

Caractères de Dirichlet (Arithmétique)

Nous reprenons ici une grande partie du DS 5 de la saison 2019-2020.
A préparer pour vendredi 15 décembre.

Notations :

- Pour deux nombres entiers relatifs a et b , on note $a \wedge b$ le PGCD de ces deux nombres.
- On note \mathcal{P} , l'ensemble des nombres premiers.
- Pour deux nombres entiers relatifs, on note $a \% b$, le reste de la division euclidienne de a par b .
Nécessairement : $b|(a - a \% b)$ et $0 \leq a \% b < b$
- Pour tout $N \in \mathbb{N}^*$, on note \mathcal{P}_N , l'ensemble des nombres entiers de $\llbracket 1, N \rrbracket$, premier avec N .

$$\mathcal{P}_N = \{a \in \llbracket 1, N \rrbracket \mid a \wedge N = 1\}$$

- Pour tout $N \in \mathbb{N}^*$, on note $\varphi(N)$, le nombre d'entiers de $\llbracket 1, N \rrbracket$, premier avec N :

$$\varphi(N) = \text{card } \mathcal{P}_N$$

L'application $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$, $N \mapsto \varphi(N)$ est appelé indicatrice d'Euler.

- Pour tout entier $N \in \mathbb{N}$, on suppose qu'il existe une application χ_N de \mathbb{Z} dans \mathbb{R} qui satisfait :

- A.** $\chi_N(0) = 0$ et χ_N est non identiquement nul.
- B.** Pour tout a dans \mathbb{Z} , non premier avec N , $\chi_N(a) = 0$.
- C.** Pour tous entiers relatifs a et b , $\chi_N(ab) = \chi_N(a)\chi_N(b)$
On dit que χ_N est complètement multiplicative
- D.** χ_N est N -périodique : pour tout a dans \mathbb{Z} , $\chi_N(a + N) = \chi_N(a)$

S'il n'y a pas de doute sur le nombre N considéré, il est possible d'écrire χ au lieu de χ_N .
Une telle application s'appelle un *caractère de Dirichlet*.

Objectif :

Dans ce problème, conformément à la demande de Rémy D., nous démontrons quelques étapes du *théorème de Dirichlet (1840)* :

Pour tout nombre $a, n \in \mathbb{N}$ tel que $a \wedge n = 1$, il existe une infinité de nombres premiers de la forme $a + kn$
 $\forall a, n \in \mathbb{N}, \quad a \wedge n = 1 \iff \text{card}\{p \in \mathcal{P} \mid p \equiv a[n]\} = +\infty$

La démonstration complète est trop longue. Nous nous contenterons de résultats intermédiaires :

- en partie A, on étudie la fonction φ (indicatrice d'Euler) et nous terminons par un théorème d'Euler qui généralise le petit théorème de Fermat.
- en partie B, on étudie la fonction arctan ce qui nous permet d'obtenir la valeur de la limite d'une certaine suite (série).
- en partie C, on étudie quelques caractères particuliers.
- en partie D, on montre la convergence d'une certaine suite, premiers pas vers le théorème de Dirichlet.

Les deux premières parties sont indépendantes. La partie C dépend de la partie B. La partie D dépend des parties A et C.

Dans la correction figurent des commentaires complémentaires. . .

A - Indicatrice d'Euler

1. Montrer que pour tout $N \in \mathbb{N}^*$, $\varphi(N) \geq 1$.
Donner tous les entiers pour lesquels $\varphi(N) = 1$.
2. Si p est un nombre premier, que vaut $\varphi(p)$?
Pour tout entier $n \in \mathbb{N}^*$, montrer que $\varphi(p^n) = p^{n-1}(p - 1)$.

3. (a) Montrer que

$$P : \mathcal{P}_{N_1 N_2} \longrightarrow \mathcal{P}_{N_1} \times \mathcal{P}_{N_2}$$

$$a \longmapsto (a \% N_1, a \% N_2)$$

est bien définie (On vérifiera que l'ensemble d'arrivée annoncé est correct).

(b) (*) Montrer que, si N_1 et N_2 sont premiers entre eux, P est bijective de $\mathcal{P}_{N_1 N_2}$ sur $\mathcal{P}_{N_1} \times \mathcal{P}_{N_2}$.
En déduire que φ est une application multiplicative, c'est-à-dire vérifiant :

$$\forall N_1, N_2 \in \mathbb{N}, \quad N_1 \wedge N_2 = 1 \implies \varphi(N_1 N_2) = \varphi(N_1) \varphi(N_2)$$

4. Soit $N \in \mathbb{N}^*$. Soit $a \in \mathcal{P}_N$.

(a) Montrer que pour tout $k \in \mathcal{P}_N$, $(ak) \% N \in \mathcal{P}_N$

(b) On définit alors :

$$\psi_a : \mathcal{P}_N \rightarrow \mathcal{P}_N, \quad k \mapsto (ak) \% N$$

Montrer que ψ_a est bijective.

(c) En déduire le théorème d'Euler (généralisation du petit théorème de Fermat) :

$$\forall a \in \mathbb{N}, \quad a \wedge N = 1 \implies a^{\varphi(N)} \equiv 1[N]$$

B - Etude de arctan

On étudie ici la fonction arctan, de classe \mathcal{C}^∞ sur \mathbb{R} (résultat du cours).

On note également ici :

$$A : \mathbb{R} \rightarrow \mathbb{C}, \quad x \mapsto \frac{1}{1 - ix}$$

1. Montrer que A est de classe \mathcal{C}^∞ sur \mathbb{R} .

Pour tout $k \in \mathbb{N}$, donner une expression de $A^{(k)}(x)$, pour tout $x \in \mathbb{R}$ (à démontrer).

2. Montrer que pour tout $x \in \mathbb{R}$, $\arctan'(x) = \operatorname{Re}(A(x))$.

En déduire une expression de $\arctan^{(k+1)}(0)$, pour tout $k \in \mathbb{N}$.

3. (a) Montrer que pour tout $x \in]0, 1[$, il existe $c_x \in]0, x[$ tel que

$$\arctan(x) = \sum_{k=0}^N \frac{\arctan^{(k)}(0)}{k!} x^k + \frac{\arctan^{N+1}(c_x)}{(N+1)!} x^{N+1}$$

On pourra considérer, x fixé, l'application $h_N : t \mapsto \arctan(x) - \sum_{k=0}^N \frac{\arctan^{(k)}(t)}{k!} (x-t)^k - R_N \frac{(x-t)^{N+1}}{(N+1)!}$

avec R_N choisit tel que $h_N(0) = 0$.

(b) En déduire qu'il existe $c_1 \in]0, 1[$ tel que

$$\frac{\pi}{4} = \sum_{k=0}^p \frac{(-1)^k}{2k+1} + \frac{1}{2p+1} \operatorname{Re} \left(\frac{i^{2p}}{(1 - ic_1)^{2p+1}} \right)$$

(c) Quelle est la limite de $\left(\sum_{k=0}^n \frac{(-1)^k}{2k+1} \right)_{n \in \mathbb{N}}$?

C. Caractères. Cas particuliers

1. Pour tout entier $N \in \mathbb{N}$, calculer $\chi_N(1)$.

2. Montrer que si $a \wedge N \neq 1$, alors $\{p \in \mathcal{P} \mid p \equiv a[N]\}$ contient au plus un élément.

En déduire que $\{p \in \mathcal{P} \mid p \equiv a[N]\} = +\infty \implies \chi_N(a) \neq 0$.

3. En supposant $N = 2$, déterminer χ_2 .

4. On suppose dans cette question que $N = 4$.

(a) Montrer que $\chi_4(3)$ ne peut prendre que les valeurs 1 ou -1 .

(b) On suppose maintenant $\chi_4(3) = -1$.

On note pour tout $n \in \mathbb{N}^*$, $S_n = \sum_{k=1}^n \frac{\chi_4(k)}{k}$.

Montrer la convergence de la suite $(S_n)_{n \in \mathbb{N}}$ et calculer la valeur de sa limite, notée $\sum_{n=1}^{+\infty} \frac{\chi_4(n)}{n}$.

5. (a) Montrer que s'il existe $a \in \mathcal{P}_N$ tel que $\{(a^k) \% N, k \in \llbracket 1, \varphi(N) \rrbracket\} = \mathcal{P}_N$, alors

$$\chi_N^a : t \mapsto \begin{cases} 0 & \text{si } t \wedge N \neq 1 \\ \exp(2i\pi \frac{k_t}{\varphi(N)}) & \text{avec } t \equiv (a^{k_t})[N] \end{cases}$$

est un caractère de Dirichlet.

(b) Montrer que χ_N^a vérifie également le critère suivant :

E. Il existe un entier $r \in \mathbb{Z}$ tel que $\chi_N^a(r) \notin \{0, 1\}$

(c) Proposer un caractère de Dirichlet vérifiant également **E** pour $N = 6$.

Et un autre pour $N = 7$.

D. Convergence de la série $\sum_{n \geq 1} \frac{\chi(n)}{n}$

Soit $N \in \mathbb{N}$, fixé. Pour la suite de cette partie, la fonction χ_N sera simplement notée χ .

On note pour toute cette partie : pour tout $n \in \mathbb{N}$, $S_n = \sum_{k=1}^n \chi(k)$ et $T_n = \sum_{k=1}^n \frac{\chi(k)}{k}$

1. Soit $a \in \mathcal{P}_N$.

En exploitant le théorème d'Euler (A.4.c.), montrer que $|\chi(a)| = 1$.

Plus précisément, montrer que $\chi(a)$ est une racine r -ième de l'unité. On donnera une expression de r , en fonction de N .

2. Établir l'identité :

$$\sum_{k=1}^{N-1} \chi(ak) = \sum_{k=1}^{N-1} \chi(k)$$

On suppose dorénavant qu'il existe $a \in \mathcal{P}_N$ vérifiant $\chi(a) \neq 1$ (critère **E**).

3. Pour tout entier h , calculer $\sum_{k=hN}^{(h+1)N-1} \chi(k)$.

On pourra commencer par le cas $h = 0$ puis exploiter la N -périodicité de χ .

4. Montrer, pour tout $m > 0$, l'inégalité :

$$\left| \sum_{k=1}^m \chi(k) \right| \leq \varphi(N)$$

5. (a) On rappelle qu'on dit qu'une suite (u_n) vérifie le critère de Cauchy si

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tel que } \forall q > p \geq n, |u_q - u_p| < \epsilon$$

Sans démonstration, rappeler la relation entre « (u_n) converge » et « (u_n) vérifie le critère de Cauchy » (on supposera que la suite (u_n) est à valeurs réelles).

(b) Démontrer que le résultat énoncé précédemment reste vraie pour (u_n) à valeurs complexes.

(c) Soit $n \in \mathbb{N}^*$. Démontrer que pour tout $q > p \geq n$,

$$\sum_{k=p}^q \frac{\chi(k)}{k} = \sum_{k=p}^{q-1} S_k \left(\frac{1}{k} - \frac{1}{k+1} \right) + \frac{S_q}{q} - \frac{S_{p-1}}{p}$$

(d) En déduire que (T_n) vérifie le critère de Cauchy.

(e) Conclure quant à la convergence de la suite $\left(\sum_{k=1}^n \frac{\chi(k)}{k} \right)_{n \geq 1}$.

Remarques !

Quel lien entre les résultats trouvés ici et le théorème de Dirichlet ?

1. On montre ici que si $a \wedge N \neq 1$, alors il y a au plus un nombre premier de la forme $a + kN$. On se place donc dans la situation $a \wedge N = 1$. On peut rendre nul les autres cas : règle **B**.
2. Comme on s'intéresse à l'ensemble $\mathcal{P}_{a,N} = \{p \in \mathcal{P} \mid p \equiv a[N]\}$, on ne différencie pas ces nombres. C'est pourquoi on vise $\chi(p_1) = \chi(p_2)$ si $p_1 \equiv p_2 \equiv a[N]$: règle **D**.
3. La « clé d'or » est une formule d'Euler, reprise par Riemann :

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$$

généralisée par Dirichlet en

$$L(s, \chi) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

par la condition que χ soient complètement multiplicative : règle **C**.

Nous établirons cette égalité lors du DM sur les séries (chapitre 27).

4. Cette formule permet de différencier les nombres premiers selon les valeurs de $\chi(p)$, caractéristiques des ensembles $\mathcal{P}_{a,N} = \{p \in \mathcal{P} \mid p \equiv a[N]\}$. On exploite des propriétés algébriques pour inverser la relation de Dirichlet (avec la série L , dérivée logarithmiquement...).

5. La convergence de la série $\sum_{n \geq 1} \frac{\chi(n)}{n}$, avec divergence de la série $\sum_{n \geq 1} \frac{|\chi(n)|}{n}$ donne pour condition nécessaire l'infinité des nombres premiers p dont chaque $\chi(p)$ a une même valeur ($\chi(a)$ par exemple).

6. Et mieux. En exploitant les méthodes d'analyse asymptotiques, La Vallée-Poussin, démontre mieux : la répartition des nombres premiers dans les classes d'équivalence $\mathcal{P}_{a,N}$ est uniforme (égale pour chaque classe ou encore : indépendante de a).

Ainsi, si on note $\Pi(a, N, x) = \text{card}\{p \in \mathcal{P} \mid p \leq x \text{ \& } p \equiv a[N]\}$, on a

$$\Pi(a, N, x) \sim_{x \rightarrow \infty} \frac{x}{\varphi(N) \ln x}$$

7. Une question résiste à notre niveau : comment construire la fonction χ ? Avec l'existence de a tel que $\chi(a) \notin \{0, 1\}$... (critère **E**). Une piste est donnée en question C.5.

Problème - Caractères de Dirichlet

A - Indicatrice d'Euler

1. Pour tout entier N , $1 \in \mathcal{P}_N$, donc

$$\forall N \in \mathbb{N}^*, \varphi(N) \geq 1$$

$$\varphi(N) = 1 \iff \mathcal{P}_N = \{1\}$$

Or pour tout $N \geq 2$, $N - 1 \in \mathcal{P}_N$, car $(N \wedge N - 1) | N$ et $(N \wedge N - 1) | N - 1$ donc $(N \wedge N - 1) | 1$.

Ainsi, pour tout $N \geq 2$, $\varphi(N) = 1 \implies N - 1 = 1 \implies N = 2$.

Réciproquement, comme $\varphi(2) = 1$ et $\varphi(1) = 1$;

les seuls entiers pour lesquels $\varphi(N) = 1$ sont 1 et 2

2. Si p est un nombre premier, alors tous les entiers de 1 à $p - 1$ sont premiers avec p ;
et ce n'est pas le cas de p .

$$\varphi(p) = p - 1$$

Soit $n \in \mathbb{N}^*$. Soit $a \in \llbracket 1, p^n \rrbracket$.

On note $\delta = a \wedge p^n$. Alors $\delta | p^n$, donc $\delta = p^m$ avec $m \in \llbracket 0, n \rrbracket$.

Ainsi on a les équivalences :

$$a \notin \mathcal{P}_{p^n} \iff \delta \neq 1 \iff \exists m \in \llbracket 1, n \rrbracket \text{ tel que } \delta = p^m \iff p | a$$

Donc $\mathcal{P}_{p^n} = \llbracket 1, p^n \rrbracket \setminus (p\mathbb{Z}) = \llbracket 1, p^n \rrbracket \setminus \{rp \mid 1 \leq r \leq p^{n-1}\}$.

$$\forall n \in \mathbb{N}^*, \varphi(p^n) = \text{Card}(\mathcal{P}_{p^n}) = (p^n - 1 + 1) - (p^{n-1} - 1 + 1) = p^n - p^{n-1} = p^{n-1}(p - 1)$$

☀ Piste de recherche...

Il s'agit donc de montrer une égalité entre fonctions définie comme cardinaux d'ensembles.

Dans cette situation, le plus courant est de montrer la bijectivité entre les deux ensembles.

Ici il s'agit du théorème dit « lemme des restes chinois ». Nous avons vu dans l'exercice 212.

$$P: \begin{array}{ccc} \mathcal{P}_{N_1 N_2} & \longrightarrow & \mathcal{P}_{N_1} \times \mathcal{P}_{N_2} \\ a & \longmapsto & (a \% N_1, a \% N_2) \end{array}$$

mais faut-il s'assurer qu'elle est bien définie; puis qu'elle est bien bijective.

(a) Soient N_1 et N_2 deux nombres premiers entre eux.

Soit $a \in \mathcal{P}_{N_1 N_2}$. Donc $a \wedge N_1 N_2 = 1$. Donc $\exists u, v \in \mathbb{Z}$ tel que $ua + vN_1 N_2 = 1$

Soit $a_1 = a \% N_1$. Donc $a_1 \in \llbracket 0, N_1 - 1 \rrbracket$ et il existe $k_1 \in \mathbb{Z}$ tel que $a = k_1 N_1 + a_1$, donc

$$1 = ua + vN_1 N_2 = ua_1 + (uk_1 + vN_2)N_1 \implies a_1 \wedge N_1 = 1$$

Ainsi $a_1 \in \mathcal{P}_{N_1}$.

Et de même si on note $a_2 = a \% N_2$, alors $a_2 \in \llbracket 0, N_2 - 1 \rrbracket$ et $a_2 \wedge N_2 = 1$, donc $a_2 \in \mathcal{P}_{N_2}$.

L'application $P: \begin{array}{ccc} \mathcal{P}_{N_1 N_2} & \longrightarrow & \mathcal{P}_{N_1} \times \mathcal{P}_{N_2} \\ a & \longmapsto & (a \% N_1, a \% N_2) \end{array}$ est donc bien définie

(b) Soient $a, a' \in \mathcal{P}_{N_1 N_2}$ tel que $P(a) = P(a')$.

Donc $a \% N_1 = a' \% N_1$, ainsi $N_1 | (a - a')$. De même $N_2 | (a - a')$.

Et comme $N_1 \wedge N_2 = 1$, d'après un lemme de Gauss $N_1 N_2 | (a - a')$.

Or $a, a' \in \mathcal{P}_{N_1 N_2}$, donc $a - a' \in \llbracket 2 - N_1 N_2, N_1 N_2 - 2 \rrbracket$.

Le seul nombre divisible par $N_1 N_2$ de cet intervalle est 0. Donc $a - a' = 0$.

Par conséquent $a = a'$ et P est injectif.

 **Piste de recherche...**

 Pour montrer la surjectivité, on considère a_1 et a_2 et on essaye de construire le nombre a tel que $P(a) = (a_1, a_2)$.

 On se rend compte que $a = a_1 + k_1 N_1 = a_2 + k_2 N_2$, donc $a_1 - a_2 = k_2 N_2 - k_1 N_1$.

 Cela nous fait penser à la décomposition de Bézout...

Soit $(a_1, a_2) \in \mathcal{P}_{N_1} \times \mathcal{P}_{N_2}$.

$N_1 \wedge N_2 = 1$. Il existe $u_1, u_2 \in \mathbb{Z}$ tel que $u_1 N_1 + u_2 N_2 = 1$.

Donc en multipliant par $a_1 - a_2$: $(a_1 - a_2)u_1 N_1 + (a_1 - a_2)u_2 N_2 = a_1 - a_2$.

Il existe $U_1 (= (a_2 - a_1)u_1), U_2 (= (a_1 - a_2)u_2) \in \mathbb{Z}$ tels que $U_1 N_1 + a_1 = U_2 N_2 + a_2$.

On note $A = U_1 N_1 + a_1$, puis $a = A \% N_1 N_2$.

Donc $a \in \llbracket 0, N_1 N_2 - 1 \rrbracket$.

Puis si $\delta | a$ et $\delta | N_1 N_2$, alors $\delta | A = a + K N_1 N_2$.

Comme $N_1 \wedge N_2 = 1$, alors $\delta | N_1$ ou $\delta | N_2$.

Sans perte de généralité, supposons que $\delta | N_1$,

comme $\delta | A = U_1 N_1 + a_1$, alors $\delta | N_1$ et $\delta | a_1$. Donc $\delta = 1$.

Donc $a \in \mathcal{P}_{N_1 N_2}$.

Enfin, par construction, $a_1 \equiv A \equiv a [N_1]$ et $a_2 \equiv A \equiv a [N_2]$.

Donc il existe $a \in \mathcal{P}_{N_1 N_2}$ tel que $P(a) = (a_1, a_2) : P$ est surjective de $\mathcal{P}_{N_1 N_2}$ sur $\mathcal{P}_{N_1} \mathcal{P}_{N_2}$.

L'application P est bijective

$\varphi(N_1) \times \varphi(N_2)$ est le cardinal du produit cartésien $\mathcal{P}_{N_1} \times \mathcal{P}_{N_2}$. Ainsi, il y a égalité des cardinaux :

$$\forall N_1, N_2 \in \mathbb{N}, \text{ tels que } N_1 \wedge N_2 = 1 \text{ alors } \varphi(N_1 N_2) = \varphi(N_1) \varphi(N_2)$$

 **Remarques !**

 En fait l'application P est un morphisme bijectif de groupes,

du groupe des inversibles de $\frac{\mathbb{Z}}{N_1 N_2 \mathbb{Z}}$, i.e. $\left(\frac{\mathbb{Z}}{N_1 N_2 \mathbb{Z}}\right)^*$, de cardinal $\varphi(N_1 N_2)$,

sur le groupe, produit cartésien, $\left(\frac{\mathbb{Z}}{N_1 \mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{N_2 \mathbb{Z}}\right)^*$ de cardinal $\varphi(N_1) \varphi(N_2)$.

 **Remarques !**

 Avec la formule multiplicative et l'expression sur les puissances des nombres premiers, on montre que

si $n = \prod_{i=1}^r p_i^{n_i}$, alors

$$\varphi(n) = \prod_{i=1}^r p_i^{n_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

4. Soit $N \in \mathbb{N}^*$. Soit $a \in \mathcal{P}_N$.

(a) Soit $k \in \mathcal{P}_N$. Par définition $ka \% N \in \llbracket 0, N \rrbracket$.

Or $k \wedge N = 1, a \wedge N = 1$, donc d'après un lemme de Gauss (facteurs relativement premiers) :

$$ak \wedge N = 1.$$

Donc, pour tout $k \in \mathcal{P}_N, ka \% N \in \mathcal{P}_N$

(b) On définit alors :

$$\psi_a : \mathcal{P}_N \rightarrow \mathcal{P}_N, k \mapsto ka \% N$$

Supposons que $\psi_a(k) = \psi_a(k')$, alors $N | (k - k')a$.

Donc, comme $N \wedge a = 1, N | k - k'$. Ainsi : $k - k' \in \llbracket 2 - N, N - 2 \rrbracket \cap (N \cdot \mathbb{Z}) = \{0\}$.

Ainsi $k = k'$ et donc ψ_a est injective.

Soit $h \in \mathcal{P}_N$. Comme $a \wedge N = 1$, alors d'après le théorème de Bézout,

il existe $u, v \in \mathbb{Z}$ tel que $ua + vN = 1$.

Donc en multipliant par h : $(hu)a + hvN = h$, et modulo N : $(hu)a \equiv h [N]$.

Enfin, en prenant $k = hu \% N$, on a donc $k \times a = h$;

et $u \wedge N = 1, h \wedge N = 1$, donc $hu \wedge N = 1$ et $k \wedge N = 1$.

Ainsi il existe $k \in \mathcal{P}_N$ tel que $a \times k = h$. Donc ψ_a est surjective.

ψ_a est bijective

Remarques !

Comme les ensembles de départ et d'arrivée de ψ_a sont finis, et qu'ils ont le même cardinal (ce sont les mêmes), on peut démontrer que

ψ_a est bijective si et seulement si ψ_a est injective ou ψ_a est surjective.

On aurait donc pu réduire l'étude précédente.

Piste de recherche...

On applique exactement la même démonstration que pour le théorème de Fermat, mais avec moins de nombres (au lieu de prendre tous les nombres de 1 à $N - 1$, on prend ceux de \mathcal{P}_N)

Soit $a \in \mathcal{P}_N$:

$$\prod_{k \in \mathcal{P}_N} ka = a^{\text{card}(\mathcal{P}_N)} \prod_{k \in \mathcal{P}_N} k = a^{\varphi(N)} \prod_{k \in \mathcal{P}_N} k$$

Mais aussi :

$$\prod_{k \in \mathcal{P}_N} ka = \prod_{k \in \mathcal{P}_N} \psi_a(k) = \prod_{h \in \mathcal{P}_N} h$$

Comme $N \wedge h = 1$, pour tout $h \in \mathcal{P}_N$, alors (Gauss) : $N \wedge (\prod_{h \in \mathcal{P}_N} h) = 1$. Donc

$$a^{\varphi(N)} \prod_{k \in \mathcal{P}_N} k = \prod_{h \in \mathcal{P}_N} h \implies a^{\varphi(N)} \equiv 1[N]$$

Si $A \in \mathbb{Z}$ et $A \wedge N = 1$, alors en prenant $a = A \% N$, on a $a \equiv A[N]$ donc $a \wedge N = 1$.

Puis, pour tout $k \in \mathbb{N}$, $A^k = (a + hN)^k = \sum_{i=0}^k \binom{k}{i} a^i (hN)^{k-i} \equiv a^k[N]$.

Et donc $A^{\varphi(N)} \equiv a^{\varphi(N)} \equiv 1[N]$.

$$\forall a \in \mathbb{N}, \quad a \wedge N = 1 \implies a^{\varphi(N)} \equiv 1[N]$$

Remarques !

On retrouve pour p premier, le petit théorème de Fermat :

$\varphi(p) = p - 1$ et donc $a^{p-1} \equiv 1[p]$

B - Etude de arctan

On étudie ici la fonction arctan, de classe \mathcal{C}^∞ sur \mathbb{R} (résultat du cours).

On note également ici :

$$A : \mathbb{R} \rightarrow \mathbb{C}, \quad x \mapsto \frac{1}{1 - ix}$$

1. A est une fraction rationnelle et son ensemble de définition est \mathbb{R} .

Donc A est de classe \mathcal{C}^∞ sur \mathbb{R} .

Posons, pour tout $k \in \mathbb{N}$, \mathcal{P}_k : « $\forall x \in \mathbb{R}, A^{(k)}(x) = \frac{k!i^k}{(1 - ix)^{k+1}}$ ».

— Pour tout $x \in \mathbb{R}, A^{(0)}(x) = A(x) = \frac{1}{1 - ix} = \frac{0!i^0}{(1 - ix)^{0+1}}$, donc \mathcal{P}_0 est vraie.

— Soit $k \in \mathbb{N}$. On suppose que \mathcal{P}_k est vraie.

Donc pour tout $x \in \mathbb{R}, A^{(k)}(x) = \frac{k!i^k}{(1 - ix)^{k+1}}$. On applique l'algorithme de dérivation :

$$\forall x \in \mathbb{R}, \quad A^{(k+1)}(x) = \frac{-k!i^k \times (k+1) \times (-i)}{(1 - ix)^{k+1+1}} = \frac{(k+1)!i^{k+1}}{(1 - ix)^{k+2}}$$

Donc \mathcal{P}_{k+1} est vraie.

$$\forall k \in \mathbb{N}, \forall x \in \mathbb{R}, A^{(k)}(x) = \frac{k!i^k}{(1-ix)^{k+1}}$$

2. Pour tout $x \in \mathbb{R}$, $\arctan'(x) = \frac{1}{1+x^2}$.

$$\text{Puis } \operatorname{Re}(A(x)) = \frac{1}{2}(A(x) + \overline{A(x)}) = \frac{1}{2} \left(\frac{1}{1-ix} + \frac{1}{1+ix} \right) = \frac{1+ix+1-ix}{2(1+x^2)} = \frac{1}{1+x^2}$$

$$\text{Pour tout } x \in \mathbb{R}, \arctan'(x) = \operatorname{Re}(A(x)).$$

Puis par linéarité de la dérivation, pour tout $k \in \mathbb{N}$:

$$\arctan^{(k+1)} = (\arctan')^{(k)} = \left(\frac{1}{2}(A + \overline{A}) \right)^{(k)} = \frac{1}{2} (A^{(k)} + \overline{A^{(k)}}) = \operatorname{Re} (A^{(k)})$$

$$\forall k \in \mathbb{N}, \arctan^{(k+1)}(0) = \operatorname{Re} \left(\frac{k!i^k}{(1-0)^{k+1}} \right) = \begin{cases} 0 & \text{si } k = 2p+1 \\ (-1)^p(2p)! & \text{si } k = 2p \end{cases}$$

3. (a) Soit $x \in]0, 1]$. Considérons

$$\begin{aligned} h_N : t &\mapsto \arctan(x) - \sum_{k=0}^N \frac{\arctan^{(k)}(t)}{k!} (x-t)^k - R_N \frac{(x-t)^{N+1}}{(N+1)!} \\ &= \arctan(x) - \left(\arctan t + \frac{\arctan'(t)}{1} (x-t) + \dots + \frac{\arctan^{(n)}(t)}{n!} (x-t)^n \right) - R_N \frac{(x-t)^{N+1}}{(N+1)!} \end{aligned}$$

$$\text{où } R_N \text{ est choisi de manière à ce que } h_N(0) = 0 \text{ i.e. } R_N = \frac{(N+1)!}{x^{N+1}} \left(\arctan(x) - \sum_{k=0}^n \frac{\arctan^{(k)}(0)}{k!} x^k \right).$$

Par ailleurs $h_N(x) = \arctan(x) - \arctan(x) = 0$.

Donc d'après le théorème de Rolle ($h_N(0) = h_N(x) = 0$), il existe $c \in]0, x[$ tel que $h'_N(c) = 0$.

Or, par télescopage

$$\begin{aligned} h'_N(t) &= - \left(\sum_{k=0}^N \frac{\arctan^{(k+1)}(t)}{k!} (x-t)^k - \frac{\arctan^{(k)}(t)}{(k-1)!} (x-t)^{k-1} \right) + \frac{R_N}{N!} (x-t)^N \\ &= - \frac{\arctan^{(N+1)}(t)}{N!} (x-t)^N + \frac{R_N}{N!} (x-t)^N \end{aligned}$$

Comme $h'_N(c) = 0$, on a donc $R_N = \arctan^{(N+1)}(c)$.

Enfin comme $h_N(0) = 0$, on a donc (en $t = 0$) :

$$\forall x \in]0, 1], \exists c_x \in]0, x[\text{ tel que } \arctan(x) = \sum_{k=0}^N \frac{\arctan^{(k)}(0)}{k!} x^k + \frac{\arctan^{N+1}(c_x)}{(N+1)!} x^{N+1}$$

(b) En $x = 1$ et $N = 2p$, avec la formule de $\arctan^{(k)}(0)$ trouvée plus haut :

Il existe $c_1 \in]0, 1[$ tel que

$$\begin{aligned} \frac{\pi}{4} &= \arctan(0) + \sum_{k=0}^{p-1} \left(\frac{\arctan^{(2k+1)}(0)}{(2k+1)!} 1^{2k+1} + \frac{\arctan^{(2k+2)}(0)}{(2k+2)!} 1^{2k+2} \right) + \frac{\arctan^{2p+1}(c_1)}{(2p+1)!} 1^{2p+1} \\ &= \sum_{k=0}^p \frac{(-1)^k (2k)!}{(2k+1)!} + \frac{1}{(2p+1)!} \operatorname{Re} (A^{2p}(c_1)) \end{aligned}$$

$$\exists c_1 \in]0, 1[\text{ tel que } \frac{\pi}{4} = \sum_{k=0}^p \frac{(-1)^k}{2k+1} + \frac{1}{2p+1} \operatorname{Re} \left(\frac{i^{2p}}{(1-ic_1)^{2p}} \right)$$

(c) Comme

$$\left| \operatorname{Re} \left(\frac{i^{2p}}{(1 - ic_1)^{2p}} \right) \right| \leq \left| \frac{i^{2p}}{(1 - ic_1)^{2p}} \right| = \left(\frac{|i|}{|1 - ic_1|} \right)^{2p} = \left(\frac{1}{|1 - ic_1|} \right)^{2p} \leq 1$$

car $|1 - ic_1| = \sqrt{1 + c_1^2} \geq 1$. Alors par théorème d'encadrement :

$$\lim_{p \rightarrow \infty} \sum_{k=0}^p \frac{(-1)^k}{2k+1} = \frac{\pi}{4}$$

C. Caractères. Cas particuliers : $N = 2$ et $N = 4$

1. Soit $N \in \mathbb{N}$. D'après la règle **C**, pour tout entier a , $\chi_N(a) = \chi_N(1 \times a) = \chi_N(1)\chi_N(a)$.
Or χ_N est non identiquement nul (règle **A**), donc il existe $a \in \mathbb{N}$, tel que $\chi_N(a) \neq 0$.

Et nécessairement $\chi_N(1) = 1$, pour tout entier $N \in \mathbb{N}$.

2. Notons $\delta = a \wedge N$ et supposons que $\delta \neq 1$. Soit $p \in \{p \in \mathcal{P} \mid p \equiv a[N]\}$.
Alors $p = a + kN = \delta(a_1 + kN_1)$, donc $\delta \mid p$. Or p est premier donc $\delta = 1$ ou $\delta = p$.
Comme $\delta \neq 1$, on a donc $\delta = p$.

Si $a \wedge N \neq 1$, $\{p \in \mathcal{P} \mid p \equiv a[N]\}$ contient 1 élément : $a \wedge N$ si $a \wedge N \in \mathcal{P}$ et 0 sinon

Par contraposée :

$\{p \in \mathcal{P} \mid p \equiv a[N]\} = +\infty \implies a \wedge N = 1 \implies \chi_N(a) \neq 0$ (Règle **B**).

3. On suppose $N = 2$. Par 2-parité :

$$\chi_2 : m \mapsto \begin{cases} 0 & \text{si } m \equiv 0[2] \\ 1 & \text{si } m \equiv 1[2] \end{cases}$$

4. (a) $\chi_4(9) = (\chi_4(3))^2 = \chi_4(1 + 2 \times 4) = \chi_4(1) = 1$.

$\chi_4(3)$ ne peut prendre que les valeurs 1 ou -1 .

- (b) On suppose maintenant $\chi_4(3) = -1$.

$\chi_4(2) = 0$, car $2 \wedge 4 = 2 \neq 1$. Donc par 4-parité :

$$\chi_4 : m \mapsto \begin{cases} 0 & \text{si } m \equiv 0[4] \\ 1 & \text{si } m \equiv 1[4] \\ -1 & \text{si } m \equiv 3[4] \end{cases}$$

Donc, pour tout entier $s \in \mathbb{N}$, en notant $s = 4q_s + r_s$ (division euclidienne par 4)

$$\sum_{n=1}^s \frac{\chi(n)}{n} = \sum_{k=0}^{q_s-1} \left(\frac{\chi(1+4k)}{1+4k} + \frac{\chi(2+4k)}{2+4k} + \frac{\chi(3+4k)}{3+4k} + \frac{\chi(4+4k)}{4+4k} \right) + \sum_{h=1}^{r_s} \frac{\chi(4q_s+h)}{4q_s+h}$$

(si $r_s = 0$, la dernière somme est nulle car vide.).

Ainsi, selon les valeurs de χ :

$$\sum_{n=1}^s \frac{\chi(n)}{n} = \sum_{k=0}^{q_s-1} \left(\frac{1}{1+4k} + \frac{-1}{3+4k} \right) + \sum_{h=1}^{r_s} \frac{\chi(4q_s+h)}{4q_s+h} = \sum_{j=0}^{2(q_s-1)} \frac{(-1)^j}{1+2j} + \sum_{h=1}^{r_s} \frac{\chi(4q_s+h)}{4q_s+h}$$

Comme, pour $s \rightarrow \infty, q_s \rightarrow \infty$:

$$\left| \sum_{h=1}^r \frac{\chi(4q_s + h)}{4q_s + h} \right| \leq \frac{2}{4q_s} \xrightarrow{s \rightarrow \infty} 0$$

Donc, d'après la partie B. :

$$\left(\sum_{n=1}^s \frac{\chi(n)}{n} \right)_n \text{ converge et } \lim_{s \rightarrow \infty} \sum_{n=1}^s \frac{\chi(n)}{n} = \frac{\pi}{4}$$

5. (a) On suppose qu'il existe $a \in \mathcal{P}_N$ tel que $\{(a^k) \% N, k \in \llbracket 1, \varphi(N) \rrbracket\} = \mathcal{P}_N$.

Il faut d'abord vérifier que χ_N^a est bien définie.

Si $t \in \mathbb{Z}$:

- ou bien $t \wedge N \neq 1$
- ou bien $t \wedge N = 1$ et dans ce cas, $t \% N \in \mathcal{P}_N$
et donc il existe $k \in \llbracket 1, \varphi(N) \rrbracket$ tel que $a^k \% N = t \% N$ i.e. $a^k \equiv t[N]$.

Les critères **A**, **B** et **D** sont évidents, par construction de χ_N^a .

Soient $b_1, b_2 \in \mathcal{P}_N$. Soit $k_1, k_2 \in \llbracket 1, \varphi(N) \rrbracket$ tel que $b_1 = a^{k_1} \% N$ et $b_2 = a^{k_2} \% N$.

Alors $b_1 \times b_2 = a^{k_1+k_2} \% N$.

- Ou bien $k_1 + k_2 \leq \varphi(N)$
et donc $\chi_N^a(b_1 b_2) = \exp(2i\pi \frac{k_1 + k_2}{\varphi(N)}) = \exp(2i\pi \frac{k_1}{\varphi(N)}) \times \exp(2i\pi \frac{k_2}{\varphi(N)}) = \chi(b_1) \times \chi(b_2)$
- Ou bien $k_1 + k_2 \geq \varphi(N)$
et donc $\chi_N^a(b_1 b_2) = \exp(2i\pi \frac{k_1 + k_2 - \varphi(N)}{\varphi(N)}) = \exp(2i\pi \frac{k_1 + k_2}{\varphi(N)}) = \chi(b_1) \times \chi(b_2)$

Dans tous les cas, le critère **B** est également vérifié.

$$\text{Donc } \chi_N^a : t \mapsto \begin{cases} 0 & \text{si } t \wedge N \neq 1 \\ \exp(2i\pi \frac{k_t}{\varphi(N)}) & \text{avec } t \equiv (a^{k_t})[N] \end{cases} \text{ est un caractère de Dirichlet.}$$

(b) $\chi_N^a(a) = \exp(2i\pi \frac{1}{\varphi(N)}) \notin \{0, 1\}$.

Donc χ_N^a vérifie également le critère **E**.

(c) $\varphi(6) = \varphi(2 \times 3) = 1 \times 2$. $\mathcal{P}_6 = \{1, 5\}$.

$$\text{On peut (doit) considérer } \chi_6 : t \mapsto \begin{cases} -1 & \text{si } m \equiv 5[6] \\ 1 & \text{si } m \equiv 1[6] \\ 0 & \text{sinon} \end{cases}$$

$\varphi(7) = 6$. $\mathcal{P}_7 = \{1, 2, 3, 4, 5, 6\}$.

On vérifie que $a = 2$ ne marche pas $2^3 \% 7$.

Mais $a = 3$ fonctionne : $((3^k) \% 7) = (3, 2, 6, 4, 5, 1)$.

On note $\alpha = e^{i\pi/3}$ ($= -j^2$), racine 6-ième primitive de l'unité

$$\text{On peut considérer } \chi_7 : t \mapsto \begin{cases} 0 & \text{si } m \equiv 0[7] \\ 1 & \text{si } m \equiv 1[7] \\ \alpha^2 = j & \text{si } m \equiv 2[7] \\ \alpha = -j^2 & \text{si } m \equiv 3[7] \\ \alpha^4 = j^2 & \text{si } m \equiv 4[7] \\ \alpha^5 = -j & \text{si } m \equiv 5[7] \\ \alpha^3 = -1 & \text{si } m \equiv 6[7] \end{cases}$$

D. Convergence de la série $\sum_{n \geq 1} \frac{\chi(n)}{n}$

1. Soit $a \in \mathcal{P}_N$. Par propriété multiplicative de χ , comme $a^{\varphi(N)} = 1$:

$$1 = \chi(1) = \chi\left(a^{\varphi(N)}\right) = [\chi(a)]^{\varphi(N)}$$

Donc $\chi(a)$ est une racine $\varphi(N)$ -ième de l'unité et ainsi $|\chi(a)| = 1$

○ Remarques !

⚡ $\varphi(4) = \varphi(2^2) = 2 \times (2 - 1) = 2$. Donc $\chi_4(3)$ est une racine deuxième (carrée) de l'unité.
 ⚡ On retrouve bien $\chi_4(3) = \pm 1$

2. Soit $a \in \mathcal{P}_N$ et $\overline{\psi}_a : \llbracket 1, N-1 \rrbracket \rightarrow \llbracket 1, N-1 \rrbracket, k \mapsto ak \% N$.

On reprend la même démonstration qu'en A.4.(b) (mais pour des ensembles plus larges).

$\overline{\psi}_a$ est bijective :

- elle est surjective, car $a \wedge N = 1$, donc d'après l'identité de Bézout : $\exists K \in \mathbb{Z}$ tel que $Ka \equiv 1[N]$.
 Pour tout $h \in \llbracket 1, N-1 \rrbracket$, avec $k = hK \% N$, alors $k \in \llbracket 0, N-1 \rrbracket$ et $ka \equiv hKA \equiv h1 \equiv h[N]$.
 Donc nécessairement $k \neq 0$ et $\overline{\psi}_a(k) = h$, donc $\overline{\psi}_a$ est surjective.
- pour des raisons de cardinaux : $\overline{\psi}_a$ est alors injective et bijective.

On a alors (changement d'indice $h = \overline{\psi}_a(k)$) :

$$\sum_{k=1}^{N-1} \chi(ak) = \sum_{k=1}^{N-1} \chi(\overline{\psi}_a(k)) = \sum_{h=1}^{N-1} \chi(h)$$

On suppose dorénavant qu'il existe $a \in \mathcal{P}_N$ vérifiant $\chi(a) \neq 1$.

3. Pour $h = 0$: notons

$$S_0 = \sum_{k=0}^{N-1} \chi(k) = \sum_{k=1}^{N-1} \chi(k)$$

Alors d'après la question précédente :

$$S_0 = \sum_{k=1}^{N-1} \chi(ak) = \chi(a) \sum_{k=1}^{N-1} \chi(k) = \chi(a) S_0$$

Or $\chi(a) \neq 1$, donc nécessairement : $S_0 = 0$.

Faisons les deux changements de variables : $u = k - hN$, par N -périodicité (règle **D.**) :

$$S_h = \sum_{k=hN}^{(h+1)N-1} \chi(k) = \sum_{u=0}^{N-1} \chi(u + hN) = \sum_{u=0}^{N-1} \chi(u) = S_0 = 0$$

Pour tout entier h , $\sum_{k=hN}^{(h+1)N-1} \chi(k) = 0$.

4. Soit $m > 0$, On considère $m = pN + r$ avec $r = m \% N$, la division euclidienne de m par N .

$$\begin{aligned} \left| \sum_{k=1}^m \chi(k) \right| &= \left| \sum_{k=0}^m \chi(k) \right| = \left| \sum_{i=0}^p \left(\sum_{h=iN}^{(i+1)N-1} \chi(h) \right) + \sum_{h=pN}^{pN+r} \chi(h) \right| = \left| 0 + \sum_{h=pN}^{pN+r} \chi(h) \right| \\ &= \left| \sum_{h=0}^r \chi(h + pN) \right| = \left| \sum_{h \in \mathcal{P}_N, h \leq r} \chi(h) \right| = \left| \sum_{h \in \mathcal{P}_N, h \leq r} 1 \right| \leq \text{card}(\mathcal{P}_N) = \varphi(N) \end{aligned}$$

$$\left| \sum_{k=1}^m \chi(k) \right| \leq \varphi(N)$$

5. (a) On dit que \mathbb{R} est complet :

Si (u_n) est une suite réelle : (u_n) converge si et seulement si (u_n) vérifie le critère de Cauchy

(b) Si (u_n) est à valeurs complexes,
Supposons que (u_n) vérifie le critère de Cauchy.

$\left|(\operatorname{Re}(u))_q - (\operatorname{Re}(u))_p\right| = |\operatorname{Re}(u_q - u_p)| \leq |u_q - u_p|$ et $\left|(\operatorname{Im}(u))_q - (\operatorname{Im}(u))_p\right| \leq |u_q - u_p|$,
alors $(\operatorname{Re}(u))_n$ et $(\operatorname{Im}(u))_n$ vérifient le critère de Cauchy (réelle),
et ainsi elles sont convergentes, donc (u_n) est convergente.

Réciproquement, si (u_n) est convergente,

$(\operatorname{Re}(u))_n$ et $(\operatorname{Im}(u))_n$ sont convergentes donc vérifient le critère de Cauchy (réelle),

puis comme $|u_q - u_p| \leq \left|(\operatorname{Re}(u))_q - (\operatorname{Re}(u))_p\right| + \left|(\operatorname{Im}(u))_q - (\operatorname{Im}(u))_p\right|$,

alors (u_n) vérifie le critère de Cauchy.

Si (u_n) est une suite complexe : (u_n) converge si et seulement si (u_n) vérifie le critère de Cauchy

Donc \mathbb{C} est également complet.

(c) On remarque que pour $k \geq 1$, $\chi(k) = S_k - S_{k-1}$,

puis on fait une transformation d'Abel (sorte d'intégration par parties, pour les sommes).

Soient $n \in \mathbb{N}^*$ et $q > p \geq n$:

$$\sum_{k=p}^q \frac{\chi(k)}{k} = \sum_{k=p}^q \frac{S_k - S_{k-1}}{k} = \sum_{k=p}^q \frac{S_k}{k} - \sum_{k=p}^q \frac{S_{k-1}}{k} = \sum_{k=p}^q \frac{S_k}{k} - \sum_{k=p-1}^{q-1} \frac{S_k}{k+1}$$

$$\sum_{k=p}^q \frac{\chi(k)}{k} = \sum_{k=p}^{q-1} S_k \left(\frac{1}{k} - \frac{1}{k+1} \right) + \frac{S_q}{q} - \frac{S_{p-1}}{p}$$

(d) Ainsi pour $q > p \geq n$,

$$\left| \sum_{k=p}^q \frac{\chi(k)}{k} \right| = \left| \sum_{k=p}^{q-1} S_k \left(\frac{1}{k} - \frac{1}{k+1} \right) + \frac{S_q}{q} - \frac{S_{p-1}}{p} \right|$$

$$\leq \sum_{k=p}^{q-1} \left| S_k \left(\frac{1}{k} - \frac{1}{k+1} \right) \right| + \frac{|S_q|}{q} + \frac{|S_{p-1}|}{p} \leq \varphi(N) \left(\sum_{k=p}^{q-1} \left| \left(\frac{1}{k} - \frac{1}{k+1} \right) \right| + \frac{1}{q} + \frac{1}{p} \right)$$

Or $\frac{1}{k} - \frac{1}{k+1} \geq 0$, donc $\left| \left(\frac{1}{k} - \frac{1}{k+1} \right) \right| = \frac{1}{k} - \frac{1}{k+1}$ et donc

$$\left| \sum_{k=p}^q \frac{\chi(k)}{k} \right| \leq \varphi(N) \left(\sum_{k=p}^{q-1} \left(\frac{1}{k} - \frac{1}{k+1} \right) + \frac{1}{q} + \frac{1}{p} \right) = \frac{2\varphi(N)}{p} \leq \frac{2\varphi(N)}{n}$$

Or $\lim_{n \rightarrow \infty} \frac{2}{n} \varphi(N) = 0$,

donc pour tout $\epsilon > 0$, il existe $n \in \mathbb{N}^*$ tel que $\forall q > p \geq m$, $\left| \sum_{k=p}^q \frac{\chi(k)}{k} \right| \leq \epsilon$.

Donc la suite $(T_n)_{n \in \mathbb{N}}$ vérifie le critère de Cauchy.

(e) Elle est donc convergente dans \mathbb{C} :

la suite $\left(\sum_{k=1}^n \frac{\chi(k)}{k} \right)_{n \geq 1}$ est convergente