L'EVARISTE

Sujet matin

Durée : 2 heures

Les téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont proscrits.

Les calculatrices sans mémoire type collège ou les calculatrices en mode examen sont autorisées.

La qualité de la rédaction est un facteur important d'appréciation des copies. L'humilité est la bienvenue à travers les raisonnements. Traitez les questions dans l'ordre que vous souhaitez.

Notations

Les notations suivantes seront utilisées dans l'énoncé. Vous êtes libres de les utiliser ou non.

On notera $\varnothing$ l'ensemble vide, $\mathbb{N}^*$ l'ensemble des entiers naturels non-nuls, et $[\![1, n]\!]$ l'ensemble fini des entiers allant de 1 à n. Si E est un ensemble, on note $\mathrm{Card}(E)$ le nombre d'éléments qu'il contient.

Dans la suite on pose, pour tout entier n, l'ensemble $\mathscr{D}_n$ des diviseurs positifs de n. On dira alors que d divise n si $d \in \mathscr{D}_n$, et on pourra noter $d|n$ la relation correspondante.

On rappelle également que les sommes sont notées $\sum$ et les produits sont notés $\prod$. Aucune sanction ne sera prononcée si les sommes ou produits sont écrits "naïvement" dans votre copie. A titre d'exemple :

$$\sum_{k=3}^{n-1} \frac{1}{k^2} = \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{(n-1)^2} \quad ; \quad \prod_{k|27} k = 1 \times 3 \times 9 \times 27$$

I - Tomber de Möbius en Euler

Le but de cette partie est de démontrer la célèbre formule d'inversion de Möbius.

On considère μ la fonction de Möbius définie pour tout $n \in \mathbb{N}^*$ par :

$$\mu(n) = \begin{cases} 1 & \text{si n=1} \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

Soient f, g deux fonctions de $\mathbb{N}^*$ dans $\mathbb{C}^*$. La formule d'inversion de Möbius assure que :

$$\forall n \in \mathbb{N}^*,\ f(n) = \sum_{d|n} g(d) \implies \forall n \in \mathbb{N}^*,\ g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) \qquad (\star)$$

1. Donner les valeurs de $\mu(20)$, $\mu(42)$ et $\mu(69)$.

• $20 = 2 \times 2 \times 5$, en particulier 20 possède deux facteurs premiers **non distincts**. Ainsi $\mu(20) = 0$.
• $42 = 2 \times 3 \times 7$, en particulier 42 possède trois facteurs premiers distincts. Ainsi $\mu(42) = (-1)^3 = -1$.
• $69 = 3 \times 23$, en particulier 69 possède deux facteurs premiers distincts. Ainsi $\mu(69) = (-1)^2 = 1$.

2. Montrer que, pour tout $m, n \in \mathbb{N}^*$ tels que $\mathrm{pgcd}(m, n) = 1$, on a $\mu(mn) = \mu(m)\mu(n)$.

- Si $m = 1$ alors $\mu(m) = 1$, donc $\mu(mn) = \mu(n) = 1 \times \mu(n) = \mu(m)\mu(n)$.

- Si $n = 1$ on obtient la même chose par un raisonnement analogue.

Supposons alors $m, n \in \mathbb{N} \setminus \{0, 1\}$. Ils sont alors décomposables en produit de facteurs premiers, et puisque $\text{pgcd}(m, n) = 1$ ils ne possèdent **aucun** facteurs premiers communs.

- Si m ou n contiennent plusieurs fois un même facteur premier dans leur décomposition, alors $\mu(n) = 0$ ou $\mu(m) = 0$. Auquel cas : $\mu(m)\mu(n) = 0$.

Et d'autre part mn contiendra par construction plusieurs fois un même facteur premier. Ainsi $\mu(mn) = 0$.

Il en découle que $\mu(mn) = \mu(m)\mu(n)$.

- Supposons finalement que chacun des facteurs premiers des décompositions de m et n soient distincts. Si m possède r facteurs premiers et n possède s facteurs premiers, alors puisqu'ils sont tous distincts :

$$\mu(m)\mu(n) = (-1)^r(-1)^s = (-1)^{r+s} = \mu(mn)$$

On a bien montré que, pour tout $m, n \in \mathbb{N}^*$ tels que $\text{pgcd}(m, n) = 1$, on a l'égalité $\mu(mn) = \mu(m)\mu(n)$.

Dans la suite on pose, pour tout entier n, l'ensemble $\mathscr{D}_n$ des diviseurs de n. On dira alors que d divise n si $d \in \mathscr{D}_n$, et on pourra noter $d|n$ la relation correspondante.

3.a. Décrivez l'ensemble $\mathscr{D}_{24}$.

On a $\mathscr{D}_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$.

b. Soient $d, d' \in \mathscr{D}_n$. Justifier l'équivalence suivante :

$$d'|d \iff \frac{n}{d}|\frac{n}{d'}$$

.

On a la chaîne d'équivalence :

$$d'|d \;\Leftrightarrow\; d'n|dn \;\Leftrightarrow\; \frac{d'n}{d'd}|\frac{dn}{d'd} \;\Leftrightarrow\; \frac{n}{d}|\frac{n}{d'}$$

4.a. Supposons que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ (décomposition en facteurs premiers de n) et $m = \prod_{i=1}^{r} p_i$. Justifier que :

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d)$$

Soit $d \in \mathscr{D}_n \setminus \mathscr{D}_m$. Alors d possède nécessairement un facteur carré dans sa décomposition en facteurs premiers. Irrémédiablement $\mu(d) = 0$, et ainsi :

$$\sum_{d\in\mathscr{D}_n} \mu(d) = \sum_{d\in\mathscr{D}_m} \mu(d) + \sum_{d\in\mathscr{D}_n\setminus\mathscr{D}_m} \mu(d) = \sum_{d\in\mathscr{D}_m} \mu(d)$$

b. Justifier par un argument combinatoire que :

$$\sum_{d|m} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i$$

Soit $d \in \mathscr{D}_m$. En particulier $d|\prod_{i=1}^{r} p_i$.

Autrement dit d est composé d'un certain nombre de facteurs premiers p_i, avec $i \in [\![1, r]\!]$.

Il existe $\binom{r}{i}$ tels diviseurs (on choisit i facteurs premiers parmi les r facteurs premiers de m). Ainsi :

$$\sum_{d\in\mathscr{D}_m} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i$$

c. En déduire que, pour tout $n \geqslant 2$:

$$\sum_{d|n} \mu(d) = 0$$

Soit $n \geqslant 2$. Alors n est décomposable en produit de facteurs premiers. Supposons que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ et posons $m = \prod_{i=1}^{r} p_i$. Alors en vertu de ce qui précède et en utilisant le binôme de Newton :

$$\sum_{d \in \mathscr{D}_n} \mu(d) = \sum_{d \in \mathscr{D}_m} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^n = 0$$

5. Prouvez ainsi la formule d'inversion de Möbius, notée $(\star)$.

Supposons que $f(n) = \sum_{d|n} g(d)$. Alors :

$$\sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d'|d} g(d') = \sum_{d'|d|n} \mu\left(\frac{n}{d}\right) g(d')$$

Il faut maintenant penser à l'habile changement d'indice $k = \dfrac{n}{d}$ et utiliser **3.b.**. Effectivement :

$$k|\frac{n}{d'} \iff d'|\frac{n}{k}|n$$

Ainsi :

$$\sum_{d'|d|n} \mu\left(\frac{n}{d}\right) g(d') = \sum_{d'|n} g(d') \sum_{k|\frac{n}{d'}} \mu(k)$$

Mais en vertu de **4.c.**, pour tout $d' \neq n$, on a :

$$\sum_{k|\frac{n}{d'}} \mu(k) = 0$$

Pour $d' = n$ la somme vaut trivialement 1. En rassemblant les morceaux, on obtient finalement :

$$\sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) = \sum_{d'|n} g(d') \sum_{k|\frac{n}{d'}} \mu(k) = g(n)$$

6. En déduire que :

$$\forall n \in \mathbb{N}^*,\ f(n) = \prod_{d|n} g(d) \implies \forall n \in \mathbb{N}^*,\ g(n) = \prod_{d|n} f(d)^{\mu\left(\frac{n}{d}\right)} \qquad (\star\star)$$

Il suffit d'appliquer la relation $(\star)$ que l'on vient de démontrer en $\ln(f)$ et en $\ln(g)$ en se rappelant que le logarithme d'un produit est la somme des logarithmes et que, par stricte croissance de ln :

$$\forall m, n \in \mathbb{N}^*, \ln(f(m)) = \ln(f(n)) \iff f(m) = f(n)$$

Effectivement :

$$f(n) = \prod_{d|n} g(d) \implies \ln(f(n)) = \ln\left(\prod_{d|n} g(d)\right) = \sum_{d|n} \ln(g(d))$$

$$\implies \ln(g(n)) = \sum_{d|n} \ln(f(d))\mu\left(\frac{n}{d}\right) = \sum_{d|n} \ln\left(f(d)^{\mu\left(\frac{n}{d}\right)}\right) = \ln\left(\prod_{d|n} f(d)^{\mu\left(\frac{n}{d}\right)}\right)$$

$$\implies g(n) = \prod_{d|n} f(d)^{\mu\left(\frac{n}{d}\right)}$$

Note : Les formules $(\star)$ et $(\star\star)$ sont en fait complètement équivalentes !

On considère désormais φ l'indicatrice d'Euler définie pour tout $n \in \mathbb{N}^*$ par :

$$\varphi(n) = \text{Card}\,\{k \in [\![1, n]\!] \mid \text{pgcd}(k, n) = 1\}$$

Autrement dit, $\varphi(n)$ est le nombre d'entiers naturels premiers avec n qui sont strictement inférieurs à n.

7. Donner les valeurs de $\varphi(10)$ et $\varphi(23)$.

- Les seuls nombres premiers avec 10 sont $1, 3, 7$ et 9, donc $\varphi(10) = 4$.
- 23 étant premier, tous les nombres inférieurs à lui sont premiers avec lui, d'où $\varphi(23) = 22$.

8. Justifier que p est premier si et seulement si $\varphi(p) = p - 1$.

Si p est premier, alors tout nombre inférieur à lui est premier avec lui, et on a bien $\varphi(p) = p - 1$.

Réciproquement si $\varphi(p) = p - 1$ alors $p \neq 1$ (car $\varphi(1) = 1$). Donc $p \geqslant 2$, et pour tout $i \in [\![1, p-1]\!]$ on a p premier avec i. Autrement dit p n'admet pas de diviseurs en dehors de 1 et lui-même ! Donc p est premier.

9.a. Soit p premier, et $\alpha, k \in \mathbb{N}^*$. Montrer que $\text{pgcd}(p^\alpha, k) \neq 1$ si et seulement si p divise k.

Si p^α et k ne sont pas premiers entre eux alors il existe $d \in \mathbb{N} \setminus \{0, 1\}$ tel que $d|k$ et $d|p^\alpha$. Or les seuls diviseurs de p^α sont de la forme p^i, avec $i \in [\![0, \alpha]\!]$. Donc $d = p^\beta$, avec $1 \leqslant \beta \leqslant \alpha$. Donc p divise k.

Réciproquement si p divise k alors k et p^α ne sont clairement pas premiers entre eux puisque p divise les deux. Donc $\text{pgcd}(p^\alpha, k) \neq 1$.

b. En déduire par un argument combinatoire que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

De par ce qui précède on a que les seuls nombres non-premiers avec p^α sont ceux qui sont divisibles par p, donc qui sont des multiples de p. Il suffit alors de dénombrer le nombre de multiples de p compris entre 1 et $p^\alpha - 1$.

On a que $k \in [\![1, p^\alpha - 1]\!]$ est un multiple de p si et seulement si $k = k'p$, avec $k' \in [\![1, p^{\alpha-1}]\!]$. Donc il y a $p^{\alpha-1}$ multiples de p compris entre 1 et $p^\alpha - 1$.

Il suit alors que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Nous admettons par la suite que : pour tout $m, n \in \mathbb{N}^*$ tels que $\text{pgcd}(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

10.a. Montrer que si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$

Il s'agit d'une conséquence directe de **9.b** et de la multiplicativité de φ ! Effectivement :

$$\varphi(n) = \varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$$

b. En déduire la valeur de $\varphi(2024)$.

On applique la formule précédente avec $2024 = 2^3 \times 11 \times 23$:

$$\varphi(2024) = 2^{3-1}(2-1) \times (11-1) \times (23-1) = 4 \times 10 \times 22 = 880$$

c. Déduire de ce qui précède que si $n \geqslant 3$ alors $\varphi(n)$ est pair.

Soit $n \geqslant 3$. Si n admet un facteur impair p_i dans sa décomposition en facteurs premiers alors $\varphi(n)$ sera pair en vertu de la formule montrée en **10.a.** (car $\varphi(n)$ sera un multiple de $(p_i - 1)$ qui est pair).

Dans le cas contraire si $\varphi(n)$ n'admet aucun facteur impair dans sa décomposition en facteurs premiers alors n s'écrit 2^α avec $\alpha \in \mathbb{N} \setminus \{0, 1\}$. Et ainsi $\varphi(n) = \varphi(2^\alpha) = 2^{\alpha-1}$ qui est clairement pair.

Dans tous les cas $\varphi(n)$ est pair.

II - Des polynômes coupant le cercle

Le but de cette partie est de s'intéresser aux polynômes cyclotomiques. A travers les propriétés de ces polynômes nous prouverons une version faible du théorème de progression arithmétique de Dirichlet.

Rappelons ici que i désigne l'unité imaginaire dont le carré vaut -1, et que $e^{i\pi} = -1$. On rappelle également que $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}} \mid 1 \leqslant k \leqslant n \right\}$ est l'ensemble des racines n-ièmes de l'unité, i.e l'ensemble des solutions de l'équation complexe $x^n = 1$.

Il sera également utile de se rappeler que l'exponentielle complexe vérifie la propriété d'additivité :

$$\forall \theta, \theta' \in \mathbb{R},\ e^{i\theta} \times e^{i\theta'} = e^{i(\theta+\theta')}$$

Soit $n \in \mathbb{N}^*$. On pose, pour tout $x \in \mathbb{C}$:

$$\Phi_n(x) = \prod_{\substack{k=1 \\ \text{pgcd}(k,n)=1}}^{n} (x - e^{\frac{2ik\pi}{n}})$$

Et on appelle Φ_n le n-ième polynôme cyclotomique. On a par exemple :

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$

1. Que vaut $\Phi_4(x)$?

Les seuls nombres premiers avec 4 sont 1 et 3. On en déduit :

$$\Phi_4(x) = \prod_{\substack{k=1 \\ \text{pgcd}(k,4)=1}}^{4} (x - e^{\frac{2ik\pi}{4}}) = (x - e^{\frac{i\pi}{2}})(x - e^{\frac{3i\pi}{2}}) = (x-i)(x+i) = x^2 + 1$$

2. Donner le degré de Φ_n pour tout $n \in \mathbb{N}^*$.

On a exactement $\deg(\Phi_n) = \varphi(n)$ par définition.

b En déduire que, pour tout $n \geqslant 3$, Φ_n' (la dérivée de Φ_n restreint sur $\mathbb{R}$) admet au moins une racine réelle.

On a Φ_n qui est un polynôme de degré pair, donc Φ_n' est de degré impair, en particulier les limites asymptotiques de Φ_n' sont $-\infty$ et $+\infty$, et Φ_n' étant une fonction polynomiale elle est par conséquent continue, et le théorème des valeurs intermédiaires assure alors qu'il existe un réel c tel que $\Phi_n'(c) = 0$.

Soit $n \in \mathbb{N}^*$ et soit d un diviseur de n. On pose $F_d = \{k \in [\![1, n]\!] \mid \text{pgcd}(k, n) = d\}$.

3.a. Montrer que $[\![1, n]\!] = \bigcup_{d|n} F_d$ et que, pour tout d, d' diviseurs de n tels que $d \neq d'$, on a $F_d \cap F_{d'} = \varnothing$.

Pour tout d diviseur de n on a clairement $F_d \subset [\![1, n]\!]$. Donc $\bigcup_{d|n} F_d \subset [\![1, n]\!]$.

Réciproquement si $k \in [\![1, n]\!]$ alors posons $d_0 = \text{pgcd}(k, n)$. On a clairement $k \in F_{d_0}$, donc $k \in \bigcup_{d|n} F_d$, et on a bien $[\![1, n]\!] \subset \bigcup_{d|n} F_d$. Par double inclusion, on déduit que $[\![1, n]\!] = \bigcup_{d|n} F_d$.

De plus, si on considère d, d' deux diviseurs de n tels que $d \neq d'$ et qu'on suppose par l'absurde que $F_d \cap F_{d'} \neq \varnothing$, alors il existe au moins un élément $k \in F_d \cap F_{d'}$. Autrement dit : $\text{pgcd}(k, n) = d$ et $\text{pgcd}(k, n) = d'$, c'est absurde car $d \neq d'$ par hypothèse.

b. Justifier que, pour tout $x \in \mathbb{C}$:

$$x^n - 1 = \prod_{k=1}^{n} (x - e^{\frac{2ik\pi}{n}})$$

Soit $x \in \mathbb{C}$. On a $x^n - 1 = 0$ si et seulement si $x^n = 1$, autrement dit les racines du polynômes $x^n - 1$ sont exactement les racines de l'unité, et ainsi, en le factorisant sur $\mathbb{C}$:

$$x^n - 1 = \prod_{k=1}^{n} (x - e^{\frac{2ik\pi}{n}})$$

c. Soit $x \in \mathbb{C}$. Pourquoi a-t-on :

$$\prod_{d|n} \Phi_d(x) = \prod_{d|n} \Phi_{\frac{n}{d}}(x)$$

Soit $n \in \mathbb{N}^*$. On considère l'application f suivante :

$$\begin{array}{rccc} f & : & \mathscr{D}_n & \to & \mathscr{D}_n \\ & & d & \mapsto & \dfrac{n}{d} \end{array}$$

C'est une bijection car trivialement injective et les ensembles de départ et d'arrivée sont finis et de même cardinal. Ainsi l'égalité souhaitée en découle.

Le second produit correspond d'ailleurs au premier produit dont l'ordre des facteurs est totalement inversé, s'en convaincre avec le cas $n = 6$:

$$\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x) = \Phi_{\frac{6}{1}}(x)\Phi_{\frac{6}{2}}(x)\Phi_{\frac{6}{3}}(x)\Phi_{\frac{6}{6}}(x)$$

d. Montrer alors que, pour tout $x \in \mathbb{C}$:

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \qquad (\#)$$

Soit $x \in \mathbb{C}$. D'une part, on a :

$$x^n - 1 = \prod_{k=1}^{n} (x - e^{\frac{2ik\pi}{n}}) = \prod_{d|n} \prod_{\substack{k=1 \\ \text{pgcd}(k,n)=d}}^{n} (x - e^{\frac{2ik\pi}{n}}) = \prod_{d|n} \prod_{\substack{k=1 \\ \text{pgcd}(\frac{k}{d}, \frac{n}{d})=1}}^{n} (x - e^{\frac{2ik\pi}{n}})$$

D'autre part, par définition des polynômes cyclotomiques :

$$\prod_{d|n}\Phi_d(x)=\prod_{d|n}\Phi_{\frac{n}{d}}(x)=\prod_{d|n}\prod_{\substack{k=1\\ \text{pgcd}(k,\frac{n}{d})=1}}^{\frac{n}{d}}(x-e^{\frac{2ik\pi}{\frac{n}{d}}})=\prod_{d|n}\prod_{\substack{k=1\\ \text{pgcd}(k,\frac{n}{d})=1}}^{\frac{n}{d}}(x-e^{\frac{2ikd\pi}{n}})$$

Et en procédant au changement d'indice $k'=\dfrac{k}{d}\in\mathbb{N}^*$ on obtient l'égalité désirée. Effectivement :

$$1\leqslant k\leqslant n\iff\frac{1}{d}\leqslant k'\leqslant\frac{n}{d}\iff 1\leqslant k'\leqslant\frac{n}{d}$$

e. En déduire que, pour tout $n\in\mathbb{N}^*$, on a :

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

Il suffit de remarquer que :

$$n=\deg(x^n-1)=\deg\left(\prod_{d|n}\Phi_d(x)\right)=\sum_{d|n}\deg(\Phi_d(x))=\sum_{d|n}\varphi(d)$$

4. Déduire alors par $(\star\star)$ et $(\#)$ que, pour tout $x\in\mathbb{C}$, pour tout $n\in\mathbb{N}^*$:

$$\Phi_n(x)=\prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}$$

On applique $(\#)$ puis $(\star\star)$ avec $f:n\longmapsto x^n-1$ et $g:n\longmapsto\Phi_n(x)$ et le résultat arrive naturellement.

5. Donner alors une expression de $\Phi_8(x)$ et de $\Phi_{23}(x)$.

On a :

$$\begin{aligned}\Phi_8(x)&=(x-1)^{\mu(8)}(x^2-1)^{\mu(4)}(x^4-1)^{\mu(2)}(x^8-1)^{\mu(1)}\\&=(x-1)^0(x^2-1)^0(x^4-1)^{-1}(x^8-1)^1\\&=\frac{x^8-1}{x^4-1}\\&=\frac{(x^4+1)(x^4-1)}{x^4-1}\\&=x^4-1\end{aligned}$$

De même :

$$\begin{aligned}\Phi_{23}(x)&=(x-1)^{\mu(23)}(x^{23}-1)^{\mu(1)}\\&=(x-1)^{-1}(x^{23}-1)^1\\&=\frac{x^{23}-1}{x-1}\\&=\frac{(x-1)\left(\sum_{k=0}^{22}x^k\right)}{x-1}\\&=\sum_{k=0}^{22}x^k\end{aligned}$$

6. Plus généralement donner une expression de $\Phi_p(x)$ lorsque p est premier.

Plus généralement si p est premier on a :

$$\begin{aligned}\Phi_p(x) &= (x-1)^{\mu(p)}(x^p-1)^{\mu(1)} \\ &= (x-1)^{-1}(x^p-1)^1 \\ &= \frac{x^p-1}{x-1} \\ &= \frac{(x-1)\left(\sum_{k=0}^{p-1} x^k\right)}{x-1} \\ &= \sum_{k=0}^{p-1} x^k\end{aligned}$$

On va désormais prouver que Φ_n est un polynôme à coefficients entiers pour tout $n \in \mathbb{N}^*$.

7.a. Pourquoi le résultat est-il trivialement vrai pour $n = 1$?

On a $\Phi_1(x) = x - 1$ qui est évidemment à coefficients entiers.

b. En supposant le résultat vrai pour tout $k \in [\![1, n-1]\!]$, montrer que le résultat est alors vrai pour n.

Supposons que Φ_k est à coefficients entiers pour tout $k \in [\![1, n-1]\!]$. Montrons qu'alors Φ_n est à coefficients entiers. On a :

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$$

Par hypothèse de récurrence on a que $\prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ est à coefficients entiers, et $x^n - 1$ également.

Or, par un principe de récurrence descendante, si $x^n - 1 = P(x)Q(x)$ avec $Q(x)$ un polynôme à coefficient entier alors on peut montrer que $P(x)$ est nécessairement à coefficients entiers. On en déduit alors que Φ_n est un polynôme à coefficients entiers.

Démontrons proprement que si $x^n - 1 = P(x)Q(x)$ avec $Q(x)$ un polynôme à coefficient entier alors $P(x)$ est nécessairement à coefficients entiers.

Posons $P(x) = \sum_{i=0}^{r} a_i x^i$ et $Q(x) = \sum_{i=0}^{s} b_j x^j$. On a : $\forall j \in [\![0, s]\!]$, $b_j \in \mathbb{Z}$.

On procède par récurrence descendante forte. Puisque $a_r b_s = 1$, alors $a_r = b_s = \pm 1$ et il suit que $a_r \in \mathbb{Z}$. Soit alors $q \in [\![0, r-1]\!]$. Supposons désormais que $a_r, a_{r-1}, \ldots, a_{q+1} \in \mathbb{Z}$, et montrons qu'alors $a_q \in \mathbb{Z}$.

Le coefficient de x^{s+q} est $a_q b_s + a_{q+1} b_{s-1} + \cdots + a_r b_{(s+q)-r} = 0$. En particulier :

$$a_q = -\frac{a_{q+1} b_{s-1} + \cdots + a_r b_{(s+q)-r}}{b_s} \in \mathbb{Z}$$

Ainsi, par le principe de récurrence descendante forte : $\forall i \in [\![0, r]\!]$, $a_i \in \mathbb{Z}$.

c. Conclure par un principe de récurrence.

Le principe de récurrence forte assure que si un prédicat $\mathcal{P}_n$ est vrai au rang 1 et qu'il est fortement héréditaire (i.e : $\forall n \in \mathbb{N}$, $[\mathcal{P}_1 \wedge \cdots \wedge \mathcal{P}_{n-1}] \implies \mathcal{P}_n$), il est alors vrai pour tout $n \in \mathbb{N}^*$.

C'est exactement ce que nous avons vérifié à travers les deux questions précédentes. Donc Φ_n est à coefficients entiers pour tout $n \in \mathbb{N}^*$.

Soit $a, n \in \mathbb{N}^*$. On admet que si p premier divise $\Phi_n(a)$ alors $p \equiv 0\ [n]$ ou $p \equiv 1\ [n]$. Nous allons déduire de ce résultat qu'il existe une infinité de nombres premiers p tels que $p \equiv 1\ [n]$.

8. Pourquoi le résultat est-il évident si $n = 1$ ou si $n = 2$?

Pour $n = 1$ cela revient à dire qu'il existe une infinité de nombres premiers, ce qui est vrai en vertu du théorème dû à Euclide, et pour $n = 2$ cela revient à dire qu'il existe une infinité de nombres premiers impairs, ce qui est également vrai puisque 2 est le seul nombre premier pair.

Supposons par l'absurde qu'il en existe un nombre fini et notons les $p_1, \dots, p_r$. On pose $a = np_1 \dots p_r$.

9.a. Justifier que $\Phi_n(a) \in \mathbb{N}^*$.

On évalue un polynôme à coefficients entiers en un entier $a \geqslant 2$, $\Phi_n(a)$ est alors un entier en tant que somme et produit d'entiers, et il est non-nul car a n'est pas racine de Φ_n (étant donné que a n'est certainement pas une racine n-ième de l'unité).

b. Pourquoi a-t-on $\Phi_n(a) \equiv \Phi_n(0)\ [a]$?

Posons $\Phi_n(x) = \sum_{k=0}^{r} \alpha_i x^i$. Alors $\Phi_n(a) = \sum_{k=0}^{r} \alpha_i a^i$, et en particulier $\Phi_n(a) \equiv \alpha_0\ [a]$.

De plus, de par la définition ci-dessus : $\Phi_n(0) = \alpha_0$. On en déduit que $\Phi_n(a) \equiv \Phi_n(0)\ [a]$.

c. En déduire que $\Phi_n(a) \equiv \pm 1\ [a]$.

On a, en vertu de ce qui précède :

$$-1 = 0^n - 1 = \prod_{d|n} \Phi_d(0)$$

Nécessairement, puisque Φ_k est à coefficients entiers pour tout $k \in [\![1, n]\!]$, on a $\Phi_n(0) = \pm 1$, et on en déduit que $\Phi_n(a) \equiv \pm 1\ [a]$.

d. Montrer que $\Phi_n(a) \geqslant 2$ pour tout $n \geqslant 2$.

On a, par définition de Φ_n :

$$\Phi_n(a) = |\Phi_n(a)| = \prod_{\substack{k=1 \\ \text{pgcd}(k,n)=1}}^{n} |a - e^{\frac{2ik\pi}{n}}| > 1$$

La dernière inégalité découlant du fait que $a \geqslant n \geqslant 2$, la distance de a à n'importe quelle racine de l'unité est donc supérieure à 1 sur le plan complexe, donc $\Phi_n(a) \in \mathbb{N}^*$ est égal à un produit de distance strictement supérieures à 1. Ainsi $\Phi_n(a) \geqslant 2$.

e. Conclure.

Puisque $\Phi_n(a) \geqslant 2$, il est décomposable en produit de facteurs premiers. Considérons alors p un nombre premier divisant $\Phi_n(a)$, i.e $\Phi_n(a) \equiv 0\ [p]$.

Alors d'après le résultat admis on a que $p \equiv 0\ [n]$ ou $p \equiv 1\ [n]$. Ceci entraîne dans le premier cas que p divise n, donc p divise a, et ainsi $\Phi_n(a) \equiv \pm 1\ [p]$ (voir éventuellement **Clarification**). C'est absurde.

Dans le second cas on a qu'il existe $i \in [\![1, r]\!]$ tel que $p = p_i$. Donc p divise une fois encore a par construction et on aboutit à une absurdité semblable.

Dans les deux cas c'est absurde, et il existe alors une infinité de nombres premiers p tels que $p \equiv 1\ [n]$.

Clarification : Supposons que p divise a. Alors : $\Phi_n(a) \equiv \pm 1\ [a] \implies \Phi_n(a) \pm 1 \equiv 0\ [a]$
$\implies a | (\Phi_n(a) \pm 1)$

$$\begin{aligned}
&\implies p|(\Phi_n(a)\pm 1)\\
&\implies \Phi_n(a)\pm 1\equiv 0\ [p]\\
&\implies \Phi_n(a)\equiv \pm 1\ [p].
\end{aligned}$$

Questions subsidiaires pour départager les plus chevronnés :

1. Expliquer pourquoi a-t-on pour tout $m,n\in\mathbb{N}^*$ tels que $\text{pgcd}(m,n)=1$ l'égalité $\varphi(mn)=\varphi(m)\varphi(n)$.

Soient m,n deux entiers premiers entre eux. Puisque m et n sont deux entiers premiers entre eux, le théorème chinois assure alors que $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, en particulier cette isomorphie sur les groupes multiplicatifs correspondant couplée au théorème d'Euler donne une égalité des cardinaux tout à fait formidable :

$$\varphi(mn)=\text{Card}(\mathbb{Z}/mn\mathbb{Z}^\times)=\text{Card}(\mathbb{Z}/m\mathbb{Z}^\times)\times\text{Card}(\mathbb{Z}/n\mathbb{Z}^\times)=\varphi(m)\varphi(n)$$

2. Montrer que si n est pair alors $\Phi_{2n}(x)=\Phi_n(x^2)$.

3. Montrer que si n est impair alors $\Phi_{2n}(x)=\Phi_n(-x)$.

Ces deux égalités peuvent se montrer via un raisonnement par récurrence forte en travaillant avec l'égalité (#), ou même pourquoi pas via la formule suivante que l'on a démontré :

$$\Phi_n(x)=\prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}$$

A condition d'être suffisamment réveillé et concentré !

Voici une preuve éventuelle de la question **2.** :

$$\begin{aligned}
\Phi_{2n}(x) &= \prod_{d|2n}(x^d-1)^{\mu\left(\frac{2n}{d}\right)}\\
&= \prod_{\substack{d|2n\\ \text{pgcd}(d,2)=1}}(x^d-1)^{\mu\left(\frac{2n}{d}\right)}\prod_{\substack{d|2n\\ \text{pgcd}(d,2)\neq 1}}(x^d-1)^{\mu\left(\frac{2n}{d}\right)}\\
&= \prod_{\substack{d|2n\\ \text{pgcd}(d,2)\neq 1}}(x^d-1)^{\mu\left(\frac{2n}{d}\right)}\\
&= \prod_{d|n}(x^{2d}-1)^{\mu\left(\frac{n}{d}\right)}\\
&= \Phi_n(x^2)
\end{aligned}$$

La troisième égalité découlant du fait que n est pair, i.e il existe $k\in\mathbb{N}$ tel que $n=2k$, ce qui donne $\mu\left(\frac{2n}{d}\right)=\mu(4)\mu\left(\frac{k}{d}\right)=0$ pour tout diviseur impair d de n.

Un mot à propos des sponsors de l'Evariste

D.E. Shaw & Co : Founded in 1988 over a small bookstore in downtown New York City, the D. E. Shaw group began with six employees and 28 million in capital and quickly became a pioneer in computational finance. In the early days of exposed pipes and extension cords, tripping on a cable could take out our whole trading system.

Today, we have more than 2,000 people around the globe and an institutional-grade (and trip-proof) infrastructure, but we still value creativity, entrepreneurship, and the spirit of discovery. We prize our culture of collaboration across disciplines, geographies, and investment strategies. Experienced leadership and diversely talented minds chart our course.

Analytical rigor, an open exploration of ideas, and a relentless pursuit of excellence drive us forward. We are dedicated to ensuring all employees—across gender identity, ethnicity, sexual orientation, religion, life experience, and more—feel welcome and empowered to do their best work at the D.E. Shaw group.

Nous remercions chaleureusement nos sponsors sans qui nous n'aurions pas pu inviter tant d'équipes à participer à cette première édition de l'Evariste !