MT 282
04/09/97

Université Paris 7
U.F.R. de Mathématiques
B. Keller

Examen de Septembre 1997

Avertissement : les calculettes sont autorisées.

1) Lors d'un spectacle folklorique, les membres d'une école de samba se regroupent d'abord dans plusieurs cercles de 15 danseurs et un petit cercle de 5; ensuite ils se dispersent pour former des rangées de 28 pendant que 9 danseurs exécutent des figures improvisées devant l'ensemble; dans le mouvement final, ils dansent dans des demi-cercles de 31 danseurs avec 3 solistes au devant de la scène. Combien de membres compte l'école de samba au moins ?

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

   a) $a = 1000^{1996}$, $b = 1997$
   b) $a = 1 + 3 + 3^2 + \cdots + 3^{125}$, $b = 127$
   c) $a = 100^{192}$, $b = 221$
   d) $a = 65^{(65^6)}$, $b = 127$

3) Déterminer l'ordre de chacun des groupes suivants. Lesquels de ces groupes sont cycliques ? Justifier. Exhiber un générateur pour chacun des groupes cycliques.

$$A = \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \qquad B = (\mathbf{Z}/17\mathbf{Z})^*$$
$$C = (\mathbf{F}_3[X]/(X^2+1), +) \qquad D = (\mathbf{F}_7[X]/(X^2+1))^*$$

4) Soit p un nombre premier et soit A l'anneau $\mathbf{F}_p[X]/(X^p)$. On note x l'image de X par la projection canonique $\mathbf{F}_p[X] \to A$. Nous allons montrer que le groupe A^* des éléments inversibles de A est isomorphe à

$$\mathbf{Z}/(p-1)\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^{p-1}\,,$$

où $(\mathbf{Z}/p\mathbf{Z})^{p-1} = \underbrace{\mathbf{Z}/p\mathbf{Z} \times \cdots \times \mathbf{Z}/p\mathbf{Z}}_{p-1 \text{ facteurs}}$.

   a) Montrer que tout élément $a \in A$ s'écrit sous la forme

$$a = a_0 + a_1 x + \ldots + a_{p-1} x^{p-1}$$

   pour des $a_i \in \mathbf{F}_p$ déterminés de façon unique par a.

   b) Montrer que les éléments de la forme $1 + bx$, $b \in A$, sont inversibles dans A. Indication : on cherchera l'inverse sous forme d'une série géométrique tronquée.

c) Montrer que les éléments de la forme a_0+bx, $a_0 \in \mathbf{F}_p^*$, $b \in A$, sont inversibles dans A. Indication : si $a_0 a_0' = 1$, on a $a_0 + bx = a_0(1 + a_0' bx)$.

d) Montrer que

$$A^* = \{a = a_0 + a_1 x + \ldots + a_{p-1}x^{p-1} \mid a_0 \in \mathbf{F}_p^*\}.$$

e) Soit $U = 1 + Ax = \{a = 1 + a_1 x + \ldots + a_{p-1}x^{p-1} \mid a_i \in \mathbf{F}_p\}$. Montrer que U est un sous-groupe de A^*. Montrer que l'application

$$\phi : \mathbf{F}_p^* \times U \to A^* \ , \ (a_0, 1 + bx) \mapsto a_0 \cdot (1 + bx)$$

est un isomorphisme de groupes.

f) Montrer que les éléments $a = 1 + x^i$, $1 \leq i \leq p-1$, vérifient $a^p = 1$. En déduire que l'application

$$f : (\mathbf{Z}/p\mathbf{Z})^{p-1} \to U \ , \ (\overline{k_1}, \ldots, \overline{k_{p-1}}) \mapsto (1 + x)^{k_1} \cdots (1 + x^{p-1})^{k_{p-1}}$$

est bien définie. Montrer que c'est un homomorphisme de groupes.

g) Montrer que l'application f est surjective. En déduire qu'elle est bijective en comparant les ordres des deux groupes.

h) Soit ζ un générateur de $\mathbf{F}_p^*$. Déduire de e) et g) que l'application

$$g : \mathbf{Z}/(p-1)\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^{p-1} \to A^*, \ (\overline{k}, \overline{k_1}, \ldots, \overline{k_{p-1}}) \mapsto \zeta^k (1+x)^{k_1} \cdots (1+x^{p-1})^{k_{p-1}}$$

est un isomorphisme de groupes.

Remarque. Le lecteur intéressé pourra essayer de démontrer que pour $n \geq 1$, le groupe $(\mathbf{F}_p[X]/(X^{(p^n)}))^*$ est isomorphe à

$$\mathbf{Z}/(p-1)\mathbf{Z} \times \prod_{i=1}^{n} (\mathbf{Z}/p^i\mathbf{Z})^{m_i}$$

où $m_i = (p-1)\phi(p^{n-i})$ en désignant par ϕ la fonction d'Euler : $\phi(N) = |(\mathbf{Z}/N\mathbf{Z})^*|$.