MT 282
25/01/97

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

Un corrié de l'examen de Janvier 1997

Avertissement : les calculettes sont autorisées.

1) Soit l le nombre de lignes de la dernière chanson de D.B. . D'après les informations fournies, nous avons

$$\begin{aligned} l &\equiv 1 \ (40) \\ l &\equiv 13 \ (37) \\ l &\equiv 32 \ (43). \end{aligned}$$

Les nombres $40, 37, 43$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution l dont la classe modulo $40 \times 37 \times 43 = 63640$ est unique. Pour trouver l, 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

$$\mathbf{Z}/63640 \xrightarrow{\sim} \mathbf{Z}/40 \times \mathbf{Z}/37 \times \mathbf{Z}/43.$$

Nous avons

$$\begin{array}{lll} 37 \times 43\, u_1 + 40\, v_1 = 1; & \text{sol. part.} & 37 \times 43 \times (-9) + 40 \times 358 = 1. \\ 40 \times 43\, u_2 + 37\, v_2 = 1; & \text{sol. part.} & 40 \times 43 \times (-2) + 37 \times 93 = 1. \\ 40 \times 37\, u_3 + 43\, v_3 = 1; & \text{sol. part.} & 40 \times 37 \times 12 + 43 \times (-413) = 1 \end{array}$$

Posons

$$x_1 = 37 \times 43 \times (-9) = -14319\,, \quad x_2 = 40 \times 43 \times (-2) = -3440\,, \quad x_3 = 40 \times 37 \times 12 = 17760.$$

Nous avons donc $l \equiv 1 \times (-14319) + 13 \times (-3440) + 32 \times 17760 \equiv 161 \ (63640)$. On a donc $l = 161 + k \times 63640$ pour un $k \in \mathbf{Z}$ et la valeur positive minimale de l est 161. *La dernière chanson de D.B. comporte (au moins)* 161 *lignes.*

2) a) $a = 1995^{456}$, $b = 229$. Le nombre $b = 229$ est premier et ne divise pas 1995. D'après le petit théorème de Fermat, nous avons donc $1995^{228} \equiv 1 \ (229)$. Comme $456 = 2 \times 228$, il s'ensuit que $1995^{456} \equiv 1 \ (229)$ et $r = 1$.

b) $a = 1996^{1233}$, $b = 2001$. Le nombre 2001 se décompose en facteurs premiers $2001 = 3 \times 23 \times 29$. Son indicatrice d'Euler est donc $\phi(2001) = 2 \times 24 \times 28 = 1232$. Le nombre 1996 se décompose en facteur premiers $1996 = 2^2 \times 499$. Donc 1996 est premier avec 2001 et d'après le théorème d'Euler, nous avons $1996^{1332} \equiv 1 \ (2001)$. Il s'ensuit que $1996^{1333} \equiv 1996 \ (2001)$ et nous avons donc $r = 1996$.

c) $a = 10^{(101^{1000})}$, $b = 31$. Le nombre 31 est premier et ne divise pas 10. D'après le petit théorème de Fermat, la classe de a modulo 31 ne dépend donc que de la classe de $a' = 101^{1000}$ modulo 30. Or 30 est premier avec 101, et d'après le théorème d'Euler, la classe de a' modulo 30 ne dépend que de la classe de 1000 modulo $\phi(30) = \phi(2)\phi(3)\phi(5) = 2 \times 4 = 8$. Or $1000 \equiv 0 \ (8)$. Donc $a' \equiv 1 \ (30)$ et $a \equiv 10^1 \equiv 10 \ (31)$. Donc le reste $r = 10$.

d) $a = 13^{60}$, $b = 385$. Le nombre 385 se décompose en facteurs premiers $385 = 5 \times 7 \times 11$. D'après le lemme chinois, pour connaître la classe de a modulo 385, il suffit de connaître ses classes modulo 5, 7 et 11. Or a est premier avec ces trois nombres et 60 est divisible par $p - 1$ pour $p = 5, 7$ ou 11. Donc $a \equiv 1 \ (p)$ pour $p \in \{5, 7, 11\}$. D'après le lemme chinois, il s'ensuit que $a \equiv 1(\mathrm{PPCM}\,(5, 7, 11))$ et donc $r = 1$.

3) Le groupe $A = \mathbf{Z}/7\mathbf{Z}$ est cyclique d'ordre 7 et d'exposant 7. Il est engendré par la classe de 1.

Le groupe $B = (\mathbf{Z}/23\mathbf{Z})^*$ est cyclique (car 23 est premier) d'ordre 22 et d'exposant 22.

D'après le lemme chinois, le groupe $C = (\mathbf{Z}/22\mathbf{Z})^*$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^* \times (\mathbf{Z}/11\mathbf{Z})^*$. Comme le groupe $(\mathbf{Z}/2\mathbf{Z})^*$ est trivial, le groupe C est donc isomorphe à $(\mathbf{Z}/11\mathbf{Z})^*$. Comme 11 est premier, il est donc cyclique d'ordre et d'exposant 10.

Le groupe $D = (\mathbf{F}_3[X], +)$ est infini. Son exposant est égal à 5. Il n'est pas cyclique.

Le groupe $E = \mathbf{F}_5[X]^*$ est formé des polynômes constants non nuls. Il est isomorphe à $\mathbf{F}_5^*$. Il est donc cyclique d'exposant et d'ordre 4.

Le polynôme $X^2 + 1$ se décompose sur $\mathbf{F}_5$ en $X^2 + 1 = (X - 2)(X + 2)$. Les polynômes $X - 2$ et $X + 2$ sont premiers entre eux. D'après le lemme chinois, le groupe $F = (\mathbf{F}_5[X]/(X^2+1))^*$ est donc isomorphe à $(\mathbf{F}_5[X]/(X - 2))^* \times (\mathbf{F}_5[X]/(X + 2))^*$. Or on a un isomorphisme $k[X]/(X - \alpha) \xrightarrow{\sim} k$ pour tout corps k. Le groupe F est donc isomorphe à $\mathbf{F}_5^* \times \mathbf{F}_5^* \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. C'est un groupe d'ordre 16 et d'exposant 4. Comme un groupe abélien fini est cyclique ssi son exposant est égal à son ordre, le groupe F n'est pas cyclique.

Le polynôme X^2+1 n'admet pas de racines dans $\mathbf{F}_7$. Comme il est de degré 2, il est donc irréductible. Ainsi l'anneau $\mathbf{F}_7[X]/(X^2 + 1)$ est un corps de cardinal 7^2. Le groupe $G = (\mathbf{F}_7[X]/(X^2 + 1))^*$ est donc cyclique d'ordre 48 et d'exposant 48.

4) Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 5 & 4 & 6 & 7 & 9 & 8 & 12 & 10 & 11 & 3 & 13 & 2 & 1 \end{pmatrix}.$$

a) Décomposition de σ en produit de cycles à supports disjoints :

$$\sigma = (1, 5, 9, 11, 13)\,(2, 4, 7, 12)\,(3, 6, 8, 10).$$

Les longueurs des cycles sont donc $l_1 = 5, l_2 = 4, l_3 = 4$, et l'ordre de σ est égal à PPCM $(5, 4, 4) = 20$. La signature de σ est

$$\epsilon(\sigma) = (-1)^{(l_1+1)+(l_2+1)+(l_3+1)} = 1.$$

b) On sait que si $(i_1, i_2, \ldots, i_k)$ et $(j_1, j_2, \ldots, j_l)$ sont deux cycles disjoints, alors

$$(i_1, j_1)\,(i_1, i_2, \ldots, i_k)\,(j_1, j_2, \ldots, j_l) = (i_1, i_2, \ldots, i_k, j_1, j_2, \ldots, j_l).$$

Posons donc $\tau_2 = (1, 2)$. Alors nous avons

$$\tau_2\sigma = (1, 5, 9, 11, 13, 2, 4, 7, 12)(3, 6, 8, 10).$$

Posons $\tau_1 = (1, 3)$. Alors nous avons

$$\tau_1\tau_2\sigma = (1, 5, 9, 11, 13, 2, 4, 7, 12, 3, 6, 8, 10)$$

qui est un cycle de longueur 13 et donc d'ordre 13.

c) Si τ est une transposition et l'ordre de $\tau\sigma$ est 13, on a $(\tau\sigma)^{13} = 1$ et donc $\varepsilon((\tau\sigma)^{13}) = 1$. Or,

$$\varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma)) = (-1)(+1) = -1$$

et donc $\varepsilon((\tau\sigma)^{13}) = (-1)^{13} = -1$. Contradiction.

5) a) Nous montrons

$$a_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2}\ ,\ n \in \mathbf{N}\ ,$$

par récurrence sur $n \in \mathbf{N}$. Notons b_n l'expression de droite. Clairement, nous avons $b_0 = 0$ et $b_1 = 1$. Supposons que $n \geq 0$ et $a_n = b_n$ et $a_{n+1} = b_{n+1}$. Montrons que $a_{n+2} = b_{n+2}$. Par hypothèse, nous avons

$$\begin{aligned} \lambda_1^{n+2} &= \lambda_1^{n+1} + \lambda_1^n \\ \lambda_2^{n+2} &= \lambda_2^{n+1} + \lambda_2^n \end{aligned}$$

Si nous prenons la différence de ces deux équations et que nous la divisons par $\lambda_1 - \lambda_2$, nous trouvons

$$b_{n+2} = b_{n+1} + b_n$$

et donc $b_{n+2} = a_{n+1} + a_n = a_{n+2}$.
Il s'ensuit que

$$\begin{aligned} \frac{a_{rs}}{a_r} &= \frac{\lambda_1^{rs} - \lambda_2^{rs}}{\lambda_1 - \lambda_2} \frac{\lambda_1 - \lambda_2}{\lambda_1^r - \lambda_2^r} = \frac{\lambda_1^{rs} - \lambda_2^{rs}}{\lambda_1^r - \lambda_2^r} \\ &= \frac{a^s - b^s}{a - b} = \frac{b^s}{b} \frac{(a/b)^s - 1}{(a/b) - 1}. \end{aligned}$$

où $a = \lambda_1^r$, $b = \lambda_2^r$. Nous trouvons donc

$$\begin{aligned} \frac{a_{rs}}{a_r} &= b^{s-1}(1 + (a/b) + (a/b)^2 + \ldots + (a/b)^{s-1}) \\ &= b^{s-1} + ab^{s-2} + a^2 b^{s-3} + \ldots + a^{s-2}b + a^{s-1} \\ &= \sum_{i=0}^{s-1} \lambda_1^{ri} \lambda_2^{r(s-1-i)}. \end{aligned}$$

b) Nous avons $0 = 0\lambda_1 + 0 \in A$ et si $k\lambda_1 + l, k'\lambda_1 + l' \in A$ nous avons $k\lambda_1 + l + k'\lambda_1 + l' = (k + k')\lambda_1 + (l + l') \in A$ et $-(k\lambda_1 + l) = (-k)\lambda_1 + (-l) \in A$. L'ensemble A est donc un sous-groupe de $(\mathbf{R}, +)$. En particulier, c'est un groupe. En outre, nous avons $1 = 0\lambda_1 + 1 \in A$ et

$$(k\lambda_1 + l)(k'\lambda_1 + l') = kk'\lambda_1^2 + (kl' + k'l)\lambda + ll' = (kl' + k'l + kk')\lambda_1 + (ll' + kk')$$

appartient à A si $k\lambda_1 + l, k'\lambda_1 + l' \in A$. Donc A est un sous-anneau de $\mathbf{R}$ et en particulier, A est un anneau.
Nous avons $\lambda_2 = 1 - \lambda_1 \in A$. Donc l'élément

$$\frac{a_{rs}}{a_r} = \sum_{i=0}^{s-1} \lambda_1^{ri} \lambda_2^{r(s-1-i)}$$

appartient à A.

c) Supposons que $k\lambda_1 + l = k'\lambda_1 + l'$. Alors $(k - k')\lambda_1 = l' - l$. Si $k \neq k'$, nous avons donc

$$\lambda_1 = \frac{l' - l}{k - k'}$$

c'est-à-dire que λ_1 est rationnel. Or nous avons

$$\lambda_1 = (1 \pm \sqrt{5})/2$$

et si λ_1 est rationnel, il en est de même pour $\sqrt{5}$. Supposons que $\sqrt{5} = r/s$ où r, s sont des entiers strictement positifs et premiers entre eux. Alors $5s^2 = r^2$. Donc 5 divise r^2. Comme 5 est premier, 5 doit alors diviser r et 5^2 divise r^2. Mais alors 5 divise s en contradiction avec l'hypothèse que r et s sont premiers entre eux. Donc $\sqrt{5}$ est irrationnel, λ_1 est irrationnel, $k = k'$ et $l = l'$.
Pour $a \in A$, les entiers k, l dans l'écriture $a = k\lambda_1 + l$ ne dépendent que de a. Donc la valeur $\gamma(a) = k\lambda_2 + l$ ne dépend que de a. En outre, comme $\lambda_2 = 1 - \lambda_1$ appartient à A, on a une application bien définie $\gamma : A \to A$. Soient $a, a' \in A$. Nous avons

$$\begin{aligned} \gamma(a + a') &= \gamma\left(k\lambda_1 + l + k'\lambda_1 + l'\right) = \gamma\left((k + k')\lambda_1 + (l + l')\right) \\ &= (k + k')\lambda_2 + (l + l') = \gamma(a) + \gamma(a') \end{aligned}$$

où $a = k\lambda_1 + l$ et $a' = k'\lambda_1 + l'$. Donc γ est un homomorphisme de groupes. Nous avons $\gamma(1) = \gamma(0\lambda_1 + 1) = 1$ et

$$(k\lambda_i + l)(k'\lambda_i + l') = kk'\lambda_i^2 + (kl' + k'l)\lambda_i + ll' = (kl' + k'l + kk')\lambda_i + (ll' + kk')$$

pour $i = 1, 2$ puisque λ_1 et λ_2 sont racines de $X^2 - X - 1$. Cela montre que $\gamma(aa') = \gamma(a)\gamma(a')$. En conclusion, γ est un homomorphisme d'annneau.

Supposons que $a = k\lambda_1 + l$ vérifie $\gamma(a) = a$. Alors $k\lambda_1 + l = k\lambda_2$. Donc $k(\lambda_1 - \lambda_2) = 0$ et $k = 0$ puisque $\lambda_1 \neq \lambda_2$. Donc $a = l$ appartient à $\mathbf{Z}$.

d) Il s'agit de montrer que a_{rs}/a_r appartient à $\mathbf{Z}$. Or, nous savons que

$$\frac{a_{rs}}{a_r} = \sum_{i=0}^{s-1} \lambda_1^{ri} \lambda_2^{r(s-1-i)}$$

appartient à A. En outre, cette expression est symétrique en λ_1 et λ_2 de façon que nous si nous calculons $\gamma(a_{rs})$ (en utilisant le fait que γ est un homomorphisme d'anneau), nous obtenons $\gamma(a_{rs}/a_r) = a_{rs}/a_r$. D'après la partie précédente, le nombre a_{rs}/a_r est bien un entier.

e) Supposons que $n = kl$. Alors, comme $a_n > 3$, on doit avoir $n > 4$. Donc $k > 2$ ou $l > 2$. Supposons $k > 2$. Mais alors $a_k > 1$ et comme a_k divise a_n, on doit avoir $a_k = a_n$ puisque a_n est premier. Ainsi $k = n$, puisque la suite des a_n est strictement monotone pour $n > 2$. Ainsi n est premier.