Mines - Ponts 2002 Mathématiques 2ème épreuve.

I.1) Supposons qu'il n'existe qu'un nombre fini de nombres premiers $\mathcal{P} = \{p_1, \dots, p_n\}$. Soit $Q = p_1 p_2 \dots p_n + 1$ est un entier qui possède un facteur premier p (car il vaut au moins 3), or Q est premier avec chacun des p_i donc p ne peut être un des p_i. Ceci contredit $p \in \mathcal{P}$. On a prouvé par l'absurde que l'ensemble des nombres premiers est infini.

I.2 a) $\alpha \frac{1}{n^\delta} < 1$ $\sum_{k=0}^{N} \frac{1}{n^{k\delta}} = \frac{1 - \left(\frac{1}{n^\delta}\right)^{N+1}}{1 - \frac{1}{n^\delta}}$, par passage à la limite on aura $\left(1 - \frac{1}{n^\delta}\right)^{-1} = \sum_{k=0}^{+\infty} \frac{1}{n^{k\delta}}$

I.2 b) La suite double $(u_{i,j})$ est une suite de termes positifs elle est sommable si et seulement si

$\forall i \quad \sum_{j \geq 0} u_{i,j}$ converge et $\sum_{i \geq 0} \left(\sum_{j=0}^{+\infty} u_{i,\delta} \right)$ converge.

on $\sum_{j \geq 0} \frac{1}{a^{i\delta} \beta^{j\delta}}$ converge vers $\frac{1}{a^{i\delta}} \frac{1}{\left(1 - \frac{1}{\beta^\delta}\right)}$ d'après I.2.a)

et $\sum_{i \geq 0} \frac{1}{a^{i\delta}} \frac{1}{\left(1 - \frac{1}{\beta^\delta}\right)}$ converge vers $\frac{1}{\left(1 - \frac{1}{a^\delta}\right)} \frac{1}{\left(1 - \frac{1}{\beta^\delta}\right)}$ toujours d'après I.2.a).

Donc $(u_{i,j})$ est sommable et $\sum_{(i,j) \in \mathbb{N}^2} u_{i,j} = \frac{1}{\left(1 - \frac{1}{a^\delta}\right)\left(1 - \frac{1}{\beta^\delta}\right)} = S$

I.2.c) - L'application $x \mapsto x^\delta$ de $\mathbb{N}^*$ vers $\mathbb{R}^{*+}$ est injective. Il suffit donc de prouver que $(\alpha_1, \dots, \alpha_n) \mapsto p_1^{\alpha_1} \dots p_n^{\alpha_n}$ est injective de $\mathbb{N}^n$ dans $\mathbb{N}^*$. Cette injectivité résulte de l'unicité de la décomposition d'un entier en facteurs premiers.

- $\delta = 1$ $n = 2$ $p_1 = 2$ $p_2 = 3$

$(m_i)_{i \in \mathbb{N}} = (1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, \dots)$

- $\delta = 1$ $n = 3$ $p_1 = 2$ $p_2 = 3$ $p_3 = 5$

$(m_i)_{i \in \mathbb{N}} = (1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, \dots)$

I.2.d) - Soit $k \leq n$ alors tout facteur premier de k est inférieur à N. Donc $\sum_{k=1}^{n} \frac{1}{k^s} \leq \sum_{m \in M_N} \frac{1}{m} = \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1}$.

- Si la suite des entiers premiers était limitée il existerait n_0 tel que pour n plus grand que n_0 N soit indépendant de n. La série à termes positifs $\sum_{k \geq 1} \frac{1}{k^s}$ aurait des sommes partielles majorées et serait convergente (pour tout s). Or pour $s = 1$ cette série diverge. Donc la suite des nombres premiers est illimitée.

- Pour la même raison, puisque $\sum_{k \geq 1} \frac{1}{k^s}$ est divergente pour s dans $]0,1]$. On aura $\lim_{n \to +\infty} f_{N_n}(s) = +\infty$.
or $(f_k(s))$ est croissante. car $\left(1 - \frac{1}{(p_i)^s}\right)^{-1} > 1$, donc $\lim_{n \to +\infty} f_n(s) = +\infty$.

I.2.e) Si $s > 1$ la série $\sum_{k \geq 1} \frac{1}{k^s}$ converge et $\forall p$ $\sum_{i=1}^{p} \frac{1}{m_i} \leq \sum_{k=1}^{m_p} \frac{1}{k^s} \leq \sum_{k=1}^{+\infty} \frac{1}{k^s}$

donc $\sum_{m \in M_n} \frac{1}{m} \leq \sum_{k=1}^{+\infty} \frac{1}{k^s}$, soit $f_N(s) \leq \sum_{k=1}^{+\infty} \frac{1}{k^s}$.

- On a déjà remarqué que $(f_n(s))_{n \in \mathbb{N}}$ est croissante. Puisqu'elle est majorée $(f_n(s))_{n \in \mathbb{N}}$ possède une limite en $+\infty$.
et $\forall n$. $\sum_{k=1}^{n} \frac{1}{k^s} \leq \lim_{n \to +\infty} f_n(s) \leq \sum_{k=1}^{+\infty} \frac{1}{k^s}$.

En faisant tendre n vers $+\infty$, on a bien $\sum_{k=1}^{+\infty} \frac{1}{k^s} = \lim_{n \to +\infty} f_n(s)$.

I.3) En prenant $s = 1$ on aura.

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

$$\ln\left(\sum_{k=1}^{n} \frac{1}{k}\right) \leq -\sum_{i=1}^{N} \ln\left(1 - \frac{1}{p_i}\right).$$

On $\lim_{n \to +\infty} \left(\sum_{k=1}^{n} \frac{1}{k}\right) = +\infty$ donc $\lim_{n \to +\infty} -\sum_{i=1}^{N} \ln\left(1 - \frac{1}{p_i}\right) = +\infty$

Puisque la série $\sum_{i\geq 1} \left(-\ln\left(1-\frac{1}{p_i}\right)\right)$ est à termes positifs et que ses sommes partielles ne sont pas majorées elle est divergente.

Or $v_i \sim w_i$ donc $\boxed{\sum_{i\geq 1} w_i = \sum_{i\geq 1} \frac{1}{p_i} \text{ diverge.}}$

Ceci veut dire que $\left(\frac{1}{p_i}\right)$ ne décroît pas trop rapidement donc que la croissance des (p_i) n'est pas trop rapide.

I.4) Soit $A>1$. sur $[A,+\infty[$ $u_k : s \mapsto \frac{1}{k^s}$ est de classe $\mathcal{C}^1$ et $u'_k(s) = -\frac{\ln k}{k^s}$.

$$\sup_{s\in[A,+\infty[} |u'_k(s)| = \frac{\ln k}{k^A} = o\left(\frac{1}{k^{\frac{A+1}{2}}}\right) \quad \text{car } \ln k = o\left(k^{\frac{A-1}{2}}\right)$$

Par conséquent

- $\sum_{k\geq 1} \frac{1}{k^A}$ converge.
- chaque u_k est de classe $\mathcal{C}^1$ sur $[A,+\infty[$
- $\sum_{k\geq 1} u'_k$ converge uniformément sur $[A,+\infty[$.

On peut affirmer que ζ est de classe $\mathcal{C}^1$ sur $[A,+\infty[$, pour tout $A>1$ donc sur $]1,+\infty[$ et $\boxed{\zeta'(s) = -\sum_{k=1}^{+\infty} \frac{\ln k}{k^s}}$

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

III.1.b) Si $n+1$ n'est pas premier alors $P_{n+1} = P_n$ donc.

$P_n \leq 4^n \Rightarrow P_{n+1} \leq 4^n \leq 4^{n+1}$

II.1.c) On suppose $r\geq 2$ et $n+1$ premier, donc $n+1\geq 3$ et $n+1$ est premier donc $n+1$ est impair et $n+1 = 2m+1$.

$C_{2m+1}^{m} = \frac{(m+2)(m+3)\cdots(2m+1)}{1\times \cdots \times m}$. Si p est un nombre premier compris entre $(m+2)$ et $(2m+1)$, alors il divise $m!\,C_{2m+1}^{m}$ $(= (m+2)\cdots(2m+1))$. Or il ne peut diviser $m!$ donc

il divise C_{2m+1}^{m}.

- $C_{2m+1}^{m} = C_{2m+1}^{m+1}$ (car $m+1 = 2m+1-m$) donc

$2\,C_{2m+1}^{m} \leq \sum_{k=0}^{2m+1} C_{2m+1}^{k} = 2^{2m+1}$. Et finalement $C_{2m+1}^{m} \leq 4^{m}$.

$P_{m+1} = P_{m+1} \prod_{i \in]} p_i$ avec $i \in] \Leftrightarrow p_i \in [m+2, \ldots, 2m+1]$

D'après le lemme de Gauss, puisque les p_i sont premiers entre eux deux à deux $\prod_{i \in]} p_i$ divise C_{2m+1}^{m}, donc $\prod_{i \in]} p_i \leq C_{2m+1}^{m} \leq 4^{m}$

Et $P_{m+1} \leq 4^{m+1} \Rightarrow P_{m+1} \leq 4^{m+1} \times 4^{m} = 4^{m+1}$.

II.1) On a $2 = P_2 \leq 16$ donc $\forall n$. $\underline{P_n \leq 4^{n}}$

II.2) $d_n = \prod_{i=1}^{N} p_i^{a_i}$ où a_i est la plus grande puissance de p_i pouvant diviser un entier inférieur à n. On a donc.

$p_i^{a_i} \leq n$ et $a_i \leq \left[\frac{\ln n}{\ln p_i}\right]$.

Réciproquement $p_i^{\left[\frac{\ln n}{\ln p_i}\right]} \leq p_i^{\frac{\ln n}{\ln p_i}} = n$..

Finalement $d_n = \prod_{i=1}^{N} p_i^{\left[\frac{\ln n}{\ln a_i}\right]}$

II.3a) L'étude de $x \mapsto x(1-x)$ sur $[0,1]$ donne $\forall x \in [0,1]$

$0 \leq x(1-x) \leq \frac{1}{2}\left(1-\frac{1}{2}\right) = \frac{1}{4}$. Donc $\underline{I_n \leq \frac{1}{4^{n}}}$

II.3β) $n+k+1 \leq 2n+1$, donc par définition du p.p.c.m. $n+k+1$ divise d_{2n+1}. ($d_{2n+1} \times \frac{1}{n+k+1}$ est un entier).

$I_n = \int_0^1 x^n \sum_{k=0}^{n} (-1)^k C_n^k x^k = \sum_{k=0}^{n} (-1)^k C_n^k \times \frac{1}{n+k+1}$

$d_{2n+1} I_n = \sum_{k=0}^{n} (-1)^k C_n^k \frac{d_{2n+1}}{n+k+1}$ est un entier d'après le résultat du début de la question précédente.

- I_n est non nul car $x \mapsto x^n(1-x)^n$ est continue, positive et non identiquement nulle sur $[0,1]$, donc $I_n > 0$. Par conséquent

$|d_{2n+1} I_n| \geq 1$ puis $\underline{d_{2n+1} \geq 4^{n}}$.

III.1) H_A est continue sur chaque intervalle $[p_r, p_{r+1}[$ car constante sur cet intervalle. H_A est aussi continue sur $[1,2[$.
H_A possède une discontinuité en p_k et $H_A(p_k) - H_A(p_k - 0) = a_k$.
(Cette discontinuité n'en étant pas une si $a_k = 0$!)

- Si f est de classe $\mathcal{C}^1$ pour tout (u,v) de $[2,+\infty[$ on a $\int_u^v f'(t)\,dt = f(v) - f(u)$.

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

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

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

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

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

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

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

III.2a) Utilisons la majoration $p_r \le 4^r$ si $p_N \le n < p_{N+1}$
en choisissant $n = E(x) = [x]$, on aura $\ln p_n \le n \ln 4 \le x \ln 4$
et $\ln P_r = \sum_{i=1}^{N} \ln p_i = \theta(x)$. D'où : $\boxed{\theta(x) \le x \ln 4}$.

III.2b) Suivons les indications de l'énoncé, $a_k = \ln p_k$. $H_A = \theta$.
$f(x) = \dfrac{1}{\ln x}$ $\quad \sum_{i=1}^{N} a_i f(p_i) = \sum_{i=1}^{N} 1 = \pi(x)$.

$$\boxed{\pi(x) = \theta(x)\frac{1}{\ln x} + \int_2^x \theta(t) \frac{dt}{(\ln t)^2} \le \ln 4 \times \left(\frac{x}{\ln x} + \int_2^x \frac{dt}{(\ln t)^2}\right)}$$

III.2c) $\displaystyle\int_2^x \frac{dt}{(\ln t)^2} = \int_2^{\sqrt{x}} \frac{dt}{(\ln t)^2} + \int_{\sqrt{x}}^x \frac{dt}{(\ln t)^2} \le \frac{\sqrt{x}}{(\ln 2)^2} + \frac{x - \sqrt{x}}{(\ln \sqrt{x})^2}$.

$$\int_2^x \frac{dt}{(\ln t)^2} \le \frac{\sqrt{x}}{(\ln x)^2} + \frac{4x}{(\ln x)^2} \quad \text{donc} \quad \boxed{\lim_{x \to +\infty} \frac{\ln x}{x} \int_2^x \frac{dt}{(\ln t)^2} = 0.}$$

Rexia

III.2.d) Il existe donc un réel x_0 tel que $\forall x \geq x_0 \quad R(x) \leq \ln 4$.

On aura $\forall x \geq x_0 \quad \pi(x) \leq \ln 4 \frac{x}{\ln x} + R(x) \frac{x}{\ln x} \leq 2 \ln 4 \frac{x}{\ln x}$.

soit $\pi(x) \leq 4 \ln 2 \frac{x}{\ln x}$.

III.3.a) Soit $x \geq 3$ et $2n+1$ le plus grand entier inférieur ou égal à x

$p_N \leq x < p_{N+1}$ implique $p_N \leq 2n+1 \leq x < p_{N+1}$.

On a $d_{2n+1} \geq 4^n$ soit $\sum_{i=1}^{N} \ln p_i \left[\frac{\ln(2n+1)}{\ln p_i}\right] \geq n \ln 4$.

Or $n \geq \frac{x-3}{2}$ et $\left[\frac{\ln(2n+1)}{\ln p_i}\right] \leq \frac{\ln(2n+1)}{\ln p_i} \leq \frac{\ln x}{\ln p_i}$

Il en résulte $\pi(x) \ln x \geq \frac{x-3}{2} \ln 4$.

et $\exists x_1 \quad \forall x \geq x_1 \quad \frac{x-3}{2} \ln 4 \geq \frac{x \ln 4}{4} = \frac{x \ln 2}{2}$

$\exists x \quad \forall x \geq x_1 \quad \pi(x) \geq \frac{\ln 2}{2} \frac{x}{\ln x}$.

IV.1a) $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si il existe $\bar{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a}\bar{u} = \bar{1}$ c'est à dire $n \mid au-1$ c'est à dire $\exists (u,v) \in \mathbb{Z}^2 \quad au + nv = 1$. Ceci veut dire que a et n sont premiers entre eux (Bézout).

$\varphi(2)=1 \quad \varphi(3)=2 \quad \varphi(4)=2 \quad \varphi(5)=4 \quad \varphi(6)=2 \quad \varphi(7)=6$.

IV.1.b) La multiplication conserve ses propriétés d'associativité et de commutativité sur $(\mathbb{Z}/n\mathbb{Z})^*$, qui est bien stable pour cette loi. $\bar{1}$ est élément neutre. L'inverse d'un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ étant lui aussi inversible tout élément de $(\mathbb{Z}/n\mathbb{Z})^*$ est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$

Donc $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe (l'énoncé est imprécis, il ne précisait pas la loi). Card $(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$.

L'application $\bar{\beta} \mapsto \bar{a}\bar{\beta}$ est une bijection de $(\mathbb{Z}/n\mathbb{Z})^*$ vers lui-même (la réciproque est $\bar{\beta} \mapsto (\bar{a})^{-1}\bar{\beta}$) (c'est le théorème de Cayley !).

Donc $c = \prod_{\bar{\beta}' \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{\beta}' = \bar{a}^{\varphi(n)} \prod_{\bar{\beta} \in (\mathbb{Z}/n\mathbb{Z})^*} \bar{\beta} = \bar{a}^{\varphi(n)} c$.

Or c est inversible donc $\bar{a}^{\varphi(n)} = \bar{1}$

IV 1.c Dans $\left(\mathbb{Z}/6\mathbb{Z}\right)^*$ $\overline{251}^{311} = \overline{251}^{311} = \overline{5}^{311}$ et $\overline{5} \in \left(\mathbb{Z}/6\mathbb{Z}\right)^*$

On $\varphi(6) = 2$ donc $\forall x \in \left(\mathbb{Z}/6\mathbb{Z}\right)^*$ $x^2 = \overline{1}$ et $\overline{5}^{311} = (\overline{5}^{155})^2 \overline{5} = \overline{5}$

Le reste de la division de 251^{311} par 6 est 5

IV.2.a) $\bar{a}$ ($a \in [0, n-1]$) est non inversible si et seulement si a n'est pas premier à pq c'est à dire si et seulement si a est divisible par q. Il y a dans $[0, pq[$ q éléments divisibles par p, p éléments divisibles par q et 1 éléments divisible par pq. Le nombre d'éléments divisibles par p ou q est donc $p+q-1$ et $\varphi(pq) = pq - (p+q-1) = (p-1)(q-1)$

IV.2b) - $\bar{e}$ est inversible dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$ car e est premier avec $(p-1)(q-1)$. Il existe donc d dans $\mathbb{N}$ tel que $\bar{e}\bar{d} = 1$ $((p-1)(q-1))$.

- $n = 6$ $(p-1)(q-1) 2$. On peut prendre $d = 1$.
- Il faut calculer $\bar{a}^5$ si $\bar{a}$ parcourt $\mathbb{Z}/6\mathbb{Z}$. On trouve, pour les six valeurs $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ $\bar{a}^5 = \bar{a}$.

IV.2c) - Si a est premier avec pq alors $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ donc $\bar{a}^{ed} = \bar{a}^{1+k(p-1)(q-1)} = \bar{a}\,(\bar{a}^{\varphi(n)})^k = \bar{a}$.

- Si a est premier avec p mais pas avec q.

alors dans $\mathbb{Z}/p\mathbb{Z}$ $a^{p-1} = 1$ (p) donc $a^{ed} \equiv a$ (p)

donc $p \mid a^{ed} - a = a(a^{ed-1} - 1)$ et $q \mid a$. Or p et q sont premiers entre eux et d'après le lemme de Gauss pq divise $a^{ed} - a$.

C'est à dire $\bar{a}^{ed} = \bar{a}$ dans $\mathbb{Z}/n\mathbb{Z}$

- Si a est premier avec q mais pas avec p.

Même raisonnement.

- Si a n'est premier ni avec p ni avec q, alors $pq \mid a$ et $0 = \bar{a}$ donc $\bar{a}^{ed} = \bar{a}$ dans $\mathbb{Z}/pq\mathbb{Z}$