Exercice 1 (e3a)

Partie A.

1. ϕ est continue sur le segment $[0,T]$ et donc bornée sur ce segment. Par ailleurs, ϕ est T-périodique et donc $\phi(\mathbb{R}) = \phi([0,T])$. $\boxed{\phi \text{ est finalement bornée sur } \mathbb{R}}$.

2. La périodicité de ϕ s'écrit

$$\forall x \in \mathbb{R},\ \phi(x+T) = \phi(x)$$

En dérivant cette relation (ce que l'on peut faire si ϕ est dérivable) on obtient

$$\forall x \in \mathbb{R},\ \phi'(x+T) = \phi'(x)$$

et $\boxed{\phi' \text{ est donc } T\text{-périodique}}$.

3. On vérifie le critère des sous-groupes.

- P_ϕ est inclus dans $\mathbb{R}$ et non vide (il contient 0).
- Soient $T, T' \in P_\phi$. On a alors

$$\forall x \in \mathbb{R},\ \phi(x+(T+T')) = \phi((x+T)+T') = \phi(x+T) = \phi(x)$$

et $T+T' \in P_\phi$.

- Soit $T \in \mathbb{R}$; on a

$$\forall x \in \mathbb{R},\ \phi(x-T) = \phi(x-T+T) = \phi(x)$$

et donc $-T \in P_\phi$.

$\boxed{P_\phi \text{ est donc un sous-groupe de } (\mathbb{R},+)}$.

4. Soit $x \in \mathbb{R}$, par critère séquentiel de la limite en $+\infty$, $(\phi(x+nT))$ converge vers $L = \lim\limits_{t\to+\infty} \phi(t)$. Or pour tout entier n, on $\phi(x+nT) = \phi(x)$, par unicité de la limite, $\phi(x) = L$ et donc $\boxed{\phi \text{ est constante sur } \mathbb{R}}$.

Partie B.

1. Si y est T-périodique alors y' et y'' le sont par **A.2.** et $f = y'' - 2y' + 2y$ **<u>l'est encore</u>**. En contraposant ce résultat, $\boxed{(E_f) \text{ n'admet pas de solution périodique si } f \text{ n'est pas périodique}}$.

2. (E_0) est linéaire du second ordre et à coefficients constants. Son équation caractéristique est $r^2 - 2r + 2 = 0$. Les solutions sont $1+i$ et $1-i$. D'après le cours, l'ensemble des solutions est

$$\boxed{Vect\Big(\ x \longmapsto e^x\cos(x)\ \ ,\ \ x \longmapsto e^x\sin(x)\ \Big)}$$

Soit y une solution périodique de (E_0). Il existe des constantes c et d telles que

$$\forall x \in \mathbb{R},\ y(x) = e^x(c.\cos(x) + d.\sin(x))$$

Par ailleurs, y est bornée (question **A.1.**) et les suites $\Big(y(2n\pi)\Big)_{n\in\mathbb{N}}$ et $\Big(y(2n\pi+\pi/2)\Big)_{n\in\mathbb{N}}$ le sont donc aussi. Ceci impose $c = d = 0$ et y est la fonction nulle. La réciproque est immédiate et $\boxed{\text{la fonction nulle est donc la seule solution périodique de } (E_0)}$.

3. On cherche une solution particulière sous la forme $x \longmapsto \alpha\cos(x) + \beta\sin(x)$. En remplaçant dans l'équation, on constate qu'il suffit que $\begin{cases} \alpha - 2\beta = 1 \\ 2\alpha + \beta = 0 \end{cases}$

Il suffit donc de choisir $\alpha = 1/5$ et $\beta = -2/5$. La solution générale de (E_c) est donc

$$\left(x \longmapsto \frac{\cos(x) - 2\sin(x)}{5}\right) + Vect(x \longmapsto e^x\cos(x), x \longmapsto e^x\sin(x))$$

La solution particulière trouvée $y_0 : x \longmapsto \dfrac{\cos(x) - 2\sin(x)}{5}$ est 2π-périodique. Soit y_1 est une (autre) solution périodique. Il existe des constantes c et d telles que

$$\forall x \in \mathbb{R},\ y(x) = y_0(x) + e^x(c.\cos(x) + d.\sin(x))$$

Comme à la question précédente, le caractère borné de y_1 impose $c = d = 0$ et donc $y_1 = y_0$. $\boxed{y_0 \text{ est ainsi l'unique solution périodique de } (E_c)}$.

Remarque : On pouvait aussi chercher une solution particulière sous la forme $x \longmapsto e^{ix}$ et prendre la partie réelle.

Partie C.

1.a.

i) On a z deux fois dérivable et

$$\forall x \in \mathbb{R},\ z'(x) = y'(x+T)\ \text{ et }\ z''(x) = y''(x+T)$$

On en déduit que

$$\forall x \in \mathbb{R},\ z''(x) - 2z'(x) + 2z(x) = f(x+T) = f(x)$$

et $\boxed{z \text{ est donc solution de } (E_f)}$.

ii) Si y est T-périodique alors y' l'est aussi et $y(0) = y(T)$, $y'(0) = y'(T)$. Réciproquement, si ces relations ont lieu alors y et z sont deux solutions de (E_f) qui ont même valeur et même

valeur de dérivée en 0. Par théorème de Cauchy-Lipschitz linéaire, y et z sont égales. Ainsi

$$\forall x \in \mathbb{R},\ y(x) = z(x) = y(x+T)$$

et y est T-périodique. On conclut donc à l'équivalence demandé.

1.b. Soit g une solution pariculière de (E_f). En notant $\phi_1(t) = e^t\cos(t)$ et $\phi_2(t) = e^t\sin(t)$, on sait que la solution générale de (E_f) s'écrit

$$y_{c,d} : t \longmapsto g(t) + c\phi_1(t) + d\phi_2(t)$$

On veut prouver l'existence de constantes c et d telles que $y_{c,d}$ vérifient les conditions de $1.a.ii$. En remplaçant, $y_{c,d}$ par son expression, on tombe sur un système vérifié par (c,d) dont la matrice est $M = \begin{pmatrix} 1-e^T\cos(T) & -e^T\sin(T) \\ 1-e^T\cos(T)+e^T\sin(T) & 1-e^T\sin(T)-e^T\cos(T) \end{pmatrix}$
Le calcul donne $\det(M) = 1 - 2e^T\cos(T) + e^{2T} = (e^T-1)^2 + 2e^T(1-\cos(T))$. Comme $T > 0$, ce déterminant est non nul et le système admet une solution convenable.

Il y a donc bien une solution périodique. *Remarque : le raisonnement permet de prouver aussi l'unicité.*

2.a.i) Soit $x \in \mathbb{R}$. P_f étant dense dans $\mathbb{R}$, on peut trouver une suite $(t_n)_{n\in\mathbb{N}}$ d'éléments de P_f qui converge vers x. Comme $t_n \in P_f$, $f(0) = f(t_n)$, un passage à la limite donne, par critère séquentiel, (f étant continue) $f(0) = f(x)$.

Ceci a lieu pour tout x et donc f est donc constante.

2.a.ii) $x \longmapsto \dfrac{f(0)}{2}$ est solution particulière de (E_f) et la solution générale de (E_f) est alors

$$\left(x \longmapsto \frac{f(0)}{2}\right) + Vect(x \longmapsto e^x\cos(x), x \longmapsto e^x\sin(x))$$

Comme en partie B, la seule solution bornée est $x \longmapsto \dfrac{f(0)}{2}$ et c'est donc la seule solution périodique envisageable. Réciproquement, c'en est bien une (on a d'ailleurs l'existence par $C.1$).

2.b. i) D'après la question $B.1$, T_1 et T_2 sont des périodes de f et sont donc dans P_f. **ii)** Il existe donc des entiers non nuls q_1 et q_2 tels que $T_1 = aq_1$ et $T_2 = aq_2$. $T = aq_1q_2$ est alors une période commune à y_1 et y_2.

iii) $y_1 - y_2$ est alors aussi T-périodique. Mais c'est une solution de (E_0) et la partie B donne $y_1 = y_2$.

Mines MP2 -2002

DS n°11

I 1) $Q \geq 2$ donc $\exists p$ 1er qui divise Q et il est clair que $\forall i \in [\![1,n]\!]$ $p_i \neq q$ donc $p > p_n > \cdots > p_1$. Si l'ensemble des nombres 1ers était fini on aurait $\mathcal{P} = \{p_1, \cdots, p_n\}$ et $p \notin \mathcal{P}$ bien que 1er : absurde donc $\mathcal{P}$ infini

I 2 a) C'est une somme de série géométrique de raison :

$q = \frac{1}{n^s} \in [0, \frac{1}{2^s}] \subset [0,1[$ comme $\sum_{n=0}^{\infty} q^n = \frac{1}{1-q}$

$\frac{1}{2^s} = e^{-s\ln 2} < 1$ car $s > 0$

donc $\boxed{\left(1 - \frac{1}{n^s}\right)^{-1} = \sum_{k=0}^{\infty} \frac{1}{n^{ks}}}$

b) Comme $u_{ij} \geq 0$, $\left(\sum u_{ij}\right)_{(i,j)\in\mathbb{N}^2}$ est sommable ssi

$\forall i \left(\sum_{j=0}^{\infty} u_{ij}\right)$ existe et $\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} u_{ij}\right)$ existe :

$\forall i$ $\sum_{j=0}^{\infty} u_{ij} = \frac{1}{a^{is}}\left(1 - \frac{1}{b^s}\right)^{-1}$ d'après la a)

et $\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} u_{ij}\right) = \left(1 - \frac{1}{b^s}\right)^{-1}\left(1 - \frac{1}{a^s}\right)^{-1}$ tjs avec la a)

d) $\left(\sum_{(i,j)\in\mathbb{N}^{*2}} u_{ij}\right)$ sommable et $S = \left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1}$

c) Posons $\varphi : \mathbb{N}^n \longrightarrow \Pi_n$

$$(\alpha_1,\dots,\alpha_n) \longmapsto p_1^{s\alpha_1}\dots p_n^{s\alpha_n}$$

si $\varphi(\alpha_1,\dots,\alpha_n) = \varphi(\beta_1,\dots,\beta_n)$

$\Rightarrow p_1^{s\alpha_1}\dots p_n^{s\alpha_n} = p_1^{s\beta_1}\dots p_n^{s\beta_n}$

$\Rightarrow p_1^{\alpha_1}\dots p_n^{\alpha_n} = p_1^{\beta_1}\dots p_n^{\beta_n}$ car $x \longmapsto x^s$ injective sur $\mathbb{R}^+$

En vertu de l'unicité de la décomposition de $\mathbb{N}$ en facteurs 1ers on a : $\alpha_i = \beta_i$ $\forall i \in [\![1,n]\!]$

$(\alpha_1,\dots,\alpha_n) = (\beta_1,\dots,\beta_n)$ et $\boxed{\varphi \text{ injective}}$

φ est clairement surjective d'où φ bijective. On $\mathbb{N}^n$ est dénombrable donc Π_n aussi d'où $\exists (q_k)$ suite de $\mathbb{N}$ t.q. $\Pi_n = \{q_k^s, k\in\mathbb{N}^*\}$

Considérons $N_1 = \{q_h, h\in\mathbb{N}^*\}$

Comme $N_1 \subset \mathbb{N}$, $m_1' = \min N_1$ existe puis $N_1 - \{m_1'\} \subset \mathbb{N}$ et non vide donc $m_2' = \min(N_1 - \{m_1'\})$ existe et $m_1' < m_2'$

et par récurrence on construit $m'_{p+1} = \min\left(N_n - \{m'_1, \dots, m'_p\}\right)$

d'où $N_n = \{m'_1 < m'_2 < \dots\}$ et en posant $m_i = (m'_i)$ il

vient $\boxed{\Pi_n = \{m_1 < m_2 < m_3 < \dots\}}$

Si $\delta = 1$ et $n = 2$ $\Pi_2 = \{2^{\alpha_1} \times 3^{\alpha_2},\ (\alpha_1, \alpha_2) \in \mathbb{N}^2\}$

d'où $\boxed{\text{si } \delta = 1 \text{ et } n = 2 : \Pi_2 = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27 \dots\}}$

de même $\boxed{\delta = 1 \text{ et } n = 3 : \Pi_3 = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, \dots\}}$

d) $\forall k \in [\![2, n]\!]$ k se décompose en produit de nb 1^{er} : q

et $q \leq k \leq n$ donc $q \leq P_N$ d'où $k^\delta \in \Pi_N$

Donc $\boxed{\sum_{k=1}^{n} \frac{1}{k^\delta} \leq \sum_{m \in \Pi_N} \frac{1}{m} = \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^\delta}\right)^{-1}}$

Pour $\underline{\delta = 1}$: $\sum_{k=1}^{n} \frac{1}{k} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right)^{-1}$

Supposons $\mathcal{P}$ fini. Alors $\exists N_0 \in \mathbb{N} \mid \forall k \in \mathbb{N}\ k^1 = k \in \Pi_{N_0}$

et donc $\forall n \geq 1$ $S_n = \sum_{k=1}^{n} \frac{1}{k} \leq K_0 = \prod_{i=1}^{N_0} \left(1 - \frac{1}{p_i}\right)^{-1}$

d'où (S_n) majorée : Absurde car $\lim_{n \to \infty} S_n = +\infty$ et $\boxed{\mathcal{P} \text{ infini}}$

on sait que $\forall \delta \in]0,1]$ $\lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{k^\delta} = +\infty$ (série de Riemann)

d'autre part, on a $p_N \leq p_N < p_{N+1}$ d'où avec $n = p_N$ et d)

on a : $f_n(\delta) \geq \sum_{k=1}^{p_N} \frac{1}{k^\delta} \geq \sum_{k=1}^{N} \frac{1}{k^\delta}$ car $\forall N \in \mathbb{N}^*$ $p_N \geq N$

(La à refaire ! par récurrence)

on a donc $f_{p_N}(\delta) \geq \sum_{k=1}^{N} \frac{1}{k^\delta} \xrightarrow[N\to\infty]{} +\infty$. En fait il est clair

que la suite $(f_n(\delta))_{n\in\mathbb{N}}$ est croissante. Par TLM et suite extraite

on conclut : $\boxed{\lim_{n\to\infty} f_n(\delta) = +\infty}$

e) La première inégalité découle de d). Pour la 2ème :

$$\prod_{i=1}^{N} \left(1 - \frac{1}{p_i^\delta}\right)^{-1} = \sum_{m \in \Pi_N} \frac{1}{m^\delta} \leq \sum_{k=1}^{\infty} \frac{1}{k^\delta} \quad \text{car } \Pi_N \subset \{k^\delta, k \in \mathbb{N}^*\}$$

d'où $\boxed{\sum_{k=1}^{N} \frac{1}{k^\delta} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^\delta}\right)^{-1} \leq \sum_{k=1}^{\infty} \frac{1}{k^\delta}}$

On a donc $\forall N \geq 1$: pour $n = p_N$

$$\sum_{k=1}^{N} \frac{1}{k^\delta} \leq \sum_{k=1}^{p_N} \frac{1}{k^\delta} \leq f_N(\delta) \leq \sum_{k=1}^{\infty} \frac{1}{k^\delta} = \zeta(\delta)$$

$N \to \infty$ (gauche), $N \to \infty$ (droite), $N \to \infty$ (milieu) $\to \zeta(\delta)$

Par th. d'encadrement : $\boxed{\lim_{n\to\infty} f_n(\delta) = \sum_{k=1}^{\infty} \frac{1}{k^\delta}}$

I 3) Pour $\delta = 1$, le d) donne :

$$f_N(1) \geq \sum_{k=1}^{P_N} \frac{1}{k} \geq \sum_{k=1}^{N} \frac{1}{k} \quad \text{d'où} \quad \ln f_N(1) \geq \ln(S_N) \text{ et } S_N = \sum_{k=1}^{N} \frac{1}{k}$$

et $\ln(f_N(1)) = -\sum_{i=1}^{N} \ln\left(1 - \frac{1}{p_i}\right) = -\sum_{i=1}^{N} v_i \geq \ln(S_N) \xrightarrow[N\to\infty]{} +\infty$

d'où $\lim\limits_{N\to\infty} \sum_{i=1}^{N} v_i = -\infty$ et $\boxed{(\Sigma v_i) \text{ diverge}}$

Enfin $v_i \sim \frac{-1}{p_i} \leq 0$ d'où, par TC, $\boxed{(\Sigma w_i) \text{ diverge}}$

csq : $\boxed{\text{Les nb } 1^{\text{ers}} \text{ restent assez nombreux dans } \mathbb{N}, \text{ sinon } (\Sigma w_i) \text{ serait convergente}}$

I 4) (Ultra-classique) $u_k(\delta) = \frac{1}{k^\delta}$ on a :

* $\forall k \in \mathbb{N}^*$ u_k C' sur $\mathcal{D} =]1, +\infty[$

* (Σu_k) converge simplement vers ζ sur $\mathcal{D}$

* $\forall 1 < a < b$, $\forall \delta \in [a, b]$ $|u_k'(\delta)| = \left|\frac{\ln k}{k^\delta}\right| \leq \frac{\ln k}{k^a} = a_k$

et $\frac{\ln k}{k^a} = o\left(\frac{1}{k^\alpha}\right)$ avec $1 < \alpha < a$: par ex. $\alpha = \frac{a+1}{2}$

d'où (Σa_k) cvg et (Σu_k) cvg normalement / $[a, b]$

Par Th 2, on conclut : $\boxed{\{c'm]1, +\infty[}$

Deuxième partie

II 1 a)

n	N	P_N	P_n	4^n
2	1	2	2	16
3	2	3	6	64
4	2	3	6	256
5	3	5	30	1024

b) Si $n+1$ n'a. 1$^{\text{a}}$ alors

si $P_N \leq n < P_{N+1}$ on a :

$P_N \leq n < n+1 < P_{N+1}$

d'où $\boxed{P_{n+1} = P_n \leq 4^n \leq 4^{n+1}}$

c) * $n \geq 2 \Rightarrow n+2 \geq 3$ donc si $n+1$ est premier i.e est impair d'où $\boxed{\exists m \in \mathbb{N} \setminus \; n+1 = 2m+1}$

$$\binom{2m+1}{m} = \frac{(2m+1)(2m)(2m-1)\cdots(m+2)}{m \times (m-1) \times \cdots \times 1} = \frac{(n+1)(2m)(2m-1)\cdots(m+2)}{m \times (m-1) \times \cdots \times 1}$$

* Soit p 1$^{\text{er}}$, $p \in [\![m+2, n+1]\!]$ $\exists k \in \mathbb{N} \setminus \binom{2m+1}{m} = \frac{pk}{m!}$

d'où $m! \binom{2m+1}{m} = pk$ donc $p \mid m! \binom{2m+1}{m}$ or

$p \wedge m! = 1$ (sinon $p \wedge m! = p$ d'où $p \mid m!$, absurde)

par le lemme de Gauss : $\boxed{p \mid \binom{2m+1}{m}}$

* $\binom{2\times 0+1}{0} = 1 \leq 4^0$, $\binom{2\times 1+1}{1} = 3 \leq 4$

supposons $\binom{2m+1}{m} \leq 4^m$, $\binom{2m+3}{n+1} = \frac{(2m+3)(2m+2)(2m+1)!}{(m+1)\,m!\,(m+2)!}$

d'où $\binom{2n+3}{n+1} = \binom{2n+1}{n} \times \frac{(2n+3)(2n+2)}{(n+1)(n+2)}$

or $\binom{2n+1}{n} \leq 4^n$ et $\frac{(2n+3)(2n+2)}{(n+1)(n+2)} - 4 = \frac{-2}{n+2} \leq 0$

d'où $\binom{2n+3}{n+1} \leq 4^n \times 4 = 4^{n+1}$ on conclut par récurrence :

$$\boxed{\forall n \in \mathbb{N} \quad \binom{2n+1}{n} \leq 4^n}$$

* $P_{n+1} = P_{n+1} \times q_1 \times q_2 \times \cdots \times q_k$ où $q_1, \dots, q_k$ sont les nombres 1^n compris entre $n+2$ et $n+1 = 2n+1$

Comme $\forall i \in [\![1, k]\!]$ $q_i \mid \binom{2n+1}{n}$. Comme les q_i sont 1^n distincts, ils sont 2 à 2 1^n entre eux d'où

$q_1 \times \cdots \times q_k \mid \binom{2n+1}{n} \neq 0$ donc $q_1 \times \cdots \times q_k \leq \binom{2n+1}{n} \leq 4^n$

d'où $P_{n+1} \leq P_{n+1} \times 4^n \leq 4^{n+1} \times 4^n = 4^{2n+1} = 4^{n+1}$

d'où $\boxed{P_{n+1} \leq 4^{n+1} \Rightarrow P_{n+1} \leq 4^{n+1}}$

d) Vu le tableau de a) H_n : "$P_n \leq 4^n$" est vraie pour $n = 2$. Supposons H_i vraie jusqu'au rang $n \geq 2$

→ si $n+1$ non 1^n $P_{n+1} = P_n \leq 4^{n+1}$ d'où H_{n+1} vraie

→ si $n+1$ est 1^n : $n+1 \geq 3 \Rightarrow 2n+1 \geq 3 \Rightarrow n \geq 1 \Rightarrow n+1 \geq 2$

et $m+1 \leqslant n$ car $n-(m+1) = 2m+1-1-(m+1) = m-1 \geqslant 0$

donc $m+1 \in [\![2, n]\!]$ on peut donc utiliser H_{m+1}

soit : $P_{m+1} \leqslant 4^{m+1}$ et d'après le c) $P_{n+1} \leqslant 4^{n+1}$

d'où H_{n+1} vraie et : $\boxed{\forall n \geqslant 2 \quad P_n \leqslant 4^n}$

II 2) On décompose $1, 2, 3, \dots, n$ en produit de facteurs 1^{er}. Ces facteurs 1^{er} sont parmi $p_1, \dots, p_N$

$\forall i \in [\![1, n]\!]$ $i = p_1^{\alpha_{i,1}} p_2^{\alpha_{i,2}} \cdots \times p_N^{\alpha_{i,N}}$ et $\forall i,j$:

$\alpha_{i,j} \geqslant 0$ (exemple : $10 = p_1^1 \times p_2^0 \times p_3^1 \times \dots \times p_N^0$)

on sait que $d_n = p_1^{\gamma_1} \times \dots \times p_N^{\gamma_N}$ avec $\forall j \in [\![1, N]\!]$: $\gamma_j = \max_{1 \leqslant i \leqslant n} (\alpha_{i,j})$

Montrons que $\gamma_j = a_j = \left[\dfrac{\ln n}{\ln p_j} \right]$

on a $p_j^{\gamma_j} \leqslant n$ (car $\forall i,j$ $p_i^{\alpha_{i,j}} \leqslant n$ et $\gamma_j = \max(\dots)$)

d'où $\begin{cases} \gamma_j \ln p_j \leqslant \ln n \\ \ln p_j \geqslant \ln 2 > 0 \end{cases} \Rightarrow \gamma_j \leqslant \dfrac{\ln n}{\ln p_j}$ (1)

d'autre part $p_j^{\gamma_j + 1} > n$ sinon $p_j^{\gamma_j+1} \in [\![1, n]\!]$ et on aurait $\gamma_{j+1} > \max_{1 \leqslant i \leqslant n} (\alpha_{i,j}) \geqslant \alpha_{i_0, j} = \gamma_{j+1}$ avec $i_0 = p_j^{\gamma_j+1}$

Absurde !

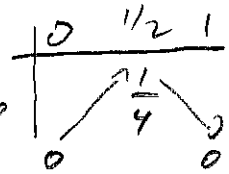
d'où $p_j^{\gamma_j+1} > n \Rightarrow \gamma_j + 1 > \dfrac{\ln n}{\ln p_j}$ (2)

---

(1) et (2) donne $\left\{ \gamma_j \leq \dfrac{\ln n}{\ln p_j} < \gamma_j + 1 \right.$

d'où $\boxed{\forall j \in [\![1, N]\!] \ \gamma_j = \alpha_j = \left[\dfrac{\ln n}{\ln p_j} \right] \text{ et } d_n = \prod_{i=1}^{N} p_i^{\alpha_i}}$

II 3 a) Etudions $\varphi(x) = x(1-x)$ $\varphi'(x) = 1 - 2x$ d'où



d'où $I_n = \int_0^1 \varphi(x)^n \, dx \leq \int_0^1 \left(\frac{1}{4}\right)^n dx = \left(\frac{1}{4}\right)^n$

↳ car $0 \leq \varphi(x) \leq 1/4$

d'où $\boxed{I_n \leq \dfrac{1}{4^n}}$

b) * Si $k \in [\![0, n]\!]$, alors $n+k+1 \in [\![n+1, 2n+1]\!] \subset [\![1, 2n+1]\!]$

d'où comme $\forall i \in [\![1, 2n+1]\!]$ i divise d_{2n+1} (définition du ppcm !)

on a : $\boxed{\forall k \in [\![0, n]\!] \ n+k+1 \text{ divise } d_{2n+1}}$

* $(1-x)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^k$ d'où $I_n = \int_0^1 \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^{k+n} \, dx$

d'où $d_{2n+1} I_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \dfrac{d_{2n+1}}{n+k+1}$

et $\forall k \in [\![0, n]\!] \ \dfrac{d_{2n+1}}{n+k+1} \in \mathbb{Z}$ car $n+k+1$ divise d_{2n+1}

donc par somme produit $d_{2n+1} I_n \in \mathbb{Z}$

or il est clair que $I_n \geq \int_0^1 0 = 0$

d'où $\boxed{d_{2n+1} I_n \in \mathbb{N}}$

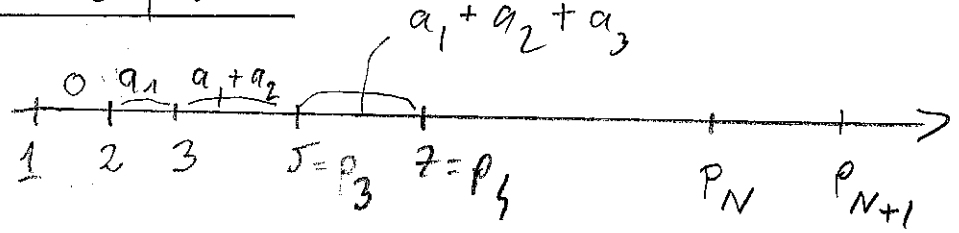
En fait $I_n > 0$ car $\forall x \in]0,1[\; x^n(1-x^n) > 0$

d'où $d_{2n+1} I_n = k \geq 1$ d'où $d_{2n+1} \geq \frac{1}{I_n} \geq 4^n$

d'où $\boxed{\forall n \in \mathbb{N} \quad d_{2n+1} \geq 4^n}$

Troisième partie

III 1



H_A est constante donc continue sur $[1,2[$ et sur chaque $]p_N, p_{N+1}[$, $\forall N \in \mathbb{N}^*$

en 2 : $\lim\limits_{\substack{n \to 2 \\ <}} H_A(n) = 0$ et $\lim\limits_{\substack{n \to 2 \\ >}} H_A(n) = H_A(2)$
$= H_A(2) - a_1$

en p_N, $N \geq 1$: H_A constante sur $[p_N, p_{N+1}[$ donc :

H_A continue à droite en p_N et à gauche :

$\lim\limits_{\substack{n \to p_N \\ <}} H_A(n) = H_A(p_{N-1}) = H_A(p_N - 0) = H_A(p_n) - a_N$

d'où H continue en p_N ssi $a_N = 0$

d :

H c° à droite en $[1, +\infty[$

H c° sur $[1,+\infty[\setminus \{ p_N , N \geq 1 \text{ et } a_N \neq 0 \}$

$\forall N \geq 1 \quad H_a(p_N) - H_a(p_N - 0) = a_N$

$$\forall x \in [p_N, p_{N+1}[: \int_2^x H_A(t) f'(t) dt = \sum_{i=1}^{N-1} \int_{p_i}^{p_{i+1}} H_A(t) f'(t) dt + \int_{p_N}^{x} H_A(t) f'(t) dt$$

$$\text{donc } \int_2^x H_A(t) f'(t) dt = \sum_{i=1}^{N-1} H_A(p_i) \int_{p_i}^{p_{i+1}} f'(t) dt + H_A(p_N) \int_{p_N}^{x} f'(t) dt$$

$$= \sum_{i=1}^{N-1} H_A(p_i) (f(p_{i+1}) - f(p_i)) + H_A(p_N) (f(x) - f(p_N))$$

$$= \sum_{i=1}^{N-1} H_A(p_i) f(p_{i+1}) - \sum_{i=1}^{N-1} H_A(p_i) f(p_i) + H_A(x) f(x) - H_A(p_N) f(p_N)$$

$$= \sum_{i=2}^{N} H_A(p_{i-1}) f(p_i) - \sum_{i=1}^{N-1} H_A(p_i) f(p_i) - H_A(p_N) f(p_N) + H_A(x) f(x)$$

"$i = i+1$"

$$= \sum_{i=2}^{N-1} \left[H_A(p_{i-1}) - H_A(p_i) \right] f(p_i) + H_A(p_{N-1}) f(p_N) - \underbrace{H_A(p_1) f(p_1)}_{a_1} - H_A(p_N) f(p_N) + H_A(x) f(x)$$

$H_A(p_{i-1}) - H_A(p_i) = -a_i$

$$= - \sum_{i=2}^{N-1} a_i f(p_i) - a_N f(p_N) - a_1 f(p_1) + H_A(x) f(x)$$

d'où $\int_2^x H_A(t) f'(t) dt = - \sum_{i=1}^{N} a_i f(p_i) + H_A(x) f(x)$

d'où $\boxed{\sum_{i=1}^{N} a_i f(p_i) = H_A(x) f(x) - \int_2^x H_A(t) f'(t)\,dt}$ (12)

Remarque : On a utilisé la Transformation d'Abel :

La voyez-vous ?

III 2 a) On a vu au II 1 d) que $\forall n \geq 2 \quad \prod_{i=1}^{N} p_i \leq 4^n$

donc $\forall n \geq 2 \quad \sum_{i=1}^{N} \ln p_i \leq n \ln 4$ avec $p_N \leq n < p_{N+1}$

d'où $\forall x \geq 2 \quad \theta(x) = \sum_{i=1}^{N} \ln p_i$ avec $p_N \leq x < p_{N+1}$

$= \theta(p_N) \leq p_N \ln 2$ avec $n = p_N$

$\leq x \ln 4$ d'où $\boxed{\forall x \geq 2 \quad \theta(x) \leq x \ln 4}$

b) Soit $x \geq 2$, avec $p_N \leq x < p_{N+1}$:

$$\sum_{i=1}^{N} \ln p_i \times \frac{1}{\ln p_i} = H_A(x) \frac{1}{\ln x} - \int_2^x H_A(t) f'(t)\,dt$$

$$\Rightarrow \sum_{i=1}^{N} 1 = \pi(x) = \left(\sum_{i=1}^{N} \ln p_i\right) \frac{1}{\ln x} - \int_2^x H_A(t) f'(t)\,dt$$

$$= \theta(x) \frac{1}{\ln x} - \int_2^x \theta(t) \left(\frac{-1}{t(\ln t)^2}\right) dt$$

$$\leq x \ln 4 \frac{1}{\ln x} + \int_2^x t \ln 4 \frac{1}{t(\ln t)^2}\,dt$$

donc $\boxed{\pi(x) \leqslant \ln 4 \left(\frac{x}{\ln x} + \int_2^x \frac{dt}{(\ln t)^2} \right)}$

c) $\forall x \geqslant 4 \quad : 0 \leqslant \frac{\ln x}{x} \left[\int_2^{\sqrt{x}} \frac{dt}{(\ln t)^2} + \int_{\sqrt{x}}^x \frac{dt}{(\ln t)^2} \right]$ (car $\sqrt{x} < x$)

$$\leqslant \frac{\ln x}{x} \left((\sqrt{x} - 2) \frac{1}{(\ln 2)^2} + (x - \sqrt{x}) \frac{1}{(\ln \sqrt{x})^2} \right)$$

car $t \longmapsto \frac{1}{(\ln t)^2}$ décroissante $/ [2, +\infty[$

d'où $0 \leqslant R(x) \leqslant \frac{\ln x}{x} \left[\frac{\sqrt{x}}{(\ln 2)^2} + x \frac{1}{(\frac{1}{2} \ln x)^2} \right]$

$$\leqslant \frac{\ln x}{\sqrt{x} (\ln 2)^2} + \frac{4}{(\ln x)} \xrightarrow[x \to +\infty]{} 0 + 0 = 0$$

Par th. d'encadrement : $\boxed{\lim_{x \to +\infty} R(x) = 0}$

d) $\forall x \geqslant 4 \quad \pi(x) \leqslant \ln 4 \frac{x}{\ln x} [1 + R(x)]$

et $\exists x_0 \geqslant 4 \mid \forall x \geqslant x_0 \quad 0 \leqslant R(x) \leqslant 1 = \varepsilon$

comme $\ln 4 = \ln 2^2 = 2 \ln 2$ on a : $\boxed{\forall x \geqslant x_0 \quad \pi(x) \leqslant 4 \ln 2 \frac{x}{\ln x}}$

III 3) d'après II 2) et II 3) on a :

$$d_{2n+1} = \prod_{i=1}^{N'} p_i^{\alpha_i} \geq 4^n \quad \text{avec} \quad p_{N'} \leq 2n+1 < p_{N'+1}$$

d'où $n \ln 4 \leq \ln(d_{2n+1}) = \sum_{i=1}^{N'} \alpha_i \ln p_i \leq \sum_{i=1}^{N'} \frac{\ln(2n+1)}{\ln p_i} \times \ln p_i$

$$\Rightarrow n \ln 4 \leq \ln(2n+1) \sum_{i=1}^{N'} 1 = \ln(2n+1)\, \pi(2n+1)$$

$$\Rightarrow \pi(2n+1) \geq \frac{n \ln 4}{\ln(2n+1)} = \frac{2 \ln 2\, n}{\ln(2n+1)}$$

Soit $\underline{n > 5}$: $\exists!\, n \geq 2 \setminus 2n+1 \leq n < 2n+3$
(↳ voir le II 3))

d'où $\pi(n) \geq \pi(2n+1) \geq \frac{2 \ln 2\, n}{\ln(2n+1)} \geq \frac{2 \ln 2 \left(\frac{n-3}{2}\right)}{\ln n}$

d'où $\pi(n) \geq \frac{\ln 2}{\ln n}(n-3) = \frac{\ln 2}{\ln n}\, n \left(\frac{n-3}{n}\right)$

et comme $\lim_{n \to +\infty} \frac{n-3}{n} = 1$, $\exists\, n_1 \geq 5 \setminus \forall n \geq n_1 : \frac{n-3}{n} \geq \frac{1}{2}$

d'où $\boxed{\forall n \geq n_1 \quad \pi(n) \geq \frac{\ln 2}{2} \frac{n}{\ln n}}$

$\underline{cl}$: $\boxed{\exists (a, A) \in \mathbb{R}_+^* \;\; \exists\, n_2 \geq 5 \setminus \forall n \geq n_2 : \quad a \frac{n}{\ln n} \leq \pi(n) \leq A \frac{n}{\ln n}}$

Quatrième Partie

IV.1 Théorème d'Euler

a) Bezout : $a \wedge n = 1 \iff \exists (u,v) \in \mathbb{Z}^2 \mid au + nv = 1$

$\Rightarrow \bar{a}\bar{u} = \bar{1} \Rightarrow \bar{a}$ inversible dans $\mathbb{Z}/n\mathbb{Z}$

Réciproquement : si $\exists \bar{b} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{a}\bar{b} = \bar{1}$ alors :

$ab - 1 \in n\mathbb{Z} \Rightarrow \exists v \in \mathbb{Z} \mid ab - 1 = nv$

$\Rightarrow \exists v \in \mathbb{Z} \mid ab - nv = 1 \Rightarrow a \wedge n = 1$

d'où $\boxed{\bar{a} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} \iff a \wedge n = 1}$

n	2	3	4	5	6	7
$\varphi(n)$	1	2	2	4	2	6

b) $\bar{1} \in (\mathbb{Z}/n\mathbb{Z})^* = G$, la multiplication est associative

si $\bar{x}$ et $\bar{y}$ sont dans G alors $\bar{x}\bar{y} \in G$ (le faire !)

de même $\bar{x}^{-1}$ aussi (idem) d'où $\boxed{((\mathbb{Z}/n\mathbb{Z})^*, \times) \text{ groupe}}$

et $\boxed{\text{Card}(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)}$

γ est bijective car : $*\ \gamma(\bar{b}) = \gamma(\bar{c}) \Rightarrow \bar{b}\bar{a} = \bar{c}\bar{a}$

$\Rightarrow \bar{b}\bar{a}\bar{a}^{-1} = \bar{c}\bar{a}\bar{a}^{-1} \Rightarrow \bar{b} = \bar{c}$ donc γ injective

et $\forall \bar{y} \in (\mathbb{Z}/n\mathbb{Z})^*$, posons $\bar{b} = \bar{y}\bar{a}^{-1}$ on a $\gamma(\bar{b}) = \bar{y}$

d'où φ injective et donc φ bijective.

d'où $c = \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^*} \gamma(b) = \prod_{b=\gamma^{-1}(c)} \gamma(\gamma(c)) = \prod_{c \in (\mathbb{Z}/n\mathbb{Z})^*} c$

$c \in (\mathbb{Z}/n\mathbb{Z})^*$

on $c = \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{b}\,\bar{a} = \left(\prod_{b \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{b}\right) \bar{a}^{\varphi(n)} = c\,\bar{a}^{\varphi(n)}$

Comme $c \in (\mathbb{Z}/n\mathbb{Z})^*$ $c = c\,\bar{a}^{\varphi(n)} \Rightarrow cc' = c'\bar{a}^{\varphi(n)}$

$= 1\ \bar{a}^{\varphi(n)} = \bar{1}$

d'où $\boxed{a^{\varphi(n)} \equiv 1 \ (n)}$

c) Dans $\mathbb{Z}/6\mathbb{Z}$: $\overline{251^{311}} = \bar{5}^{311} = (\bar{-1})^{311} = \bar{-1}$!

d'où $\boxed{\text{le reste de } 251^{311} \text{ par 6 est 5}}$

rem. pour utiliser le b) on remarque que $251 \wedge 6 = 1$

d'où $251^{\varphi(6)} = 251^2 \equiv 1 \ (6)$ d'où $251^{311} = 251^{310} \times 251$

$\equiv 251 \equiv 5 \ (6)$

IV-2 a) $a \wedge n = 1 \iff a \wedge (pq) = 1$

$\iff p \nmid a$ et $q \nmid a$

d'où $a \wedge n \neq 1 \iff p \mid a$ ou $q \mid a$

cherchons dans $[\![1, n-1]\!]$ les entiers a tels que $a \wedge n \neq 1$

Il y a les multiples de p : $p, 2p, \dots, (q-1)p$; les multiples

de q : $q, 2q, \dots, (p-1)q$.

Ces 2 listes $\{p, 2p, \dots, (q-1)p\}$ et $\{q, 2q, \dots, (p-1)q\}$

sont disjointes (intersection vide) d'où :

$$\text{card}\{k \in [\![1, n-1]\!] \setminus k \wedge n \neq 1\} = q-1+p-1$$

d'où $\varphi(n) = \text{card}\{k \in [\![1, n-1]\!] \mid k \wedge n = 1\} = n-1-(q+p-2)$

$$= n-p-q+1 = (p-1)(q-1) \quad \text{car } n = pq$$

cl $\boxed{\varphi(n) = (p-1)(q-1)}$

b) Puisque $e \wedge (p-1)(q-1) = 1$, $\bar{e} \in (\mathbb{Z}/N\mathbb{Z})^*$ & $N = (p-1)(q-1)$

d'où $\exists \bar{d} \in (\mathbb{Z}/N\mathbb{Z}) \setminus \bar{e}\bar{d} = \bar{1}$

cl $\boxed{\exists d \in \mathbb{Z} \mid ed \equiv 1 \ ((p-1)(q-1))}$

$\bar{a}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{a}^{ed}$	0	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

avec $d \setminus 5d \equiv 1 \ (2)$ par exemple $\underline{d = 1}$:

$\bar{a}^{ed} = \bar{a}^5$. Si $a \wedge 6 = 1$ $\bar{a}^{\varphi(6)} = \bar{a}^2 = \bar{1}$ d'où $\bar{a}^5 = \bar{a}$

reste $\bar{a} = \bar{2}$ ou $\bar{a} = \bar{3}$ --- à la main.

c) c'est clair si $a \wedge n = 1$ car $a^{ed} = a^{1+\varphi(n)k} \equiv a \times 1 \ (n)$

Sinon montrons que avec $ed = 1 + \varphi(n)k = 1 + (p-1)(q-1)k$

on a $a^{ed} \equiv a \ (p)$ et $a^{ed} \equiv a \ (q)$

si $a \wedge p = 1$ $a^{ed} = a \times (a^{p-1})^{q-1} \equiv a \times 1^{q-1} \equiv a \ (p)$

si $a \wedge p \neq 1$ alors $p \mid a$ (p ne 1^{er}) d'où :

$$a^{ed} \equiv a \equiv 0 \ (p)$$

donc $\forall a \in \mathbb{Z}$ $a^{ed} \equiv a \ (p)$. Par symétrie :

on a $a^{ed} \equiv a \ (q)$ d'où p et q divise $a^{ed} - a$

comme $p \wedge q = 1$ (Gauss) $p \times q$ divise $a^{ed} - a$

soit $a^{ed} - a \equiv 0 \ (n = p \times q)$

d'où $\boxed{\forall a \in \mathbb{Z} \quad a^{ed} \equiv a \ (n)}$

Remarque : c'est le système à clé publique (RSA)