MT 282
04/09/97

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

Un corrigé de l'examen de Septembre 1997

1) Soit d le nombre de danseurs de samba. D'après les informations fournies, nous avons

$$\begin{aligned} d &\equiv 5 \ (15) \\ d &\equiv 9 \ (28) \\ d &\equiv 3 \ (31). \end{aligned}$$

Les nombres $15, 28, 31$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution d dont la classe modulo $15 \times 28 \times 31 = 13020$ est unique. Pour trouver d, nous déterminons d'abord x_1, x_2, x_3 dont les classes sont les images réciproques de $(1,0,0), (0,1,0), (0,0,1)$ par la projection

$$\mathbf{Z}/13020 \xrightarrow{\sim} \mathbf{Z}/15 \times \mathbf{Z}/28 \times \mathbf{Z}/31.$$

Nous avons

$$\begin{array}{lll} 28 \times 31\, u_1 + 15\, v_1 = 1; & \text{sol. part.} & 28 \times 31 \times 7 + 15 \times (-405) = 1. \\ 15 \times 31\, u_2 + 28\, v_2 = 1; & \text{sol. part.} & 15 \times 31 \times 5 + 28 \times (-83) = 1. \\ 15 \times 28\, u_3 + 31\, v_3 = 1; & \text{sol. part.} & 15 \times 28 \times 11 + 31 \times (-149) = 1 \end{array}$$

Posons

$$x_1 = 28 \times 31 \times 7 = 6076\,, \quad x_2 = 15 \times 31 \times 5 = 2325\,, \quad x_3 = 15 \times 28 \times 11 = 4620.$$

Nous avons donc $l \equiv 5 \times 6076 + 9 \times 2325 + 3 \times 4620 \equiv 65 \ (13020)$. On a donc $d = 65 + k \times 13020$ pour un $k \in \mathbf{Z}$ et la valeur positive minimale de d est 65. *Le nombre de danseurs de samba est (au moins) de* 65.

2) a) $a = 1000^{1996}$, $b = 1997$. Le nombre 1997 est premier et ne divise pas 1000. D'après le petit théorème de Fermat, nous avons donc $1000^{1996} \equiv 1 \ (1997)$ et $r = 1$.

b) $a = 1 + 3 + 3^2 + \cdots + 3^{125}$, $b = 127$. Nous avons

$$a = \frac{3^{126} - 1}{3 - 1}$$

et donc $2a = 3^{126} - 1$. Le nombre 127 est premier et ne divise pas 3. D'après le petit théorème de Fermat, on a donc $3^{126} \equiv 1 \ (127)$ et $2a \equiv 0 \ (127)$. Puisque 2 est inversible modulo 127, il s'ensuit que $a \equiv 0 \ (127)$ et donc $r = 0$.

c) $a = 100^{192}$, $b = 221$. Nous avons $b = 13 \times 17$ et $\phi(b) = 12 \times 16 = 192$. Puisque 100 est premier avec 221, nous avons $100^{192} \equiv 1 \ (221)$ d'après le théorème d'Euler. Donc $r = 1$.

d) $a = 65^{(65^6)}$, $b = 127$. Le nombre $b = 127$ est premier et ne divise pas 65. D'après le petit théorème de Fermat, la classe de a modulo 127 ne dépend donc que de la classe de $c = 65^6$ modulo 126. Nous avons $126 = 2 \times 7 \times 9$. Réduisons modulo les trois facteurs :

$$\begin{aligned} 65^6 &\equiv 1^6 \equiv 1 \ (2) \\ 65^6 &\equiv 2^6 \equiv 1 \ (7) \quad \text{(Fermat)} \\ 65^6 &\equiv 2^6 \equiv 1 \ (9) \quad \text{(Euler : } \phi(9) = 6) \end{aligned}$$

Puisque 2, 7 et 9 sont premiers entre eux deux à deux, il s'ensuit d'après le théorème chinois que $65^6 \equiv 1 \ (126)$. Donc $a \equiv 65^1 \equiv 65 \ (127)$ et $r = 65$.

3) D'après le théorème chinois, nous avons $A \xrightarrow{\sim} \mathbf{Z}/15\mathbf{Z}$. Le groupe A est donc cyclique d'ordre 15. L'élément $(\overline{1}, \overline{1})$ en est un générateur.

Puisque 17 est premier, le groupe $B = (\mathbf{Z}/17\mathbf{Z})^*$ est cyclique d'ordre 16. Il est engendré par la classe de 3. En effet, nous avons $3^2 = 9$, $3^4 = -4$, $3^8 = -1$ dans $\mathbf{Z}/17\mathbf{Z}$. Donc 3 est bien d'ordre 16.

D'après un théorème du cours, l'application

$$\mathbf{F}_3 \times \mathbf{F}_3 \to \mathbf{F}_3[X]/(X^2+1)\ ,\ (a,b) \mapsto aX + b$$

est un isomorphisme de groupes (pour l'addition). Il s'ensuit que le groupe C est d'ordre 9 et qu'il n'est pas cyclique car l'ordre maximal d'un élément y est de 3 (puisque c'est le cas pour $\mathbf{F}_3 \times \mathbf{F}_3$).

Le polynôme X^2+1 n'admet pas de racine dans $\mathbf{F}_7$ (car les seuls carrés modulo 7 sont 1, 4 et 2). Puisqu'il est de degré 2, il est donc irréductible, et $\mathbf{F}_7[X]/(X^2+1)$ est un corps (à $7^2 = 49$ éléments). Il s'ensuit que le groupe $D = (\mathbf{F}_7[X]/(X^2+1)^*$ est cyclique d'ordre $49 - 1 = 48$. Cherchons un générateur : la classe de 2 est clairement d'ordre 3 dans $\mathbf{F}_7^*$ et donc dans D (qui contient $\mathbf{F}_7$ comme le sous-groupe image des polynômes constants non nuls). On vérifie aussi que l'élément $\alpha = 2x+3$ est d'ordre 16 (on a $\alpha^2 = -2x-2$, $\alpha^4 = x$ et $\alpha^8 = -1$). Puisque 3 et 16 sont premiers entre eux et que D est commutatif, il s'ensuit que $2\alpha = 4x+6$ est d'ordre $3 \times 16 = 48$. L'élément $4x+6$ est donc un générateur de D.

4) a) D'après un théorème du cours, si $P \in \mathbf{F}_p[X]$ est de degré n, alors les éléments de $\mathbf{F}_p[X]/(P)$ s'écrivent de façon unique sous la forme $a_0 + a_1 x + \ldots + a_n x^{n-1}$, $a_i \in \mathbf{F}_p$. Comme X^p est de degré p, l'affirmation en résulte.

b) Nous avons

$$(1+bx)(1-bx+(bx)^2-(bx)^3+\ldots+(-1)^{p-1}(bx)^{p-1}) = 1.$$

L'élément $1+bx$ est donc inversible d'inverse $1-bx+(bx)^2-(bx)^3+\ldots+(-1)^{p-1}(bx)^{p-1}$.

c) L'élément $1+a_0'b$ est inversible d'après b). Donc le produit $a_0(1+a_0'b) = a_0 + bx$ est inversible aussi (d'inverse $a_0'(1+a_0'b)^{-1}$).

d) Si $a_0 \in \mathbf{F}_p^*$, alors $a = a_0 + bx$ où $b = a_1 + a_2 x + \ldots a_{p-1}x^{p-2}$. Cet élément est inversible d'après c). Si $a_0 = 0$, alors $a = bx$ et $a^p = b^p x^p = 0$. Dans ce cas a ne peut être inversible (sinon, $a^p = 0$ le serait aussi; contradiction).

e) Clairement $1 = 1 + 0 \cdot x$ appartient à U et si $1+bx$ et $1+b'x$ appartiennent à U alors $(1+bx)(1+b'x) = 1 + x(b+b'+bb'x)$ appartient à U. Donc U est bien un sous-groupe. Ce sous-groupe est formé des éléments $1 + a_1 x + a_2 x^2 + \ldots + a_{p-1}x^{p-1}$ qui, d'après a), sont au nombre de p^{p-1}. Donc U est d'ordre p^{p-1}.

L'application ϕ est un homomorphisme de groupes car

$$\begin{aligned}\phi((a_0, 1+bx), (a_0', 1+b'x)) &= \phi((a_0a_0', (1+bx)(1+b'x)) = a_0a_0'(1+bx)(1+b'x) \\ &= a_0(1+bx)a_0'(1+b'x) = \phi((a_0, 1+bx))\phi((a_0', 1+b'x)).\end{aligned}$$

L'application ϕ est bijective d'inverse $\psi : a_0 + bx \mapsto (a_0, 1 + a_0^{-1}bx)$. Donc c'est un isomorphisme de groupes.

f) Soit $1 \leq i \leq p-1$ et $a = 1 + x^i$. Alors $a^p = (1+x^i)^p = 1 + x^{ip} = 1$. Il s'ensuit que si $\overline{k} \in \mathbf{Z}/p\mathbf{Z}$, alors $(1+x^i)^k$ ne dépend pas du choix du représentant k de $\overline{k}$. Donc l'application f est bien définie.

g) Soit I l'image de f. Soit $U_j = \{1 + bx^j \mid b \in A\}$, $1 \leq j \leq p$. Montrons par récurrence descendante sur j que $U_j \subset I$. Clairement $U_p = \{1\}$ est contenu dans I. Supposons que nous avons déjà montré que U_{j+1} est contenu dans I. Soit $a = 1 + a_j x^j + bx^{j+1} \in U_j$. Alors

$$(1+x^j)^{-a_j}a = (1 - a_j x^j + b'x^{j+1})(1 + a_j x^j + bx^{j+1}) = 1 + b''x^{j+1} \in U_{j+1}$$

pour certains $b', b'' \in A$. Donc a est le produit de $(1+x^j)^{a_j}$ par un élément de U_{j+1}. Puisque $(1+x^j)^{a_j}$ appartient à I et que U_{j+1} est contenu dans I (par l'hypothèse de récurrence), il s'ensuit que a appartient à I.

h) L'application g est la composée de ϕ avec

$$\Phi : \mathbf{Z}/(p-1)/\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^{p-1} \to \mathbf{F}_p^* \times U \ , \ (\overline{k}, \overline{k_1}, \ldots, \overline{k_{p-1}}) \mapsto (\zeta^k, f(\overline{k_1}, \ldots, \overline{k_{p-1}})).$$

L'application Φ est un isomorphisme car $\overline{k} \mapsto \zeta^k$ est un isomorphisme de $\mathbf{Z}/(p-1)\mathbf{Z}$ sur $\mathbf{F}_p^*$ et f est un isomorphisme $(\mathbf{Z}/p\mathbf{Z})^{p-1}$ sur U. Donc $g = \phi \circ \Phi$ est un isomorphisme.