10) Montrer que l'équation $y^2 = x^3 - 12$ n'a pas de solutions $(x, y) \in \mathbf{Z}^2$.