

Avant de commencer, quelques mots sur l'application χ . Sa périodicité permet de définir une application $\tilde{\chi}$ de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{R}$ par $\tilde{\chi}(\bar{k}) = \chi(k)$. Cette application $\tilde{\chi}$ est un morphisme pour les lois produits, nulle en dehors de $(\mathbb{Z}/N\mathbb{Z})^*$, ne s'annulant pas sur $\mathbb{Z}/N\mathbb{Z}$ (sinon χ serait nulle, ... preuve à détailler, un peu comme à la question 1). On en déduit que $\tilde{\chi}$ induit un morphisme du groupe multiplicatif $((\mathbb{Z}/N\mathbb{Z})^*, \times)$ sur le groupe multiplicatif $(\mathbb{R}^*, \times)$.

1. $\chi(1) = \chi(1 \times 1) = \chi(1)^2$; donc $\chi(1)$ vaut 0 ou 1. Comme $\forall k \in \mathbb{Z}, \chi(k) = \chi(1 \times k) = \chi(1) \cdot \chi(k)$ et que χ n'est pas identiquement nulle, $\chi(1) \neq 0$. Donc $\chi(1) = 1$.

2. Nécessairement, par périodicité, $\forall k \in \mathbb{Z}, \chi(k) = \begin{cases} 0 & \text{si } k \text{ est pair} \\ 1 & \text{si } k \text{ est impair} \end{cases}$

Inversement, cette application vérifie les 4 axiomes.

3. $\chi(3) = \chi(-1)$. De plus, $\chi(-1)^2 = \chi((-1) \times (-1)) = \chi(1) = 1$. Donc $\chi(3) = \chi(-1) \in \{1, -1\}$.

4. $\forall k \in \mathbb{Z}, \chi(k) = \begin{cases} 0 & \text{si } k \text{ est pair} \\ 1 & \text{si } k \equiv 1 \pmod{4} \\ -1 & \text{si } k \equiv 3 \pmod{4} \end{cases}$; donc $\chi(2k+1) = (-1)^k$.

$$\sum_{k=1}^n \frac{\chi(k)}{k} = \sum_{k=0}^{E((n-1)/2)} \frac{\chi(2k+1)}{2k+1} = \sum_{k=0}^{E((n-1)/2)} \frac{(-1)^k}{2k+1} \xrightarrow{n \rightarrow +\infty} \arctan 1 = \frac{\pi}{4} \text{ d'après les rappels.}$$

5. Je ne vois pas comment prouver le résultat demandé sans le résultat de la question 7. On peut prolonger la définition de r_k à $k = 0$. Si $r_k = r_l$, alors N divise $ak - al = a(k - l)$. Comme a est premier avec N , N divise $k - l$. Si $k, l \in \{0, 1, \dots, N-1\}$, alors $|k - l| \leq N-1$; donc $k - l = 0$.

Donc l'application $k \mapsto r_k$ est une injection de l'ensemble fini $\{0, 1, \dots, N-1\}$ dans lui-même, donc une bijection. Comme $r_0 = 0$, $k \mapsto r_k$ est une bijection de l'ensemble fini $\{1, \dots, N-1\}$ sur lui-même.

De plus, soit $k \in P$; si d divise r_k et N , il divise ak et est premier avec a ; donc il divise k (et N); donc d vaut ± 1 . Donc r_k est dans P .

On en déduit que $k \mapsto r_k$ est une injection, donc une bijection, de P dans lui-même.

La question 5 maintenant! Pour tout $k \in P$, $ak \equiv r_k \pmod{N}$; donc $\prod_{k \in P} ak \equiv \prod_{k \in P} r_k \pmod{N}$. Or $\prod_{k \in P} r_k = \prod_{k \in P} k$; donc

N divise $\prod_{k \in P} ak - \prod_{k \in P} k = (a^{\varphi(N)} - 1) \prod_{k \in P} k$. Comme N est premier avec chaque élément de P , il est premier avec leur produit, donc il divise $a^{\varphi(N)} - 1$.

Autre preuve en travaillant dans le groupe multiplicatif $(\mathbb{Z}/N\mathbb{Z})^* = \{\bar{k}, k \in P\}$:

Comme $\bar{a}$ est inversible dans $\mathbb{Z}/N\mathbb{Z}$, l'application $x \mapsto \bar{a}x$ est une bijection de $(\mathbb{Z}/N\mathbb{Z})^*$ (mais aussi de $\mathbb{Z}/N\mathbb{Z}$ et de $\mathbb{Z}/N\mathbb{Z} \setminus \{\bar{0}\}$). Donc $\prod_{k \in P} ak = \prod_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \bar{a}x = \prod_{x \in (\mathbb{Z}/N\mathbb{Z})^*} x$. Or $\prod_{k \in P} ak = \bar{a}^{\varphi(N)} \prod_{x \in (\mathbb{Z}/N\mathbb{Z})^*} x$. Comme $\prod_{x \in (\mathbb{Z}/N\mathbb{Z})^*} x$ est inversible, de l'égalité $\prod_{x \in (\mathbb{Z}/N\mathbb{Z})^*} x = \bar{a}^{\varphi(N)} \prod_{x \in (\mathbb{Z}/N\mathbb{Z})^*} x$, on tire $\bar{a}^{\varphi(N)} = \bar{1}$, i.e. N divise $a^{\varphi(N)} - 1$.

6. Par périodicité, $\chi(a^{\varphi(N)}) = \chi(1)$; par morphisme, $\chi(a^{\varphi(N)}) = \chi(a)^{\varphi(N)}$. Comme $\chi(a)$ est un réel, $\chi(a) = \pm 1$.
7. Voir la question 5.

8. Par périodicité, $\sum_{k=1}^{N-1} \chi(ak) = \sum_{k=1}^{N-1} \chi(r_k)$. Par bijectivité de $k \mapsto r_k$ sur $\{1, \dots, N-1\}$, $\sum_{k=1}^{N-1} \chi(r_k) = \sum_{k=1}^{N-1} \chi(k)$.

D'où l'identité demandée.

9. Comme $\chi(n) = \chi(n+N)$, $\sum_{k=n}^{n+N-1} \chi(k)$ ne dépend pas de n .

Pour $n = 0$: $\sum_{k=0}^{N-1} \chi(k) = \sum_{k=1}^{N-1} \chi(k) = \sum_{k=1}^{N-1} \chi(ak) = \chi(a) \sum_{k=1}^{N-1} \chi(k)$. En choisissant a tel que $\chi(a) \neq 1$, ce qui est possible d'après l'énoncé: $\sum_{k=1}^{N-1} \chi(k) = 0$ et $\sum_{k=0}^{N-1} \chi(k) = 0$ également.

10. On considère l'entier q tel que $qN \leq k < (q+1)N$.

$$\sum_{k=1}^m \chi(k) = \sum_{k=0}^m \chi(k) = \sum_{k=0}^{qN-1} \chi(k) + \sum_{k=qN}^m \chi(k) = \sum_{i=0}^{q-1} \sum_{k=iN}^{iN+N-1} \chi(k) + \sum_{k=qN}^m \chi(k) = \sum_{k=qN}^m \chi(k) = \sum_{k=qN}^{m-qN} \chi(k) = \sum_{k=0}^{m-qN} \chi(k)$$

Comme $\chi(k) \in \{-1, 0, 1\}$, que $m - qN \leq N - 1$, et qu'entre 1 et $N - 1$ il y a exactement $\varphi(N)$ valeurs de k telles que $\chi(k) \neq 0$, $\left| \sum_{k=1}^m \chi(k) \right| = \left| \sum_{k=1}^{m-qN} \chi(k) \right| \leq \varphi(N)$.

11. On pose $T_n = \sum_{k=0}^n \chi(k) = \sum_{k=1}^n \chi(k)$ et on utilise la transformation d'Abel avec $u_k = \frac{1}{k}$; pour $n \geq 2$, on a :

$$\sum_{k=2}^n \frac{\chi(k)}{k} = -\frac{T_1}{2} + \sum_{k=2}^{n-1} T_k \left(\frac{1}{k} - \frac{1}{k+1} \right) + \frac{T_n}{n}.$$

Comme (T_n) est une suite bornée, $\frac{T_n}{n} \xrightarrow{n \rightarrow +\infty} 0$.

Comme $\left| T_k \left(\frac{1}{k} - \frac{1}{k+1} \right) \right| \leq \varphi(N) \left(\frac{1}{k} - \frac{1}{k+1} \right)$, que $\varphi(N)$ est une constante et que la série $\sum \left(\frac{1}{k} - \frac{1}{k+1} \right)$ converge (car la suite $(1/k)$ converge), la série $\sum T_k \left(\frac{1}{k} - \frac{1}{k+1} \right)$ converge absolument, donc converge.

D'où la convergence de la suite $\left(\sum_{k=2}^n \frac{\chi(k)}{k} \right)$ et celle de $\left(\sum_{k=1}^n \frac{\chi(k)}{k} \right)$.

12. On se limite aux diviseurs dans N . Comme n et m sont premiers entre eux, tout diviseur de nm s'écrit de manière unique comme produit d'un diviseur de n et d'un diviseur de m et le produit d'un diviseur de n par un diviseur de m est un diviseur de nm . On peut donc écrire :

$$f_{nm} = \sum_{d|nm} \chi(d) = \sum_{u|n \text{ et } v|m} \chi(uv) = \sum_{u|n \text{ et } v|m} \chi(u)\chi(v) = \sum_{u|n} \sum_{v|m} \chi(u)\chi(v) = \sum_{u|n} \chi(u) \sum_{v|m} \chi(v) = f_n f_m.$$

13. Comme p est premier, les diviseurs de p^α sont les p^β avec $0 \leq \beta \leq \alpha$.

Comme $\chi(p^\beta) = \chi(p)^\beta$ et que $\chi(p) \in \{-1, 0, 1\}$, on a :

$$f_{p^\alpha} = \sum_{\beta=0}^{\alpha} \chi(p)^\beta = \begin{cases} \alpha+1 & \text{si } \chi(p) = 1 \\ \frac{1 - \chi(p)^{\alpha+1}}{1 - \chi(p)} & \text{sinon} \end{cases} = \begin{cases} \alpha+1 & \text{si } \chi(p) = 1 \\ 1 & \text{si } \chi(p) = 0 \\ 0 & \text{si } \chi(p) = -1 \text{ et } \alpha \text{ impair} \\ 1 & \text{si } \chi(p) = -1 \text{ et } \alpha \text{ pair} \end{cases} ; \text{ donc } f_{p^\alpha} \geq 0.$$

14. Comme n possède au plus n diviseurs dans $\mathbb{N}$ et que $\chi \leq 1$, on a : $f_n \leq n$.

Si $n \geq 2$: on utilise l'écriture primaire de n : $n = \prod_{i=1}^q p_i^{\alpha_i}$, où les p_i sont des nombres premiers distincts et les α_i des entiers au moins égaux à 1. Par multiplicativité de f , comme les $p_i^{\alpha_i}$ sont premiers entre eux deux à deux, $f_n = \prod_{i=1}^q f_{p_i^{\alpha_i}}$. Donc $f_n \geq 0$.

15. Pour $n \geq 2$, on reprend les notations de la question précédente. Alors $f_{n^2} = \prod_{i=1}^q f_{p_i^{2\alpha_i}}$. Or, à la question 13, avec α pair, quelle que soit la valeur de $\chi(p) \in \{-1, 0, 1\}$, $f_{p^\alpha} > 0$. Donc $f_{n^2} > 0$. Comme f_{n^2} est dans $\mathbb{Z}$, $f_{n^2} \geq 1$.

16. Si $|x| < 1$, alors la suite $(f_n x^n)$ converge vers 0 (puisque $|f_n x^n| \leq n |x|^n$). Donc le rayon de convergence de la série entière vaut au moins 1. Si $|x| > 1$, alors la suite $(f_{n^2} x^{n^2})$ tend vers l'infini (puisque $|f_{n^2} x^{n^2}| \geq |x|^{n^2}$). Donc le rayon de convergence de la série entière vaut au plus 1. Finalement le rayon de convergence vaut 1.

17. Comme $x \geq 0$ et $f_n \geq 0$, on a : $f(x) \geq \sum_{n=1}^{\infty} f_{n^2} x^{n^2} \geq \sum_{n=1}^{\infty} x^{n^2}$.

On définit la fonction g par $g(t) = x^{t^2} = e^{t^2 \ln x}$; g est continue sur $[1, +\infty[$, décroissante, intégrable ($\ln x < 0$).

Pour tout $n \geq 1$, on a : $g(n) = \int_n^{n+1} g(n) dt \geq \int_n^{n+1} g(t) dt$.

$$\text{Donc } f(x) \geq \sum_{n=1}^{\infty} g(n) \geq \sum_{n=1}^{\infty} \int_n^{n+1} g(t) dt = \int_1^{+\infty} g(t) dt.$$

Le changement de variable affine $u = t\sqrt{-\ln x}$ s'écrit :

$$\int_1^{+\infty} g(t) dt = \frac{1}{\sqrt{-\ln x}} \int_{\sqrt{-\ln x}}^{+\infty} e^{-u^2} du \geq \frac{1}{\sqrt{-\ln x}} \int_{\sqrt{\ln 2}}^{+\infty} e^{-u^2} du \quad (\text{car } -\ln x \leq \ln 2).$$

D'où la minoration demandée.