MT 282
03/12/94

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

Un corrigé du partiel No. 1

1) Soit t le nombre de minutes qui se sont écoulées depuis midi. D'après les informations fournies, nous avons

$$\begin{aligned} t &\equiv -3 \ (5) \\ t &\equiv -6 \ (9) \\ t &\equiv -31 \ (32). \end{aligned}$$

Les nombres $5, 9, 32$ sont premiers entre eux deux à deux. Ce système de congruences admet donc une solution t dont la classe modulo $5 \times 9 \times 32 = 1440 = 24 \times 60$ est unique. Les données permettent donc de retrouver le temps actuel avec certitude. 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

$$\mathbf{Z}/1440 \xrightarrow{\sim} \mathbf{Z}/5 \oplus \mathbf{Z}/9 \oplus \mathbf{Z}/32.$$

Nous avons

$$\begin{array}{llll} 288\,u_1 + 5\,v_1 = 1; & \text{sol. part.} & 288 \times 2 + 5 \times (-115) = 1. & \text{Posons} \quad x_1 = 576. \\ 160\,u_2 + 9\,v_2 = 1; & \text{sol. part.} & 160 \times 4 + 9 \times (-71) = 1. & \text{Posons} \quad x_2 = 640. \\ 45\,u_3 + 32\,v_3 = 1; & \text{sol. part.} & 45 \times 5 + 32 \times (-7) = 1 & \text{Posons} \quad x_3 = 225. \end{array}$$

Comme $-3 \equiv 2 \ (5)$, $-6 \equiv 3 \ (9)$ et $-31 \equiv 1 \ (9)$, nous avons $t \equiv 2 \times 576 + 3 \times 640 + 1 \times 225 \equiv 3297 \equiv 417 \ (1440)$. Puisque $417 = 6 \times 60 + 57$, il est 18h 57 et **le prochain métro part à 19h**.

2) Nous avons

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ \sigma^3 = e$$

et $\tau^2 = e$. Il s'ensuit que

$$\sigma^l \in \{e, \sigma, \sigma^2\} \text{ et } \tau^l \in \{e, \tau\}$$

quel que soit $l \in \mathbf{Z}$. Comme l'intersection de $\{e, \sigma, \sigma^2\}$ avec $\{e, \tau\}$ est réduite à l'élément neutre e, il s'ensuit que σ^l est égal à τ^l si et seulement si les deux sont égaux à e. Puisque σ est d'ordre 3 et τ d'ordre 2, c'est le cas si et seulement si l est divisible à la fois par 2 et 3; donc par 6. Ainsi nous avons $\sigma^l = \tau^l$ **si et seulement si** $l \equiv 0 \ (6)$**.**

3) a) Soient $\alpha = (8, 15)$, $\beta = (4, 15)$, $\gamma = (6, 20)$, $\delta = (3, 20)$. Nous avons $\pi(\alpha) = (8, 3, 5)$, $\pi(\beta) = (4, 3, 5)$, $\pi(\gamma) = (2, 4, 3, 5)$ et $\pi(\delta) = (4, 3, 5)$. D'après le théorème de classification, **les seuls couples de groupes isomorphes sont** (B, D) **et** (D, B).

b) Soit $\alpha = (15, a)$, $\beta = (20, b)$. Puisque les ordres sont égaux, nous avons $15a = 20b$, donc $3a = 4b$ et $a = 4k$, $b = 3k$ pour un $k \in \mathbf{N}$. Supposons que $k = 2^r 3^s l$, où $\text{PGCD}\,(l, 2) = \text{PGCD}\,(l, 3) = 1$. Donc

$$\begin{aligned} a = 4k &= 2^{r+2} 3^s l \\ b = 3k &= 2^r 3^{s+1} l \end{aligned}$$

Donc nous avons, à l'ordre des composantes près,

$$\begin{aligned} \pi(\alpha) &= (2^{r+2}, 3, 3^s, 5, \ldots) \\ \pi(\beta) &= (2^2, 2^r, 3^{s+1}, 5, \ldots) \end{aligned}$$

où $\ldots$ désigne les facteurs provenant de l. On voit que ces suites sont égales si et seulement si $r = 0$ et $s = 0$. Donc **l'isomorphisme a lieu si et seulement si** $a = 4k$ **et** $b = 3k$**, où** k **est un entier** ≥ 1 **qui n'est divisible ni par** 2 **ni par** 3.

4) a) Nous avons dans $\mathbf{Z}/31\mathbf{Z}$

$$2^2 = 4\,,\ 2^4 = 16\,,\ 2^5 = 32 = 1.$$

Ainsi, 2 **est d'ordre 5**. Nous avons

$$3^2 = 9\,,\ 3^4 = 81 = 19\,,\ 3^8 = 361 = 20\,,\ 3^{16} = 400 = 28 = -3.$$

Donc $3^{16} \neq 3$ et $3^{15} \neq 1$. En outre, $3^{10} = 3^2\,3^8 = 25 \neq 1$ et $3^6\,3^2\,3^4 = 16 \neq 1$. Comme l'ordre de 3 est un diviseur de 30, et que les diviseurs maximaux de 30 sont $15, 10$ et 6, il s'ensuit que 3 **est d'ordre** 30 **et** $(\mathbf{Z}/31\mathbf{Z})^*$ **est cyclique engendré par** 3.

b) Comme $(\mathbf{Z}/31\mathbf{Z})^*$ est cyclique d'ordre 30, engendré par 3, les solutions de $x^3 = 1$ sont $1, 3^{10}, 3^{20}$. On a

$$3^{10} = 3^2 \times 3^8 = 9 \times 20 = 180 = 25\,,\ 3^{20} = 3^4 \times 3^{16} = 19 \times (-3) = -57 = 5.$$

Les solutions sont les classes de $1, 25, 5$ **dans** $\mathbf{Z}/31\mathbf{Z}$**.**

5) a) Posons $b = 10$. On a $\overline{b}^c = \overline{1}$ dans $\mathbf{Z}/a\mathbf{Z}$. Donc a divise

$$b^c - 1 = (b-1)(b^{c-1} + b^{c-2} + \ldots + b + 1).$$

Puisque $\mathrm{PGCD}\,(a, b-1) = 1$, il s'ensuit d'après le lemme de Gauss que a divise $b^{c-1} + b^{c-2} + \ldots + b + 1$.

b) Puisque $\mathrm{PGCD}\,(a, b-1) = 1$, le nombre a divise

$$b^{l-1} + b^{l-2} + \ldots + b + 1$$

si et seulement si il divise

$$b^l - 1 = (b-1)(b^{l-1} + b^{l-2} + \ldots + b + 1).$$

Ceci est le cas ssi $\overline{b}^l = \overline{1}$ dans $\mathbf{Z}/a\mathbf{Z}$. Donc, **il faut et il suffit que**

$$l \equiv 0 \ \ (c).$$

a)

b) Substituons $y = t(x-1)$ dans l'équation $x^2 - y^2 = 1$. Nous trouvons

$$\begin{aligned} ((x-1)+1)^2 - t^2(x-1)^2 &= 1 \\ (x-1)^2 + 2(x-1) + 1 - t^2(x-1)^2 &= 1 \\ (1-t^2)(x-1)^2 + 2(x-1) &= 0 \end{aligned}$$

Nous écartons la solution $x = 1$ et nous supposons $t > 1$. Nous obtenons alors

$$x - 1 = \frac{2}{t^2-1} \tag{1}$$

$$x = \frac{t^2+1}{t^2-1} \tag{2}$$

$$y = t(x-1) = \frac{2t}{t^2-1}. \tag{3}$$

Si t est rationnel, il en est de même pour x et y, clairement. Deux valeurs différentes de t donnent lieu à des points différents, car $t = y/(x-1)$ d'après les équations (1) et (3).

c) Soit

$$\varphi : \mathbf{Q}_{>1} \to C^+ \,,\ t \mapsto (x,y) = \left(\frac{t^2+1}{t^2-1}, \frac{2t}{t^2-1}\right).$$

et soit

$$\psi : C^+ \to \mathbf{Q}_{>1} \,,\ (x,y) \mapsto t = \frac{y}{x-1}.$$

D'après les équations (1) et (3), on a $\psi(\varphi(t)) = t$. Soit $(x,y) \in C^+$. Vérifions que $\varphi(\psi(x,y)) = (x,y)$. Pour $t = y/(x-1)$, nous avons successivement

$$t^2 - 1 = \left(\frac{y}{x-1}\right)^2 - 1 = \frac{y^2-(x-1)^2}{(x-1)^2} = \frac{y^2-x^2+2x-1}{(x-1)^2} = \frac{2x-2}{(x-1)^2} = \frac{2}{x-1}\,,$$

où nous avons utilisé $y^2 - x^2 = -1$. Maintenant, on trouve

$$\frac{2}{t^2-1} = x-1\,, \quad \frac{t^2+1}{t^2-1} = x\,, \quad \frac{2t}{t^2-1} = 2\frac{y}{x-1}\frac{x-1}{2} = y.$$

Donc φ et ψ sont des bijections inverses l'une de l'autre.

d) D'après le point précédent, tout $(x,y) \in C^+$ est de la forme $\varphi(t)$ pour un $t \in \mathbf{Q}_{>1}$. Clairement, on a $t = u/v$ pour certains entiers $u > v \geq 1$ premiers entre eux. Il est alors immédiat de constater que

$$x = \frac{u^2+v^2}{u^2-v^2}\,, \quad y = \frac{2uv}{u^2-v^2}.$$