MT 282 Université Paris 7
07/12/96 U.F.R. de Mathématiques
B. Keller

Examen partiel

Avertissement : les calculettes sont autorisées.

1) A la fin des années cinquante, trois satellites, A, B et C, furent mis en orbite. Le premier émettait un signal toutes les 37 secondes, le second, toutes les 31 secondes et le troisième toutes les 30 secondes. Un beau jour, à midi précis, dans son laboratoire, le professeur E. reçut les trois signaux au même instant. Quelle heure était-il quand, pour la première fois après cette coïncidence, le signal de C fut reçu une seconde après celui de B qui avait été reçu une seconde après celui de A ?

2) Déterminer le *reste* r de la division euclidienne de a par b dans chacun des cas suivants :

   a) $a = 1995^{1996}$, $b = 1997$,
   b) $a = 995^{996}$, $b = 1996$,
   c) $a = 17^{19^{12}}$, $b = 29$,
   d) $a = x^{80}$, $b = 561$, où x est un entier premier avec 561.

3) a) Quel est le nombre d'éléments $x \in (\mathbf{Z}/17\mathbf{Z})^*$ tels que $x^4 = 1$?
   b) Quel est le nombre d'éléments $x \in (\mathbf{Z}/29\mathbf{Z})^*$ qui sont de la forme $x = y^5$ pour un $y \in (\mathbf{Z}/29\mathbf{Z})^*$?
   c) Résoudre l'équation $x^4 = 1$ dans $(\mathbf{Z}/17\mathbf{Z})^*$.

4) Soit p un nombre premier > 3. On note $M(2, \mathbf{Z}/p\mathbf{Z})$ l'anneau des matrices 2×2 à coefficients dans $\mathbf{Z}/p\mathbf{Z}$. Soient $I, J \in M(2, \mathbf{Z}/p\mathbf{Z})$ les matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; J = \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix}.$$

Soit A l'ensemble des matrices

$$x\,I + y\,J = \begin{bmatrix} x & 3y \\ y & x \end{bmatrix}.$$

   a) Montrer que A est un sous-groupe du groupe additif $M(2, \mathbf{Z}/p\mathbf{Z})$, que $I \in A$ et que le produit de deux matrices de la forme $x\,I + y\,J$, $x, y \in \mathbf{Z}/p\mathbf{Z}$, est encore de cette forme.

Il s'ensuit que l'ensemble A des matrices de la forme $x\,I + y\,J$ est un sous-anneau de $M(2, \mathbf{Z}/p\mathbf{Z})$. C'est donc un anneau pour l'addition et la multiplication des matrices.

b) Soit $a = x\,I + y\,J \in A$. Montrer que a est inversible ssi $x^2 - 3y^2$ est non nul dans $\mathbf{Z}/p\mathbf{Z}$.

c) Supposons que l'équation $z^2 = 3$ n'admet pas de solution z dans $\mathbf{Z}/p\mathbf{Z}$. Montrer que A est un corps. En déduire qu'on a

$$a^{p^2-1} = I$$

pour tout élément $a \in A \setminus \{0\}$.

d) Supposons qu'il existe un élément $z \in \mathbf{Z}/p\mathbf{Z}$ tel que $z^2 = 3$. Montrer que l'application

$$f : A \to \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}\ ,\ x\,I + y\,J \mapsto (x + zy, x - zy)$$

est un isomorphisme d'anneaux. En déduire qu'on a

$$a^{p-1} = I$$

pour tout élément inversible a de A.

e) (facultatif) On suppose $p = 17$. On va exhiber un élément d'ordre $17^2 - 1 = 288$ dans $A \setminus \{0\}$.

   e1) Montrer que 3 n'est pas un carré dans $\mathbf{Z}/p\mathbf{Z}$ (on pourra utiliser l'exercice 3). Quel est l'ordre de la matrice inversible J ? Indication : on se souviendra du fait que $J^2 = 3\,I$.

   e2) On considère la matrice $a = -2\,I + J$. Montrer que a est d'ordre 9. En déduire que la matrice

$$aJ = \begin{bmatrix} 3 & -6 \\ -2 & 3 \end{bmatrix}$$

   est d'ordre 288.