

CORRIGÉ DS 3 : *Arithmétiques.*  
*Groupes cycliques.*  
*Suites numériques.*

MPSI-Maths.

Mr Mamouni & El Hassani : [myismail1@menara.ma](mailto:myismail1@menara.ma)

Source disponible sur :

©<http://www.chez.com/myismail>

Lundi 10 Décembre 2007.

Durée: 3 heures 30mn.

**Problème 1. (Fonction indicatrice d'Euler.)**

- 1)  $n$  est premier  $\iff k \wedge n = 1, \forall 1 \leq k \leq n \iff \varphi(n) = 1$ .
- 2)  $k \wedge n = 1 \iff \exists u, v \in \mathbb{Z}$  tel que  $nu + kv = 1$   
 $\iff \exists v \in \mathbb{Z}$  tel que  $kv \equiv 1 [n]$   
 $\iff \exists \bar{v} \in \mathbb{Z}$  tel que  $\bar{k} \bar{v} = 1$   
 $\iff \bar{k}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$
- 3)  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un corps  $\iff \forall 1 \leq k \leq n, \bar{k}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$   
 $\iff \forall 1 \leq k \leq n, k \wedge n = 1$   
 $\iff n$  est premier
- 4)  $\text{card}U(\mathbb{Z}/n\mathbb{Z}) = \text{card}\{k \in [1, n] \text{ tel que } k \wedge n = 1\} = \varphi(n)$
- 5) Soit  $(m, n) \in \mathbb{N}^*$  tel que  $n \wedge m = 1$ .

- a) On vérifie d'abord que  $\theta(\bar{1}, \bar{1}) = \bar{1}$ ,  $\theta(\bar{a} + \bar{c}, \bar{b} + \bar{d}) = \varphi(\bar{a}, \bar{b}) + \varphi(\bar{c}, \bar{d})$  et enfin  $\theta(\bar{a} \bar{c}, \bar{b} \bar{d}) = \theta(\bar{a}, \bar{b}) \theta(\bar{c}, \bar{d})$   
**Injection :** Montrer que  $\text{Ker}(\theta) = \{(\bar{0}, \bar{0})\}$ .  
**Surjection :** Les ensembles de départ et d'arrivées ont même cardinal.
- b)  $\bar{x}$  inversible dans  $\mathbb{Z}/n\mathbb{Z}$ ,  $\bar{y}$  inversible dans  $\mathbb{Z}/m\mathbb{Z}$ , est évident par définition de l'inversibilité.  
 $(\bar{x}, \bar{y})$  inversible dans  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \iff \theta(\bar{x}, \bar{y}) \bar{x} \bar{y}$  inversible dans  $\mathbb{Z}/nm\mathbb{Z}$ , car  $\theta$  est un isomorphisme.
- c) D'après la question précédente, on a :

$$\begin{aligned}\varphi(nm) &= \text{card}(U(\mathbb{Z}/nm\mathbb{Z})) \\ &= \text{card}(U(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})) \\ &= \text{card}(U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})) \\ &= \varphi(n)\varphi(m)\end{aligned}$$

6) Par récurrence sur  $r$ .

$$\begin{aligned}7) \quad \varphi(p^\alpha) &= \text{card}\{k \in [1, p^\alpha] \text{ tel que } k \wedge p^\alpha = 1\} \\ &= p^\alpha - \text{card}\{k \in [1, p^\alpha] \text{ tel que } k \wedge p \neq 1\} \\ &= p^\alpha - \text{card}\{k \in [1, p^\alpha] \text{ tel que } p \text{ divise } k\} \\ &= p^\alpha - \text{card}\{k = qp \text{ tel que } q \in [1, p^{\alpha-1}]\} \\ &= p^\alpha - p^{\alpha-1}\end{aligned}$$

8) *Application :*

$$\begin{aligned}a) \quad \text{Posons } n &= \prod_{i=1}^r p_i^{\alpha_i}, \text{ avec } p_1 < \dots < p_r, \text{ donc } \varphi(n) = \\ \varphi\left(\prod_{i=1}^r p_i^{\alpha_i}\right) &= \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r p_i^{\alpha_i-1}(p_i - 1), \text{ si } \varphi(n) \text{ divise } n, \\ \text{alors } \prod_{i=1}^r (p_i - 1), &\text{ qui est pair divise } \prod_{i=1}^r p_i, \text{ ceci est impossible}\end{aligned}$$

si  $r \geq 3$  car 4 divisera  $\prod_{i=1}^r p_i$ , le seul cas possible est  $r = 2$  avec  $p_1 = 2, p_2 = 3$ .

$$\begin{aligned}b) \quad \text{Le nombre de fractions } \frac{k}{n}, &\text{ tel que } 1 \leq k \leq n \text{ qu'on peut} \\ \text{mettre sous la forme } \frac{a}{d}, &\text{ avec } a \wedge d = 1 \text{ est } \varphi(d), \text{ or au total} \\ \text{il y a exactement } n \text{ fraction, donc } &\sum_{d \text{ divise } n} \varphi(d) = n.\end{aligned}$$

## Problème 2. (Groupes cycliques)

- 1) Soit  $(x, y) \in G^2$ , or  $G = \langle a \rangle$ , donc  $\exists(p, q) \in \mathbb{Z}^2$  tel que  $x = a^p, y = a^q$ , donc  $x.y = a^{p+q} = y.x$ .
- 2) Posons  $p = kq$ , donc  $x \in \langle a^p \rangle \implies x = a^{\alpha p} = a^{\alpha k q} \in \langle a^q \rangle$ .

$$\begin{aligned}3) \quad a) \quad \text{On a } o(a) = n, \text{ donc } a^n = e \text{ et } (a^k)^{\frac{n}{n \wedge k}} &= (a^n)^{\frac{k}{n \wedge k}} = e, \text{ d'où} \\ m = o(a^k) \text{ divise } \frac{n}{n \wedge k}, \text{ d'autre part } a^{mk} = (a^k)^m = e, \text{ donc} \\ o(a) = n \text{ divise } mk, \text{ donc } \frac{n}{n \wedge k} \text{ divise } m \frac{k}{n \wedge k}, \text{ or } \frac{n}{n \wedge k} \wedge \frac{k}{n \wedge k}, \\ \text{donc } \frac{n}{n \wedge k} \text{ divise } m.\end{aligned}$$

$$b) \quad G = \langle a^k \rangle \iff \text{card}G = o(a^k) \iff n = \frac{n}{n \wedge k} \iff k \wedge n = 1.$$

c) Le nombre des générateurs de  $G$  est celui des entier  $k$ , tel que  $1 \leq k \leq n$  tel que  $k \wedge n = 1$ , c'est à dire  $\varphi(n)$ .

$$\begin{aligned}4) \quad \text{Il est clair que } 1 \in \mathbb{U}_n. \text{ Soit } z_1, z_2 \in \mathbb{U}_n, \text{ alors } (z_1 z_2^{-1})^n &= \frac{z_1^n}{z_2^n}, \text{ donc} \\ z_1 z_2^{-1} \in \mathbb{U}, \text{ d'où } \mathbb{U} \text{ est un sous-groupe de } (\mathbb{C}^*, \times).\end{aligned}$$

D'autre part :  $\mathbb{U}_n = \{e^{i\frac{2k\pi}{n}}, 0 \leq k \leq n-1\} = \langle w \rangle$  où  $w = e^{i\frac{2\pi}{n}}$ , donc monogène, or il est fini de cardinal,  $n$ , donc cyclique.

Il y exactement  $\varphi(n)$  racines  $n^{\text{ème}}$  primitives de l'unité, ce sont les  $w^k$  tel que ,  $1 \leq k \leq n$  et  $k \wedge n = 1$ .

Pour  $n = 3, w = j$ , les racines primitives sont  $j$  et  $j^2$ .

Pour  $n = 4, w = i$ , les racines primitives sont  $i$  et  $i^3 = -i$ .

$$\begin{aligned}5) \quad a) \quad \text{Il est très simple de montrer que } H_d \text{ est un sous groupe de} \\ (G, \cdot), \text{ en vérifiant que, } e \in H(e^d = e) \text{ et que si } (x, y) \in H^2, \\ (x^d = y^d = e), \text{ alors } x.y^{-1} \in H_d \text{ car } (x.y^{-1})^d = x^d y^{-d} = e. \text{ Mon-} \\ \text{trons maintenant que } H_d = \langle a^{\frac{n}{d}} \rangle, \text{ par double inclusion, en} \\ \text{utilisant surtout que } o(a) = n.\end{aligned}$$

$$\begin{aligned}- \quad x \in H_d \subset G = \langle a \rangle &\implies x = a^p, x^d = e \\ &\implies x = a^p, a^{pd} = e \\ &\implies x = a^p \text{ et } n \text{ divise } pd \\ &\implies x = a^p \text{ et } \frac{n}{d} \text{ divise } p = k \frac{n}{d} \\ &\implies x = a^{k \frac{n}{d}} \in \langle a^{\frac{n}{d}} \rangle\end{aligned}$$

$$\begin{aligned}- \quad \text{Inversement, } x \in \langle a^{\frac{n}{d}} \rangle &\implies x = a^{k \frac{n}{d}} \implies x^d = a^{nk} = e \\ &\implies x \in H_d\end{aligned}$$

b) Soit  $H$  un sous groupe de  $(G, \cdot)$ .

i. Cette question a été déjà traité en TD, les étapes à suivre sont les suivantes.

- Montrer que  $f$  est un morphisme de groupe.
- En déduire que  $f^{-1}(H)$  est un sous-groupe de  $(\mathbb{Z}, +)$ , donc de la forme  $p\mathbb{Z}$ .
- Montrer par double inclusion que  $H = \langle a^p \rangle$ .

ii. Puisque  $p \wedge n$  divise  $p$ , alors  $\langle a^p \rangle \subset \langle a^{p \wedge n} \rangle$ , d'autre part  $\text{card} \langle a^{p \wedge n} \rangle = o(a^{p \wedge n}) = \frac{o(a^{p \wedge n})}{n \wedge (p \wedge n)} = \frac{n}{p \wedge n} = o(a^p) = \text{card} \langle a^p \rangle$

6) La surjection découle de la question 5.b.ii), car pour tout  $h \in \mathcal{H}, \exists d = p \wedge n \in \mathcal{D}_n$  tel que  $H = H_d$ .

L'injection, soit  $d_1, d_2 \in \mathcal{D}_n$ ,

$$\begin{aligned} \Phi(d_1) = \Phi(d_2) &\implies H_{d_1} = H_{d_2} \\ &\implies \left\langle a^{\frac{n}{d_1}} \right\rangle = \left\langle a^{\frac{n}{d_2}} \right\rangle \\ &\implies o\left(\frac{n}{d_1}\right) = o\left(\frac{n}{d_2}\right) \\ &\implies \frac{n}{n \wedge \frac{n}{d_1}} = \frac{n}{n \wedge \frac{n}{d_2}} \\ &\implies d_1 = d_2 \end{aligned}$$

donc  $\Phi$  est bijective.

7) Comme  $\Phi$  est bijective, alors le nombre de sous groupes dans  $G$ , est égale a celui des diviseurs de  $n = p^\alpha$ , qui sont les  $p^k$  tel que  $0 \leq k \leq \alpha$ , il y en a exactement  $\alpha + 1$ .

### Problème 3. (Étude d'une suite récurrente)

Préliminaire : Étudier la fonction  $\ln(1+x) - x$  sur  $[-1, +\infty[$ .

- $1 - u_{n+1} = (1 - u_n)(1 - \delta u_n)$ .
  - On montre d'abord (facile) par récurrence que  $0 \leq u_n \leq 1$ , donc  $(u_n)$  est croissante, car  $u_{n+1} - u_n = \delta u_n(1 - u_n)$ , d'où  $u_n \geq u_0 = a$ .
  - $(u_n)$  est croissante, majorée par 1, donc converge vers  $l$  tel que  $0 = \delta l(1 - l)$  or  $u_n \geq \delta > 0$ , donc  $l \geq \delta > 0$ , d'où  $l = 1$ .
- $1 - u_{n+1} = (1 - \delta u_n)(1 - u_n) \leq (1 - \delta a)(1 - u_n)$ , car  $a \leq u_n \leq 1$ .

b) Par récurrence.

c)  $0 \leq \delta, u_k \leq 1 \implies 1 - \delta u_k \geq 1 - \delta \geq 0 \implies$

$$\ln x_{k+1} - \ln x_k = \ln \frac{1 - \delta u_k}{1 - \delta} \geq 0, \text{ d'autre part :}$$

$$\ln \frac{1 - \delta u_k}{1 - \delta} = \ln \left( 1 + \frac{\delta(1 - u_k)}{1 - \delta} \right) \leq \frac{\delta(1 - u_k)}{1 - \delta} \leq \frac{\delta}{1 - \delta} (1 - a) q^k.$$

d)  $S_{n+1} - S_n = \ln x_{n+1} - \ln x_n \geq 0$ , donc  $S_n$  est croissante, d'autre

$$\begin{aligned} \text{part } S_n &\leq \sum_{k=0}^{n-1} \frac{\delta}{1 - \delta} (1 - a) q^k \\ &= \frac{\delta}{1 - \delta} (1 - a) \frac{1 - q^n}{1 - q} \\ &\leq \frac{\delta}{1 - \delta} (1 - a) \frac{1}{1 - q} \end{aligned}$$

donc majorée et par suite converge.

e)  $S_n$  est une somme télescopique, avec  $S_n = \ln x_n - \ln x_0$  qui converge vers  $S$ , donc  $\ln x_n = S_n + \ln x_0$  converge vers  $S + \ln x_0$ , d'où  $x_n$  converge vers  $\mu = e^{S + \ln x_0} = e^S x_0 = e^S (1 - a) > 0$ , donc

$$x_n = \frac{1 - u_n}{(1 - \delta)^n} \sim \mu, \text{ donc } 1 - u_n \sim \mu(1 - \delta)^n.$$

3) a) On a :  $\frac{y_{k+1}}{y_k} = \frac{u_{k+1}}{u_k} \frac{1 - u_k}{1 - u_{k+1}} \frac{(1 + \delta)^n}{(1 + \delta)^{n+1}}$

$$= \frac{1 + \delta(1 - u_k)}{(1 + \delta)(1 - \delta u_k)}$$

$$= \frac{(1 + \delta)(1 - \delta u_k) + \delta^2 u_k}{(1 + \delta)(1 - \delta u_k)}$$

$$= 1 + \frac{\delta^2 u_k}{(1 + \delta)(1 - \delta u_k)}$$

b) On remarque d'abord que :

$$\begin{aligned} \ln \left( \frac{(1 - a)y_n}{a(1 - u_n)(1 + \delta)^n} \right) &= \ln \left( \frac{y_n}{(1 - u_n)(1 + \delta)^n} \right) - \ln \left( \frac{a}{1 - a} \right) \\ &= \ln y_n - \ln y_0 \\ &= T_n \end{aligned}$$

Il suffit donc de montrer que  $0 \leq T_n = \sum_{k=0}^{n-1} \ln \frac{y_{k+1}}{y_k} \leq \frac{n\delta^2}{1-\delta^2}$ .

En effet,

$$\frac{y_{k+1}}{y_k} = 1 + \frac{\delta^2 u_k}{(1+\delta)(1-\delta u_k)} \geq 1 \implies \ln \frac{y_{k+1}}{y_k} \geq 0 \implies T_n \geq 0.$$

D'autre part,  $\ln \frac{y_{k+1}}{y_k} = \ln \left( 1 + \frac{\delta^2 u_k}{(1+\delta)(1-\delta u_k)} \right)$

$$\leq \frac{\delta^2 u_k}{(1+\delta)(1-\delta u_k)}$$

$$= \frac{\delta^2}{(1-\delta^2)} \cdot \frac{u_k(1-\delta)}{1-\delta u_k}$$

$$= \frac{\delta^2}{(1-\delta^2)} \cdot \frac{u_k - \delta u_k}{1-\delta u_k}$$

$$\leq \frac{\delta^2}{(1-\delta^2)}$$

Donc,  $T_n = \sum_{k=0}^{n-1} \ln \frac{y_{k+1}}{y_k} \leq \sum_{k=0}^{n-1} \frac{\delta^2}{(1-\delta^2)} = n \frac{\delta^2}{(1-\delta^2)}$ .

4) a)  $\left\lceil \frac{t}{\delta} \right\rceil \leq \frac{t}{\delta} \leq \left\lceil \frac{t}{\delta} \right\rceil + 1 \implies \left\lceil \frac{t}{\delta} \right\rceil \delta \leq t \leq \left( \left\lceil \frac{t}{\delta} \right\rceil + 1 \right) \delta$ .

b)  $\left\lceil \frac{t}{\delta} \right\rceil \delta \leq t \leq \left( \left\lceil \frac{t}{\delta} \right\rceil + 1 \right) \delta \implies t - \delta \leq \left\lceil \frac{t}{\delta} \right\rceil \delta \leq t$ ,

donc  $\lim_{\delta \rightarrow 0} \left\lceil \frac{t}{\delta} \right\rceil \delta = t$ .

$$\ln(1+\delta)^{\left\lceil \frac{t}{\delta} \right\rceil} = \left\lceil \frac{t}{\delta} \right\rceil \ln(1+\delta) = \left( \left\lceil \frac{t}{\delta} \right\rceil \delta \right) \frac{\ln(1+\delta)}{\delta} \longrightarrow t.$$

Donc  $\lim_{\delta \rightarrow 0} (1+\delta)^{\left\lceil \frac{t}{\delta} \right\rceil} = e^t$ .

c) Posons  $n = \left\lceil \frac{t}{\delta} \right\rceil$ , donc  $n\delta^2 = \left( \left\lceil \frac{t}{\delta} \right\rceil \delta \right) \delta \longrightarrow 0$ ,

or  $0 \leq T_n = \ln y_n - \ln y_0 \leq \frac{n\delta^2}{1-\delta^2}$ , d'où  $\lim_{\delta \rightarrow 0} y_n = y_0$ , d'autre part

$$y_n = \frac{u_n}{(1-u_n)(1+\delta)^n}, \text{ donc } u_n = \frac{y_n}{y_n + \frac{1}{(1+\delta)^n}} \longrightarrow \frac{y_0}{y_0 + e^{-t}}, \text{ avec}$$

$$y_0 = \frac{a}{1-a}.$$

## Exercice. (Groupe symétrique)

Vu en TD

1)  $(\alpha\sigma\alpha^{-1})\alpha(i_1) = (\alpha\sigma)(i_1) = \alpha(i_2)$ , et ainsi de suite.

2)  $(1\ 3\ 2)(1\ 2\ 3\ 4)(1\ 2\ 3) = (3\ 1\ 2\ 4)$ , prendre  $\alpha = (1\ 3\ 2)$  et  $\sigma = (1\ 2\ 3\ 4)$ .

3)  $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$  et  $(1\ 2\ 3\ 4)^3 = (1\ 4\ 3\ 2)$ .

**Fin.**