D.M. 14 : solutions

1. Racines primitives de l'unité

1.1. Autour de la définition :

a) En suivant les définitions :
- Pour $n = 2$: $\mathbb{U}_2 = \{-1, 1\}$ et $\mathbb{P}_2 = \{-1\}$
- Pour $n = 3$, $\mathbb{U}_3 = \{1, j, j^2\}$ et $\mathbb{P}_3 = \{j, j^2\}$,
- Pour $n = 4$, $\mathbb{U}_4 = \{1, i, -1, -i\}$ et $\mathbb{P}_4 = \{i, -i\}$.
- Pour $n = 5$, $\mathbb{U}_5 = \{e^{2ik\pi/5},\ k \in [\![0, 4]\!]\}$ et $\mathbb{P}_5 = \{e^{2ik\pi/5},\ k \in [\![1, 4]\!]\}$.
- Pour $n = 6$, en notant $\eta = \omega_1 = e^{i\pi/3}$, on a $\mathbb{U}_6 = \{1, \eta, j, -1, \overline{j}, \overline{\eta}\}$ et $\mathbb{P}_6 = \{\eta, \overline{\eta}\}$.

b) On sait que, comme pour tout groupe cyclique, $G =< \omega_1 >$; $\Phi : (\mathbb{Z}/n\mathbb{Z}, +) \to (\mathbb{U}_n, \times)$, $\overline{k} \mapsto \omega_1^k$ est un *isomorphisme de groupes.*

Ici on note $\omega_k := \omega_1^k$.

Via l'isomorphisme Φ, ω_k est générateur du groupe ssi $\overline{k}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$.

c) D'après le cours $\overline{k}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ ssi $k \wedge n = 1$.

(On peut le redémontrer pour être sûr d'avoir tout les points : $\overline{k}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$ ssi il existe un p tel que $p.\overline{k} = \overline{1}$ ce qui équivaut à une relation de Bézout $pk + nu = 1$ dans $\mathbb{Z}$)

1.2. Ordre et fonction φ

a) Par déf. l'ordre de $\omega_k = \omega_1^k$ est le plus petit d tel que dk soit divisible par n donc est tel que dk soit le ppcm de n et de k.

Donc $dk = ppcm(n, k)$ et $d = ppcm(n, k)/k = pgcd(n, k)/n$ ce qui donne aussi l'égalité de l'énoncé $n/d = n \wedge k$.

b) Première inclusion ; : pour chaque $d|n$,$\mathbb{P}_d \subset \mathbb{U}_d \subset \mathbb{U}_n$ et trivialement si $d \neq d'$, $\mathbb{P}_d \cap \mathbb{P}'_d = \emptyset$ puisque dire que $\omega \in \mathbb{P}_d$ dit que $< \omega >= \mathbb{U}_d$ et que $\mathbb{U}_d = \mathbb{U}'_d$ ssi $d = d'$.

Ceci montre que $\coprod_{d|n} \mathbb{P}_d \subset \mathbb{U}_n$.

Inclusion inverse : soit $\omega \in \mathbb{U}_n$, on note d son ordre, c'est-à-dire que le plus petit entier strictement positif d tel que $\omega^d = 1$, on sait alors $< \omega >$ admet d éléments distincts, donc c'est $\mathbb{U}_d$ entier donc $\omega \in \mathbb{P}_d$ On sait aussi que $d|n$ par le cours

Ainsi $\omega \in \coprod_{d|n} \mathbb{P}_d$ ce qui donne l'inclusion réciproque $\mathbb{U}_n \subset \coprod_{d|n} \mathbb{P}_d$.

c) Par propriété du cardinal pour une union disjointe $\mathrm{Card}(\coprod_{d|n} \mathbb{P}_d) = \sum_{d|n} \mathrm{Card}(\mathbb{P}_d) \quad (1)$.

D'autre part, pour chaque d, on sait que $\mathrm{Card}(\mathbb{P}_d) = \varphi(d)$ par le cours, on obtient que : $\mathrm{Card}(\mathbb{U}_n) = \sum_{d|n} \varphi(d)$. Finalement comme $\mathrm{Card}(\mathbb{U}_n) = n$, on conclut que :

$$n = \sum_{d|n} \varphi(d).$$

2 Polynômes cyclotomiques

2.1. Premiers exemples

a) $\Phi_2(X) = (X - (-1)) = (X + 1)$,

$\Phi_3(X) = (X - j)(X - j^2) = X^2 + X + 1$,

$\Phi_4(X) = (X - i)(X + i) = X^2 + 1$,

$\Phi_6(X) = (X - e^{i\pi/3})(X - e^{-i\pi/3}) = X^2 - X + 1$.

b) Si $p \in \mathbb{P}$ alors $\mathbb{P}_p = \mathbb{U}_p \setminus \{1\}$ donc $\Phi_p(X) = \dfrac{\prod_{\omega \in \mathbb{U}_p}(X-\omega)}{X-1} = \dfrac{X^p-1}{X-1}$.

Or d'après l'identité géométrique $\dfrac{X^p-1}{X-1} = \sum\limits_{k=0}^{p-1} X^k$.

Ainsi $\Phi_p(X) = \sum\limits_{k=0}^{p-1} X^k$.

c) D'après la définition de Φ_n, c'est un produit de facteurs de degré 1, et le nombre de facteurs est $\mathrm{Card}(\mathbb{P}_n)$ qui vaut $\varphi(n)$.
Donc $\deg(\Phi_n) = \varphi(n)$.

d) Soit $\omega \in \mathbb{U}_{2q}$, qu'on écrit $\omega = e^{\frac{2ik\pi}{2q}}$.
Alors, on sait que $\omega \in \mathbb{P}_{2q}$ ssi $k \wedge (2q) = 1$.
Or $-\omega = e^{\frac{2ik\pi}{2q}} e^{i\pi} = e^{\frac{i(2k+2q)\pi}{2q}} = e^{\frac{i(k+q)\pi}{q}}$.
Comme q est impair, pour k impair, on sait que $(k+q)$ est pair et donc de même $-\omega \in \mathbb{P}_q$ ssi $\dfrac{(k+q)}{2} \wedge q = 1$.
On veut donc montrer, pour k impair, l'équivalence $k \wedge (2q) = 1 \Leftrightarrow \dfrac{(k+q)}{2} \wedge q = 1$.
Bien sûr ; $k \wedge (2q) = 1$ équivaut à $k \wedge q = 1$ et k est impair.

2.2. Formule du produit et conséquence : coefficients entiers, valeur de $\Phi_n(1)$

a) Avec la formule du 1.2. b), on peut écrire $\Phi_n(X) = \prod_{d|n} \prod_{\omega \in \mathbb{P}_d}(X-\omega) = \prod_{d|n} \Phi_d(X)$.

b) Changeons les notations de l'énoncé (pour noter plutôt Q pour le quotient) et appelons plutôt f et g les deux polynômes dans $\mathbb{Z}[X]$.
L'algorithme de division euclidienne de f par g consiste à partir de $R_0 = f$ et $Q_0 = 0$, à fabriquer des suites de polynômes R_k et Q_k telle qu'à chaque étape : $Q_{k+1}(X) = Q_k(X) + \dfrac{MD(R_k(X))}{MD(g(X))}$ et $R_{k+1}(X) = R_k(X) - Q_k(X).g(X)$.
La notation MD désigne le monôme dominant. Si le monôme dominant $MD(g(X))$ est à coefficient un, tous ces polynômes sont à coefficients entiers.
A l'arrêt de l'algorithme (quand $\deg(R_k) < \deg(g)$, on a $R = R_k$ le reste et $Q = Q_k$ le quotient, tous les deux à coefficients entiers.

c) Notons $H(n)$ le prédicat : Φ_n est à coefficients entiers. Montrons par récurrence forte que $H(n)$ est vraie pour tout $n \in \mathbb{N}^*$.
- On sait que $H(1)$ est vraie puisque $\Phi_1(X) = X-1$.
- Supposons que pour un $n \geq 2$, on ait $\forall\ k \in [\![1, n-1]\!]$, $H(k)$. Montrons que $H(n)$ est vraie.

On sait que $X^n - 1 = \Phi_n(X) \prod\limits_{d|n, d\ \neq n} \Phi_d(X) \quad (*)$.
En notant $f(X) = X^n - 1$ et $g(X) = \prod_{d|n,d\ \neq n} \Phi_d(X)$, alors f et g sont deux polynômes à coefficients entiers (pour g c'est donné par l'hypothèse de récurrence) et le coefficient dominant de g est 1.
Donc par b), le quotient de la division euclidienne de f par g est à coefficients entiers et par $(*)$, ce quotient, c'est Φ_n, donc $H(n)$ est vraie et la récurrence est établie. □

d) Avec la même formule $\prod_{d|n} \Phi_d(X) = X^n - 1$, si dans le produit on isole le facteur $\Phi_1(X) = X - 1$, alors

$$\prod_{d|n, d\neq 1} \Phi_d(X) = \frac{X^n-1}{X-1}$$

Grâce à l'identité géométrique, on en déduit que

$$\prod_{d|n, d\ \neq 1} \Phi_d(X) = \sum_{k=0}^{n-1} X^k \quad (*)$$

$$\prod_{d|n,\ d\neq 1} \Phi_d(1) = n$$

> Avertissement : la question qui suit est un peu plus difficile et moins importante aussi !

e) D'après la formule du 2.1. b), on sait que si p est un nombre premier, alors pour tout $x \in \mathbb{C}$, $\Phi_p(x) = X^{p-1} + X^{p-2} + \cdots + X + 1$ donc $\Phi_p(1) = p$.
On va utiliser le :
Lemme : Pour tout p premier et $r \in \mathbb{N}^*$, pour tout $x \in \mathbb{C}$, $\Phi_{p^r}(x) = \Phi_p(x^{p^r-1})$.
Démonstration du lemme (idée) L'essentiel est de comprendre que pour $\zeta \in \mathbb{C}$, on a $\zeta \in \mathbb{P}_{p^r} \Leftrightarrow \zeta^{p^r-1} \in \mathbb{P}_r$. On laisse cela en exercice. Il aurait été normal que ceci fasse l'objet d'une question en soi dans la partie 2.1.
Application du lemme : . pour tout p premier et $r > 0$, $\Phi_{p^r}(1) = \Phi_p(1) = p$.
Notons $n = \prod_{k=1}^s p_k^{r_k}$, avec $p_1, \ldots, p_s$ premiers deux à deux distincts, et $r_k > 0$ la décomposition en facteurs premiers de n.
Notons D l'ensemble des diviseurs de n, privé de 1. On décompose D en une union disjointe $D = D_1 \coprod D_2$ où D_1 est formé de tous les diviseurs de la forme $p_k^{s_k}$ avec $1 \leq s_k \leq r_k$ et D_2 est formé de tous les diviseurs composés d'au moins deux diviseurs premiers.
Précisément $D_1 = \{p_i^j,\ i \in [\![1, s]\!],\ j \in [\![1, r_i]\!]\}$.
Alors la formule finale du 2.2. d) s'écrit : $n = \left(\prod_{d \in D_1} \Phi_d(1)\right)\left(\prod_{d \in D_2} \Phi_d(1)\right) \quad (**)$.
Or $\prod_{d \in D_1} \Phi_d(1) = \prod_{i=1}^{s}\prod_{j=0}^{r_i} \Phi_{p_i^j}(1) = \prod_{i=1}^{s}\prod_{j=1}^{r_i} p_i = \prod_{i=1}^{s} p_i^{r_i} = n$
Donc la formule $(**)$ donne que : $\prod_{d \in D_2} \Phi_d(1) = 1 \quad (***)$.
Or tous les Φ_d sont des polynômes à coefficients entiers, donc tous les $\Phi_d(1)$ sont des entiers.
Donc $(***)$ donne que pour tout $d \in D_2$, $|\Phi_d(1)| = 1$.
En particulier pour $d = n$ (on rappelle que n a, par hypothèse, au moins deux diviseurs premiers), on a $|\Phi_n(1)| = 1$.
D'autre part, avec la même récurrence que celle faite au 2.2. c) on montre que pour tout $n \in \mathbb{N}_{\geq 1}$, Φ_n est positif sur $[1, +\infty[$.
Donc $\boxed{\Phi_n(1) = 1.}$

3 Notion de fonctions multiplicatives en arithmétique

3.1. Définitions

a) i) Si f est une fonction multiplicative, alors pour tout $m \in \mathbb{N}^*$ $f(m) = f(m.1) = f(m)f(1)$. Comme f n'est pas la fonction nulle, il existe au moins un m tel que $f(m) \neq 0$. Donc pour un tel m l'égalité $f(m) = f(m)f(1)$ entraîne $\boxed{f(1) = 1}$.

ii) Montrons que si $m_1, \ldots, m_s$ sont des entiers *deux à deux premiers entre eux* et si f est multiplicative alors $f(\prod_{i=1}^{s} m_i) = \prod_{i=1}^{s} f(m_i)$.
Par récurrence finie : pour $k \in [\![1, s]\!]$, on note $H(k)$ la propriété $f(\prod_{i=1}^k m_i) = \prod_{i=1}^k f(m_i)$.
• $H(1)$ est triviale.
• Hypothèse de réc on suppose que pour un $k \in [\![1, s-1]\!]$, $f(\prod_{i=1}^{k} m_i) = \prod_{i=1}^{k} f(m_i)$.
Comme m_{k+1} est premier avec $m_1, \ldots, m_k$ par un lemme du cours on sait que m_{k+1} est premier avec $\prod_{i=1}^{k} m_i$.

Comme f est multiplicative, on a donc : $f(m_1 \dots m_{k+1}) = f((\prod_{i=1}^{k} m_i)m_{k+1}) = f(\prod_{i=1}^{k} m_i)f(m_{k+1})$.

On applique alors l'hypothèse de récurrence et on obtient la prop. $H(k+1)$. La réc. est établie.

b) **Remarque culturelle :** on a vu en cours un autre exemple de fonction arithmétiquement multiplicative, la fonction φ. On a démontré cette propriété de multiplicativité avec le théorème Chinois.

Pour la fonction μ par contre c'est beaucoup plus facile puisqu'on a défini μ à l'aide de la D.F.P. : soient a et b deux entiers premiers entre eux.

• Si au moins l'un des deux est divisible par le carré d'un nombre premier p^2, alors le produit ab est divisible par p^2 et donc $\mu(ab) = 0$, et $\mu(a) = 0$ ou $\mu(b) = 0$ donc $\mu(ab) = \mu(a).\mu(b)$.

• Sinon $a = p_1 \dots p_r$ avec $p_1, \dots, p_r$ premiers deux à deux distincts, $b = q_1 \dots q_s$ avec $q_1, \dots, q_s$ premiers deux à deux distincts et distincts de tous les $p_1, \dots, p_r$ puisque $a \wedge b = 1$.

Alors $ab = p_1 \dots p_r q_1 \dots q_s$. Donc $\mu(ab) = (-1)^{r+s}$ et $\mu(a) = (-1)^r$ et $\mu(b) = (-1)^s$ d'où l'égalité $\mu(ab) = \mu(a).\mu(b)$.

3.2. Fonction « somme » d'une fonction multiplicative

a) Soient n_1 et n_2 deux nombres premiers entre eux. Tout diviseur d de n_1n_2 s'écrit de façon unique $d = d_1.d_2$ avec d_1 qui divise n_1 et d_2 qui divise n_2.

Mieux l'application : $\Delta(n_1) \times \Delta(n_2) \to \Delta(n_1n_2)$, $(d_1, d_2) \mapsto d_1.d_2$ est *bijective.*

Alors :

$$F(n_1n_2) = \sum_{d|n_1n_2} f(d) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1.d_2) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2) = \sum_{d_1|n_1} f(d_1) \sum_{d_2|n_2} f(d_2) = F(n_1).F(n_2)$$

b) (i) et (ii) ensemble. On note donc $f = \varphi$ et $F : n \mapsto \sum_{d|n} \varphi(d)$.

Par le a), on sait que F est (arithmétiquement) multiplicative. Donc pour $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ (D.F.P.), on sait que $F(n) = F(p_1^{\alpha_1}) \dots F(p_r^{\alpha_r})$.

Donc pour montrer que $F = \mathrm{id}$, il suffit de montrer que pour $p \in \mathbb{P}$, et $\alpha \in \mathbb{N}$, $F(p^\alpha) = p^\alpha \quad (C)$.

Or $F(p^\alpha) = \sum_{k=0}^{\alpha} \varphi(p^k) = \varphi(1) + \sum_{k=1}^{\alpha} \varphi(p^k) = 1 + \sum_{k=1}^{\alpha} (p^k - p^{k-1})$

On a une somme télescopique, qui donne bien $F(p^\alpha) = p^\alpha$ et donc la conclusion (C) qui suffit à montrer que $F = \mathrm{id}$. □

c) (i) Par déf. de μ, $\mu(p^k) = 0$ si $k > 1$ et $\mu(p^k) = 1$ pour $k = 0$ et $\mu(p^k) = -1$ si $k = 1$. Donc si $r \geq 1$, $F(p^r) = \sum_{k=0}^{r} \mu(p^k) = 2$.

(ii) Donc si $n \geq 2$, n aura au moins un p^r avec $r \geq 1$ dans sa décomposition et $F(n) = F(p_1^{r_1}) \dots f(p_s^{r_s}) = 0$.

En revanche $F(1) = \mu(1) = 1$.

(iii) Avec la condition $\mu(1) = 1$ on peut interpréter la formule $\sum_{d|n} \mu(d) = 0$ comme une sorte relation de récurrence.

Si on a calculé tous les $\mu(k)$ pour $k \leq n$ on calcule $\mu(n+1) = -\sum_{d|n+1} \mu(k)$.

3.3.Le rôle clef de la fonction de Möbius pour l'inversion d'une somme

a)

b) La formule s'appelle *formule d'inversion de Möbius*

3.4. La convolution arithmétique

a) • **Commutativité :** l'application $\psi : D_n \to D_n$, $x \mapsto n/x$ est bijective, car $\psi \circ \psi = \mathrm{id}$.
En appliquant le changement d'indice induit par ψ, on a immédiatement la commutativité.
Une autre écriture, plus symétrique du produit de Dirichlet est de l'écrire : $(f * g)(n) = \sum_{(a,b)\in\mathbb{N}^2,\, ab=n} f(a)g(b)$.

• **Associativité :**
Soit $(f,g,h) \in E^3$. Pour tout $n \in \mathbb{N}^*$, on peut écrire $f * (g * h)(n) = \sum_{(a,b)\in\mathbb{N}^{*2}} f(a)(g*h)(b) = \sum_{ab=n} f(a) \sum_{cd=b} g(c)h(d) = \sum_{acd=n} f(a)g(c)h(d)$. Cette écriture est invariante par toute permution de f, g, h.

b) • **Neutre :** soit δ la fonction définie par $\delta(1) = 1$ et $\forall\, n \geq 2$, $\delta(n) = 0$.
On vérifie immédiatement que e est neutre pour $*$. (On rappelle que si le neutre existe, il est unique).

c) **Distributivité de $*$ par rapport à + :**
Par déf., avec des notations évidentes, $((f+g)*h)(n) = \sum_{d\in D_n} (f+g)(d)h(\frac{n}{d}) = \sum_{d\in D_n} f(d)h(\frac{n}{d}) + \sum_{d\in D_n} g(d)h(\frac{n}{d}) = f * h(n) + g * h(n)$. D'où la conclusion (la distributivité d'un côté suffit car $*$ est commutative).

d) Il s'agit de montrer que $\mu * 1 = \delta$.
Autrement dit que : $\mu(1) = 1$ et que pour tout $n \geq 2$, $\sum_{d|n} \mu(d) = 0$.
Or c'est exactement le résultat de la question 3.2. c) (ii).

e) *Idée : A partir de $F = f * 1$, on peut utiliser l'inverse de 1 qui est μ pour « inverser »cette équation !*
Précisément en appliquant $*\mu$ aux deux membres de $F = f * 1$, on obtient :
$F * \mu = f * 1 * \mu = f * \delta = f$.
Cette relation $f = F * \mu$ est exactement la relation du 3.3.b)

f) La formule $n = \sum_{d|n} \varphi(d)$ dit que $\mathrm{id} = \varphi * 1$
En appliquant $*\mu$ aux deux membres on obtient $\mathrm{id} * \mu = \varphi$ i.e. pour tout $n \in \mathbb{N}$, $\varphi(n) = \sum_{d|n} d\mu(n/d)$.