

## DS n°7

ÉNS, durée 6 heures

On désigne par  $\mathbb{N}^*$  l'ensemble des entiers  $\geq 1$ . On notera  $d \mid n$  la relation de divisibilité entre deux entiers  $d$  et  $n$ . On appelle *fonction arithmétique* tout élément de  $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$ . On munit  $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$  d'une loi de composition interne  $*$  appelée *convolution* et définie par

$$(f * g)(n) := \sum_{d \mid n} f(d)g(n/d),$$

où la somme porte sur les diviseurs  $d$  de  $n$ . On admettra que la convolution est bien une opération interne et qu'elle est commutative et associative.

On appelle *série de Dirichlet* associée à  $f$  la série, dépendant d'un paramètre réel  $s$ ,

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

On note  $L(s, f)$  la somme de cette série en tout point de convergence  $s \in \mathbb{R}$ .

On considère la fonction  $\tau_k \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  définie par  $\tau_k = \mathbf{1} * \cdots * \mathbf{1}$  où  $\mathbf{1} \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  désigne la fonction constante valant 1. Lorsque  $n \in \mathbb{N}^*$ , on a donc

$$\tau_k(n) = \sum_{\substack{(m_1, \dots, m_k) \in (\mathbb{N}^*)^k \\ m_1 \cdots m_k = n}} 1 = \text{card}\{(m_1, \dots, m_k) \in (\mathbb{N}^*)^k : m_1 \cdots m_k = n\}.$$

Ainsi  $\tau_2(n)$  désigne le nombre de diviseurs de l'entier  $n$  et  $\tau_1(n) = 1$  pour tout  $n \in \mathbb{N}^*$ .

On note  $D_k(s, f) = L(s, \tau_k f)$  la somme de la série de Dirichlet associée au produit (classique)  $\tau_k f$  des fonctions arithmétique  $\tau_k$  et  $f$  en tout point de convergence  $s \in \mathbb{R}$ . Finalement, étant donné un nombre premier  $p$ , on introduit la fonction  $\mu_p : \mathcal{F}(\mathbb{N}^*, \mathbb{C}) \rightarrow \mathbb{C}$  définie par

$$\mu_p(f) := \sum_{k=1}^p f(k).$$

Le but de ce problème est d'étudier dans quel cas une fonction  $f \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  qui est  $p$ -périodique satisfait  $D_k(1, f) = 0$ . On obtiendra un résultat complet lorsque  $f$  est à valeurs dans  $\mathbb{Q}$ .

On introduit aussi la somme  $S_f : \mathbb{R}^+ \rightarrow \mathbb{C}$  appelée *fonction sommatoire associée à la fonction arithmétique*  $f \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  définie par

$$S_f(x) := \sum_{1 \leq n \leq x} f(n),$$

où  $x \in \mathbb{R}^+$ . La sommation sur les entiers  $n$  tels que  $1 \leq n \leq x$  signifie que l'on somme  $n$  entre 1 et  $[x]$  où  $[x]$  désigne la partie entière de  $x$ .

### I– Séries de Dirichlet et formules de sommation.

Soit  $p$  un nombre premier. On note  $\mathcal{F}(\mathbb{Z}, K)$  l'ensemble des applications de  $\mathbb{Z}$  dans  $K$  où  $K$  est un corps qui pourra être  $\mathbb{R}$ ,  $\mathbb{C}$  ou  $\mathbb{Q}$  et  $\mathcal{F}_p^-(\mathbb{Z}, K)$  l'ensemble des éléments de  $\mathcal{F}(\mathbb{Z}, K)$  qui sont de plus impairs et  $p$ -périodiques.

1. Lorsque  $f \in \mathcal{F}_p^-(\mathbb{Z}, \mathbb{C})$ , montrer que l'on a  $\mu_p(f) = 0$ .
2. Sommation d'Abel. Soient  $g : [1, +\infty[ \rightarrow \mathbb{C}$  une fonction dérivable sur l'intervalle  $[1, +\infty[$  tout entier et  $h \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  une fonction arithmétique. Montrer que l'identité suivante est valable pour tout  $x \geq 1$ ,

$$\sum_{1 \leq n \leq x} h(n)g(n) = S_h(x)g(x) - \int_1^x S_h(t)g'(t)dt.$$

3. La méthode de l'hyperbole. Montrer que pour toutes  $f, g \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  et tous  $x, y \in \mathbb{R}$  tels que  $1 \leq y \leq x$  on a :

$$S_{f*g}(x) = \sum_{1 \leq n \leq y} g(n)S_f(x/n) + \sum_{1 \leq n \leq x/y} f(n)S_g(x/n) - S_f(x/y)S_g(y).$$

4. (a) Soient  $f \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  bornée et  $s > 1$ . Montrer que la série

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

est absolument convergente. On note  $L(f, s)$  sa somme.

- (b) Soient  $f$  et  $g$  dans  $\mathcal{F}(\mathbb{N}^*, \mathbb{C})$ . Montrer que lorsque les séries  $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$  et  $\sum_{n=1}^{\infty} \frac{g(n)}{n^s}$  sont

absolument convergentes, alors la série  $\sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s}$  est encore absolument convergente.

- (c) On appelle fonction complètement multiplicative une fonction  $f \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  vérifiant  $f(mn) = f(m)f(n)$  pour tous  $m, n \in \mathbb{N}^*$ . Soit  $f \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  complètement multiplicative. Montrer que pour tout  $s > 1$  on a

$$L(s, f) = \prod_{\ell \text{ premier}} \left(1 - \frac{f(\ell)}{\ell^s}\right)^{-1}.$$

5. (a) Soit  $f \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  telle qu'il existe  $\alpha > 0$  et  $M > 0$  tels que  $|S_f(x)| \leq Mx^\alpha$  pour tout  $x \geq 1$ . En utilisant une sommation d'Abel (Question I.2), montrer que, pour tout  $s > \alpha$ , la série  $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$  converge et que sa somme vaut

$$L(s, f) = s \int_1^{+\infty} S_f(t)t^{-s-1}dt.$$

- (b) En déduire que l'application  $] \alpha, +\infty[ \rightarrow \mathbb{C}, s \mapsto L(s, f)$  est continue.
- (c) Soit  $f \in \mathcal{F}_p^-(\mathbb{Z}, \mathbb{C})$ . Montrer que, pour tout réel  $s > 0$ , la série  $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$  est convergente et que l'application  $]0, +\infty[ \rightarrow \mathbb{C}, s \mapsto L(s, f)$  est continue.
- (d) On pose  $\zeta(s) := L(s, 1)$  en tout point de convergence  $s \in \mathbb{R}$ . Soit  $s > 1$ . Montrer que la série  $\sum_{n=1}^{\infty} \frac{1}{n^s}$  est bien convergente. En s'inspirant de la question a), montrer

$$\lim_{\substack{s \rightarrow 1 \\ s > 1}} ((s-1)\zeta(s)) = 1.$$

## II– Caractères modulo $p$ .

Nous rappelons que  $p$  est un nombre premier fixé. Soit  $G = (\mathbb{Z}/p\mathbb{Z})^\times$  le groupe multiplicatif des éléments inversibles de l'anneau  $\mathbb{Z}/p\mathbb{Z}$ . Soit

$$\widehat{G} = \{g : G \rightarrow \mathbb{U} \text{ morphisme}\}$$

le groupe des morphismes de  $G$  vers le groupe multiplicatif  $\mathbb{U}$  des nombres complexes de module 1. On munit  $\widehat{G}$  de la loi de groupe déduite de la multiplication dans  $\mathbb{U}$ . On peut relever un morphisme  $g \in \widehat{G}$  en une fonction  $\chi \in \mathcal{F}(\mathbb{Z}, \mathbb{C})$  en posant

$$\chi(n) = \begin{cases} g(n) & \text{si } \text{pgcd}(n, p) = 1, \\ 0 & \text{sinon.} \end{cases}$$

On dit alors que  $\chi$  est un *caractère modulo  $p$* . On appelle *caractère principal modulo  $p$*  la fonction  $\chi_0 \in \mathcal{F}(\mathbb{Z}, \mathbb{C})$  associée à l'élément neutre de  $\widehat{G}$ . Autrement dit  $\chi_0$  est définie par

$$\chi_0(n) = \begin{cases} 1 & \text{si } \text{pgcd}(n, p) = 1, \\ 0 & \text{sinon.} \end{cases}$$

On définit le conjugué  $\bar{\chi}$  d'un caractère  $\chi$  par  $\bar{\chi}(n) = \overline{\chi(n)}$  pour tout  $n \in \mathbb{Z}$ .

6. Soit  $\chi$  un caractère modulo  $p$ .

- (a) Montrer que  $\chi$  est une fonction arithmétique complètement multiplicative.
- (b) Montrer que  $\chi$  est impair si, et seulement si, l'on a  $\chi(-1) = -1$ .
- (c) Montrer que, pour tous entiers  $k \geq 1$  et  $n \geq 1$ , on a

$$(\chi\tau_{k+1})(n) = (\chi * (\chi\tau_k))(n).$$

7. Soit  $H$  un groupe fini commutatif.

- (a) Soient  $x \in H$  d'ordre  $s$  et  $y \in H$  d'ordre  $t$  avec  $\text{pgcd}(s, t) = 1$ . Montrer qu'il existe un élément  $z \in H$  d'ordre égal à  $st$ .
- (b) En déduire que si  $x \in H$  est d'ordre  $s$  et  $y \in H$  est d'ordre  $t$  avec  $\text{pgcd}(s, t) = 1$  alors il existe  $z \in H$  tel que l'ordre de  $z$  soit  $\text{ppcm}(s, t)$ .
- (c) Soit  $h \in H$  d'ordre maximal. Montrer que pour tout  $x \in H$  l'ordre de  $x$  divise l'ordre de  $h$ .
- (d) En déduire que le groupe  $G = (\mathbb{Z}/p\mathbb{Z})^\times$  est cyclique.

8. (a) Montrer que  $\widehat{G}$  est un groupe de cardinal  $p-1$  et que  $\widehat{G}$  est cyclique.

- (b) Soit  $\chi$  caractère non principal modulo  $p$  différent de  $\chi_0$ . Montrer que  $\mu_p(\chi) = 0$ .

(c) Montrer de plus que, pour tout entier  $c$  premier à  $p$ , on a :

$$\sum_{\chi \bmod p} \chi(n) \bar{\chi}(c) = \begin{cases} p-1 & \text{si } n \equiv c \pmod{p}, \\ 0 & \text{sinon.} \end{cases}$$

9. (a) Soit  $\varepsilon > 0$ . On admettra qu'il existe un nombre réel  $T_{2,\varepsilon}$  tel que, pour tout  $n \in \mathbb{N}^*$ , on ait  $\tau_2(n) \leq T_{2,\varepsilon} n^\varepsilon$ . Montrer qu'alors, pour tout entier  $k \geq 3$ , il existe un nombre réel  $T_{k,\varepsilon}$  tel que, pour tout  $n \in \mathbb{N}^*$ , on ait  $\tau_k(n) \leq T_{k,\varepsilon} n^\varepsilon$ .
- (b) On pourra utiliser librement la question a) pour répondre à la question suivante. Soit  $\chi$  un caractère modulo  $p$  différent de  $\chi_0$ . En utilisant la méthode de l'hyperbole (Question I.3) avec un choix pertinent de  $y$ , montrer que, pour tout  $k \in \mathbb{N}^*$  et tout  $\varepsilon > 0$ , il existe  $M_k(p, \varepsilon)$  tel que, pour tout  $x \in \mathbb{R}^+$  on ait

$$|S_{\chi\tau_k}(x)| \leq M_k(p, \varepsilon) x^{1-1/k+\varepsilon}.$$

10. Soit  $\chi$  un caractère modulo  $p$  différent de  $\chi_0$  et soit  $k$  un entier  $> 0$ . Dédurre de la question précédente que, pour tout  $s \in ]1 - 1/k, +\infty[$ , la série  $\sum_{n=1}^{\infty} \frac{\tau_k(n) \chi(n)}{n^s}$  est convergente et que la fonction  $]1 - 1/k, +\infty[ \rightarrow \mathbb{C}, s \mapsto D_k(s, \chi)$  est une fonction continue. Montrer la relation

$$D_k(1, \chi) = L(1, \chi)^k.$$

### III– Calculs autour de $D_k(1, f)$ .

Etant donné un nombre premier  $p$ , un entier strictement positif  $k$  et un entier relatif  $r$ , on considère la somme finie

$$x_k(r; p) := \frac{1}{p^k} \sum_{\substack{(m_1, \dots, m_k) \in \{1, \dots, p-1\}^k \\ m_1 \cdots m_k \equiv r \pmod{p}}} \cot\left(\frac{\pi m_1}{p}\right) \cdots \cot\left(\frac{\pi m_k}{p}\right),$$

où  $\cot$  désigne la fonction cotangente qui est le rapport du cosinus avec le sinus. Lorsque cette somme est vide, on conviendra qu'elle vaut 0.

On note  $\langle x \rangle := x - [x]$  la partie fractionnaire d'un nombre réel  $x$  et aussi  $B : \mathbb{R} \rightarrow \mathbb{R}$  la première fonction de Bernoulli définie par

$$B(x) := \begin{cases} \langle x \rangle - \frac{1}{2} & \text{si } x \notin \mathbb{Z}, \\ 0 & \text{sinon.} \end{cases}$$

On admettra que, pour tout  $x \in \mathbb{R}$ , la série

$$-\frac{1}{\pi} \sum_{n=1}^{\infty} \frac{\sin(2\pi n x)}{n}$$

converge simplement vers  $B(x)$ .

11. Montrer que l'application  $\mathbb{Z} \rightarrow \mathbb{C}, r \mapsto x_k(r; p)$  est impaire et  $p$ -périodique.
12. Soit  $k$  un entier strictement positif et soit  $r$  un entier relatif premier à  $p$ . Montrer que

$$\lim_{N \rightarrow +\infty} \left( \sum_{\substack{|n| \leq N \\ n \equiv r \pmod{p}}} \frac{\tau_k(|n|)}{n} \right) = \frac{1}{p-1} \sum_{\substack{\chi \bmod p \\ \chi \neq \chi_0}} \bar{\chi}(r) (1 - \chi(-1)) L(1, \chi)^k.$$

13. On note, dans cette question et dans les questions suivantes,

$$\mathbf{e}(t) = e^{2\pi it} \quad (t \in \mathbb{R}).$$

Soit  $m$  un entier relatif premier à  $p$ . Montrer que

$$\sigma_p(m) := \sum_{a=1}^{p-1} B\left(\frac{a}{p}\right) \mathbf{e}\left(\frac{am}{p}\right) = -\frac{i}{2} \cot\left(\frac{\pi m}{p}\right).$$

14. Soient  $\chi$  un caractère modulo  $p$  et un entier  $n \in \mathbb{Z}$ . On appelle *somme de Gauss* le nombre complexe  $\tau(\chi, n)$  défini par la somme finie

$$\tau(\chi, n) := \sum_{m=1}^p \chi(m) \mathbf{e}(mn/p).$$

On notera simplement  $\tau(\chi)$  le nombre  $\tau(\chi, 1)$ .

(a) Supposons  $\chi \neq \chi_0$ . Montrer que

$$\tau(\chi, n) = \overline{\chi}(n) \tau(\chi).$$

(b) Supposons  $\chi \neq \chi_0$ . En calculant  $\sum_{n=1}^p |\tau(\chi, n)|^2$ , montrer que

$$|\tau(\chi)|^2 = p.$$

(c) En utilisant les questions a et b, montrer que

$$L(1, \chi) = \frac{\pi i \tau(\chi)}{p} \sum_{a=1}^p \overline{\chi}(a) B\left(\frac{a}{p}\right).$$

15. Soit  $\chi$  un caractère modulo  $p$  impair. En utilisant la formule de la question précédente, montrer que

$$L(1, \chi) = \frac{\pi}{2p} \sum_{m=1}^p \chi(m) \cot\left(\frac{\pi m}{p}\right).$$

16. Soit  $k \in \mathbb{N}^*$  et soit  $r$  un entier relatif premier à  $p$ . Montrer que

$$x_k(r; p) := \frac{1}{2} \left(\frac{2}{\pi}\right)^k \lim_{N \rightarrow +\infty} \left( \sum_{\substack{|n| \leq N \\ n \equiv r \pmod{p}}} \frac{\tau_k(|n|)}{n} \right).$$

En déduire que pour tout  $f \in \mathcal{F}_p^-(\mathbb{Z}, \mathbb{C})$  on a

$$D_k(1, f) = 2 \left(\frac{\pi}{2}\right)^k \sum_{r=1}^{(p-1)/2} f(r) x_k(r; p).$$

17. Soit  $s > 1$ . Montrer que

$$\sum_{\substack{n \in \mathbb{N}^* \\ n \equiv 0 \pmod{p}}} \frac{\tau_k(n)}{n^s}$$

est convergente de somme égale à  $\zeta(s)^k - L(s, \chi_0)^k$ . Puis montrer que

$$L(s, \chi_0)^k = \zeta(s)^k (1 - 1/p^s)^k.$$

18. Dans cette question, on suppose que le nombre premier  $p$  est impair. Soient  $k$  un entier  $\geq 2$  et  $f$  une fonction  $p$ -périodique dans  $\mathcal{F}(\mathbb{Z}, \mathbb{C})$ . Montrer que  $D_k(s, f)$  tend vers une limite finie lorsque  $s$  tend vers 1 par valeur supérieure si, et seulement si,  $f(0) = 0$  et  $\mu_p(f) = 0$ . Dans ce cas-là, montrer que l'on a

$$\lim_{\substack{s \rightarrow 1 \\ s > 1}} D_k(s, f) = \frac{1}{p-1} \sum_{\substack{\chi \\ \chi \neq \chi_0}} c_\chi(f) L(1, \chi)^k,$$

où la somme porte sur l'ensemble des caractères modulo  $p$  et où  $c_\chi(f) = \sum_{r=1}^p f(r) \overline{\chi}(r)$ . Pour cela, on pourra utiliser la question III.16.

#### IV– Un peu d'algèbre linéaire ...

19. Soit  $\alpha$  un nombre complexe qui annule un polynôme non nul de  $\mathbb{Q}[X]$ .  
 Soit  $\mathbb{Q}[\alpha] = \{z \in \mathbb{C} : \exists P \in \mathbb{Q}[X] \quad z = P(\alpha)\}$ . On considère  $\pi_\alpha$  le polynôme unitaire de  $\mathbb{Q}[X]$  de degré minimal qui admet pour racine  $\alpha$ .
- (a) Montrer que  $\mathbb{Q}[\alpha]$  est un  $\mathbb{Q}$ -espace vectoriel de dimension  $\deg(\pi_\alpha)$ .
  - (b) Soit  $x$  un élément non nul de  $\mathbb{Q}[\alpha]$ . Montrer que la multiplication par  $x$  induit un endomorphisme de  $\mathbb{Q}[\alpha]$ . En déduire que  $x$  admet un inverse dans  $\mathbb{Q}[\alpha]$ .
  - (c) En déduire que  $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$  avec

$$\mathbb{Q}(\alpha) = \{z \in \mathbb{C} : \exists P, R \in \mathbb{Q}[X] \quad z = P(\alpha)/R(\alpha), \quad R(\alpha) \neq 0\}.$$

On rappelle que  $p$  est un nombre premier fixé.

20. Dans cette question, on pourra utiliser librement que si  $P \in \mathbb{Z}[X]$  est un polynôme de degré  $n$  de la forme  $P(X) = \sum_{0 \leq k \leq n} a_k X^k$  satisfaisant  $p \nmid a_n, p \mid a_k$  pour tout  $0 \leq k \leq n-1$  et  $p^2 \nmid a_0$ , alors  $P$  est irréductible dans  $\mathbb{Q}[X]$ .
- (a) Soit  $P_p(X) = X^{p-1} + X^{p-2} + \dots + 1$ . En considérant  $P_p(X+1)$ , montrer que le polynôme  $P_p$  est irréductible dans  $\mathbb{Q}[X]$ .
  - (b) Soient  $\xi_p = e(1/p)$ . Montrer que  $P_p$  est le polynôme minimal de  $\xi_p$ . Montrer que, pour tout entier  $1 \leq c \leq p-1$ , on a  $P_p(\xi_p^c) = 0$ .
  - (c) Soit  $c$  un entier premier à  $p$ . Montrer qu'il existe une application  $\Phi_c : \mathbb{Q}[\xi_p] \rightarrow \mathbb{Q}[\xi_p]$  vérifiant

$$\Phi_c(P(\xi_p)) = P(\xi_p^c).$$

Montrer que  $\Phi_c$  définit un automorphisme du corps  $\mathbb{Q}[\xi_p]$ .

- (d) Soient  $Q$  et  $R \in \mathbb{Q}[X]$  tels que  $R(\xi_p) \neq 0$ . Montrer que

$$\Phi_c\left(\frac{Q(\xi_p)}{R(\xi_p)}\right) = \frac{Q(\xi_p^c)}{R(\xi_p^c)}.$$

On supposera dorénavant que le nombre premier  $p$  est impair.

21. Soient  $k$  un entier strictement positif et  $r$  un entier relatif premier à  $p$ .
- (a) Montrer que  $i^k x_k(r; p) \in \mathbb{Q}(\xi_p)$ .
  - (b) Montrer que  $\Phi_c(i^k x_k(r; p)) = i^k x_k(c^k r; p)$ .

Soit  $\mathbf{v} = (v_0, \dots, v_{m-1}) \in \mathbb{C}^m$ . On pose

$$A_m(\mathbf{v}) := \begin{pmatrix} v_0 & v_1 & \dots & v_{m-2} & v_{m-1} \\ v_1 & v_2 & \dots & v_{m-1} & -v_0 \\ \vdots & \vdots & & \vdots & \vdots \\ v_{m-1} & -v_0 & -v_1 & \dots & -v_{m-2} \end{pmatrix}.$$

22. Soient  $k$  un entier naturel premier à  $p-1$  et  $f \in \mathcal{F}_p^-(\mathbb{Z}, \mathbb{Q})$  tels que  $D_k(1, f) = 0$ . On note  $a$  un générateur du groupe cyclique  $(\mathbb{Z}/p\mathbb{Z})^\times$ .

(a) Montrer que

$$\sum_{j=0}^{p-2} f(a^j) x_k(a^j; p) = 0.$$

En utilisant les morphismes  $\Phi_c$ , montrer que, pour tout  $\ell \in \mathbb{Z}$ , on a

$$\sum_{j=0}^{p-2} f(a^j) x_k(a^{j+\ell}; p) = 0.$$

En déduire la relation

$$\sum_{j=0}^{(p-3)/2} f(a^j) x_k(a^{j+\ell}; p) = 0.$$

(b) Soient  $\mathbf{x} = (x_k(1; p), x_k(a; p), \dots, x_k(a^{(p-3)/2}; p)) \in \mathbb{C}^{(p-1)/2}$  et  $\mathbf{y}$  le vecteur colonne défini par  ${}^t\mathbf{y} = (f(1), f(a), \dots, f(a^{(p-3)/2})) \in \mathbb{C}^{(p-1)/2}$ . Déduire de la question précédente que

$$A_{(p-1)/2}(\mathbf{x}) \cdot \mathbf{y} = 0 \in \mathbb{C}^{(p-1)/2}.$$

23. Le but de cette question est de montrer que pour tout  $m \geq 1$  et  $\mathbf{v} \in \mathbb{C}^m$  on a

$$\det(A_m(\mathbf{v})) = \left( \cos\left(\frac{1}{2}\pi m\right) + \sin\left(\frac{1}{2}\pi m\right) \prod_{\substack{\ell=0 \\ \ell \text{ impair}}}^{2m} \left( \sum_{j=0}^{m-1} v_j \xi_{2m}^{j\ell} \right) \right).$$

(a) Commencer par vérifier cette formule lorsque  $\mathbf{v} = \mathbf{e}_1$ , où  $\mathbf{e}_1 = (1, 0, \dots, 0)$ .

(b) Soit  $(\mathbf{e}_j)_{j=0}^{m-1}$  la base canonique de  $\mathbb{C}^m$ . Montrer que  $A_m(\mathbf{v})A_m(\mathbf{e}_1) = C_m(\mathbf{v})$  avec

$$C_m(\mathbf{v}) = \begin{pmatrix} v_0 & -v_{m-1} & \dots & -v_2 & -v_1 \\ v_1 & v_0 & \dots & -v_3 & -v_2 \\ \vdots & \vdots & & \vdots & \vdots \\ v_{m-1} & v_{m-2} & v_1 & \dots & v_0 \end{pmatrix}.$$

(c) Montrer que les vecteurs

$$c_\ell = ({}^t(\xi_{2m}^{m\ell}, \xi_{2m}^{(m-1)\ell}, \dots, \xi_{2m}^\ell))$$

avec  $\ell$  impair et  $1 \leq \ell \leq 2m$  sont des vecteurs propres de  $C_m(\mathbf{v})$  dont on calculera les valeurs propres.

(d) En déduire le résultat concernant la valeur de  $\det(A_m(\mathbf{v}))$ .

24. (a) D  duire de la question pr  c  dente que pour

$$\mathbf{x} = (x_k(1; p), x_k(a; p), \dots, x_k(a^{(p-3)/2}; p))$$

on a

$$\det(A_{(p-1)/2}(\mathbf{x})) = (\cos(\frac{1}{4}\pi(p-1)) + \sin(\frac{1}{4}\pi(p-1))) \frac{2^{(k-1)(p-1)/2}}{\pi^{k(p-1)/2}} \prod_{\substack{\ell=0 \\ \ell \text{ impair}}}^{p-1} L(1, \chi_*^\ell)^k,$$

o    $\chi_*$  est un g  n  rateur du groupe des caract  res modulo  $p$ .

- (b) Soit  $V = \mathcal{F}_p^-(\mathbb{Z}, \mathbb{Q})$ . D  duire de a) que, si  $L(1, \chi) \neq 0$  pour tout caract  re  $\chi$  impair modulo  $p$ , alors la dimension du  $\mathbb{Q}$ -sous-espace vectoriel

$$\{f \in V : D_k(1, f) = 0\}$$

vaut 0.

25. Soient  $p \equiv 3 \pmod{4}$  et  $\chi$  un caract  re r  el impair modulo  $p$ . Montrer    partir du r  sultat de la question III-14c que l'on a  $L(1, \chi) \neq 0$ .

\* \* \*

Fin du sujet