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

Un corrigé de l'examen partiel du 07.12.96

1) Soit t le nombre de secondes qui se sont écoulées depuis la coïncidence des trois signaux. D'après les informations fournies, nous avons

$$\begin{aligned} t &\equiv 0 \ (30) \\ t &\equiv 1 \ (31) \\ t &\equiv 2 \ (37). \end{aligned}$$

Les nombres $30, 31, 37$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution t dont la classe modulo $30 \times 31 \times 37 = 34410$ est unique. Pour trouver t, 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

$$\mathbf{Z}/34410 \xrightarrow{\sim} \mathbf{Z}/30 \oplus \mathbf{Z}/31 \oplus \mathbf{Z}/37.$$

Nous avons

$$\begin{aligned} 31 \times 37\, u_1 + 30\, v_1 = 1; &\quad \text{sol. part.} \quad 31 \times 37 \times 13 + 30 \times (-497) = 1. \\ 30 \times 37\, u_2 + 31\, v_2 = 1; &\quad \text{sol. part.} \quad 30 \times 37 \times 5 + 31 \times (-179) = 1. \\ 30 \times 31 \times\ u_3 + 37\, v_3 = 1; &\quad \text{sol. part.} \quad 30 \times 31 \times 15 + 37 \times (-375) = 1 \end{aligned}$$

Posons

$$x_1 = 31 \times 37 \times 13 = 17797\,, \quad x_2 = 5 \times 30 \times 37 = 5550\,, \quad x_3 = 30 \times 31 \times 15 = 13950.$$

Nous avons donc $x \equiv 0+1\times 5550+2\times 13950 \equiv 33450 \ (34410)$. On a donc $t = 33450+k\times 34410$ pour un $k \in \mathbf{Z}$ et la valeur positive minimale de t est 33450. *Depuis la coïncidence,* $33450'' = 557'\,30'' = 9h\,17'\,30''$ *sétaient écoulées, et il était* $21h\,17'\,30''$.

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

b) Nous avons la décomposition en facteurs premiers $1996 = 2^2 \times 499$. Donc $\phi(1996) = \phi(4) \times \phi(499) = 2 \times 498 = 996$. Le nombre 995 est premier avec 1996, et le théoème d'Euler permet donc de conclure que $995^{\phi(1996)} \equiv 995^{996} \equiv 1 \ (1996)$ et $r = 1$.

c) Le nombre 29 est premier et ne divise pas 17. D'après le petit théorème de Fermat, la classe de 29^a ne dépend donc que de la classe de a modulo $29 - 1 = 28$, quel que soit l'entier a. Il s'agit donc de calculer la classe de $a = 19^{12}$ modulo 28. Or le nombre 19 est premier avec 28 et $\phi(28) = \phi(4 \times 7) = \phi(4) \times \phi(7) = 2 \times 6 = 12$. D'après le théorème d'Euler, nous avons $19^{12} \equiv 1 \ (28)$. Donc $a \equiv 17^1 \equiv 17 \ (29)$ et $r = 17$.

d) Posons $a = x^{80}$. Nous avons la décomposition en facteurs premiers $561 = 3 \times 11 \times 17$. D'après le lemme chinois, la classe de a modulo 561 est déterminée par les classes de a modulo 3, 11 et 17. Or, comme x est premier avec 561, il n'est divisible ni par 3 ni par 11 ni par 17. Par le petit théorème de Fermat, nous avons $x^2 \equiv 1 \ (3)$, $x^{10} \equiv 1 \ (11)$ et $x^{16} \equiv 1 \ (17)$. Ainsi nous arrivons aux système

$$\begin{aligned} x^{80} &\equiv 1 \ (3) \\ x^{80} &\equiv 1 \ (11) \\ x^{80} &\equiv 1 \ (17) \end{aligned}$$

Par le lemme chinois, il s'ensuit que $x \equiv 1 \ (561)$. Donc $r = 1$.

3) Si p est un nombre premier, on sait que le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique d'ordre $p-1$. Pour $a \in \mathbf{Z}$, l'équation

$$x^a = 1$$

admet donc PGCD $(p-1, a)$ solutions. Nous trouvons donc 4 éléments dans a). L'application $x \mapsto x^a$ a pour image le sous-groupe engendré par g^a où g est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$. Le cardinal de l'image est donc égal à $(p-1)/\text{PGCD}\,(p-1, a)$. Nous trouvons donc 28 éléments dans b).

c) Le groupe $(\mathbf{Z}/17\mathbf{Z})^*$ est cyclique engendré par 3 (En effet, les puissances successives de 3 sont $1, 3, 9, 10, -4, 5, -2, -6, -1, \ldots$). Les solutions de $x^4 = 1$ sont donc 1, $3^4 = -4$, $3^8 = -1$, et $3^{12} = 4$.

4) a) Clairement, nous avons $0 = 0\,I + 0\,J \in A$,

$$(x\,I + y\,J) + (x'\,I + y'\,J) = (x + x')\,I + (y + y')\,J \in A$$

et $-(x\,I + y\,J) = (-x)\,I + (-y)\,J \in A$ si $x\,I + y\,J, x'\,I + y'\,J \in A$. En outre, on calcule que $J^2 = 3\,I$. Donc

$$(x\,I + y\,J)(x'\,I + y'\,J) = (xx' + 3yy')\,I + (xy' + yx')\,J \in A.$$

b) Si a est inversible dans A, il est encore inversible dans $M(2, \mathbf{Z}/p\mathbf{Z})$, donc de déterminant non nul. Ainsi, si

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

alors $\det(a) = x^2 - 3y^2$ est non nul dans $\mathbf{Z}/p\mathbf{Z}$.

Réciproquement, si $x^2 - 3y^2$ est non nul, la matrice a est inversible dans l'anneau $M(2, \mathbf{Z}/p\mathbf{Z})$; soit b la matrice inverse. L'élément a sera inversible dans A si la matrice b est élément de A. Un calcul standard donne

$$b = (x^2 - 3y^2)^{-1} \begin{bmatrix} x & -3y \\ -y & x \end{bmatrix}.$$

Cette matrice est élément de A car égale à $x'\,I + y'\,J$, où $x' = (x^2 - 3y^2)^{-1}x$ et $y' = -(x^2 - 3y^2)^{-1}y$.

Une autre démonstration de la condition suffisante est la suivante : Nous avons $(x\,I + y\,J)(x\,I - y\,J) = (x^2 - 3y^2)\,I$. Donc si $x^2 - 3y^2$ est inversible d'inverse u, alors $(x\,I + y\,J)$ est inversible d'inverse $u(x\,I - y\,J)$.

c) Il s'agit de montrer que $a = x\,I + y\,J$ est inversible si $a \neq 0$. D'après b), il suffit de montrer que $x^2 = 3y^2$ n'admet pas de solutions différentes de $x = 0, y = 0$ dans $\mathbf{Z}/p\mathbf{Z}$. Or, si nous avons une solution où $x \neq 0$, alors clairement $y \neq 0$. On peut donc supposer que $y \neq 0$. Soit u l'inverse de y dans $\mathbf{Z}/p\mathbf{Z}$. Alors nous avons $x^2u^2 = 3 = (xu)^2$ contrairement à l'hypothèse que 3 n'est pas un carré dans $\mathbf{Z}/p\mathbf{Z}$.

Le corps A est de cardinal p^2 et donc le groupe $A \setminus \{0\}$ est de cardinal $p^2 - 1$. D'après le théorème de Lagrange, nous avons donc

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

pour tout $a \in A \setminus \{0\}$. Remarquons que le groupe $A \setminus \{0\}$ est en fait cyclique (tout sous-groupe fini du groupe des éléments inversibles d'un corps commutatif est cyclique, d'après un théorème du cours).

d) Il est clair que l'application f est un homomorphisme de groupes abéliens. En outre, on a $f(I) = (1, 1)$. Vérifions que f est compatible à la multiplication : Si $a = x\,I + y\,J$,

$a' = x'\,I + y'\,J$, nous avons

$$\begin{aligned} f(a)f(a') &= (x+zy, x-zy)(x'+zy', x'-zy') \\ &= ((x+zy)(x'+zy'), (x-zy)(x'-zy')) \\ &= ((xx'+3yy') + (xy'+yx')z, (xx'+3yy') - (xy'+yx')z) \\ &= f(aa') \end{aligned}$$

L'application f est donc un homomorphisme d'anneaux. Elle est surjective : en effet, comme $p > 3$, il existe un inverse v de 2 et un inverse z' de $z \neq 0$ dans $\mathbf{Z}/p\mathbf{Z}$, et nous avons

$$(r, s) = f(v(r+s)\,I + vz'(r-s)\,J).$$

Comme les deux anneaux sont de cardinal p^2, il s'ensuit que f est bijective et donc un isomorphisme. Pour montrer qu'on a $a^{p-1} = I$, il suffit donc de vérifier cette égalité dans $B = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Or, un élément $(b_1, b_2) \in B$ est inversible ssi b_1 et b_2 le sont et dans ce cas on a bien $(b_1, b_2)^{p-1} = (b_1^{p-1}, b_2^{p-1}) = (1, 1)$ d'après le petit théorème de Fermat. Remarquons aussi que nous avons un isomorphisme de groupes entre A^* et $(\mathbf{Z}/p\mathbf{Z})^* \times (\mathbf{Z}/p\mathbf{Z})^*$.

e) e1) D'après l'exercice 3, l'élément 3 est un générateur de $(\mathbf{Z}/17\mathbf{Z})^*$. Or, si on avait $3 = z^2$, alors 3 serait au plus d'ordre 8 (car $z^{16} = 1$). Donc 3 n'est pas un carré dans $\mathbf{Z}/17\mathbf{Z}$.

Comme 3 est d'ordre 16 et $J^2 = 3$, il s'ensuit que J est d'ordre 32.

e2) On calcule que $a^3 = 8\,I + 15\,J$ et $a^9 = I$. Donc a est bien d'ordre 9. Comme 9 et 32 sont premiers entre eux et que J et a commutent, il s'ensuit que aJ est d'ordre 288.