Corrigé de JL. Lamard (jean-louis.lamard@prepas.org)

I.1. La suite des nombres premiers est illimitée.

Raisonnement classique par l'absurde basé sur la décomposition en produit de nombres premiers de tout entier supérieur ou égal à 2. CQFD.

I2. Ensemble M_n.

a. $0 < \dfrac{1}{n^s} < 1$ d'où la relation proposée. CQFD.

b. Ainsi les familles de réels positifs $\left(\dfrac{1}{a^{is}}\right)_{i\in\mathbb{N}}$ et $\left(\dfrac{1}{a^{js}}\right)_{j\in\mathbb{N}}$ sont sommables (puisque positives et que les séries correspondantes convergent) donc la famille produit est sommable de somme le produit des sommes. CQFD.

c. Notons φ l'application proposée et soient $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ et $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ deux éléments de $\mathbb{N}^n$ tels que $\varphi(\alpha) = \varphi(\beta)$. En élevant ce réel positif à la puissance $\dfrac{1}{s}$, il vient que $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ donc $\alpha = \beta$ par unicité de la décomposition en facteurs premiers. Ainsi l'application φ est injective. CQFD.

- L'ensemble des puissances 1/s des éléments de M_n est un sous-ensemble infini de $\mathbb{N}$ qui peut donc être classiquement indexé de manière croissante (axiome de Peano par exemple). Donc M_n également puisque $x \longmapsto x^s$ est croissante sur $\mathbb{R}^+$. CQFD. À noter que la question précédente est inutile pour établir cela.

- $M_2 = \{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, \dots\}$
  $M_3 = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, \dots\}$.

- Les n familles de réels positifs $\left(\dfrac{1}{p_i^{s\alpha_i}}\right)_{\alpha_i\in\mathbb{N}}$ sont sommables de somme $\left(1 - \dfrac{1}{p_i^s}\right)^{-1}$ donc la famille produit est sommable de somme le produit des sommes.
  Ainsi $\displaystyle\sum_{m\in M_n} \frac{1}{m} = \sum_{j=1}^{+\infty} \frac{1}{m_j} = \prod_{i=1}^{n} \left(1 - \frac{1}{p_i^s}\right)^{-1}$. CQFD.

d. Notons $N = N(n)$.
Il vient $\displaystyle\sum_{k=1}^{n} \frac{1}{k^s} = \sum_{m\in M_{N(n)};\, m\leqslant n^s} \frac{1}{m} \leqslant f_{N(n)}(s)$ et cela pour tout entier $n \geqslant 2$ et tout réel $s > 0$. CQFD.

- En particulier $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \leqslant f_{N(n)}(1)$. Supposons qu'il n'existe que N_0 entiers premiers.
  Il en résulte que $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \leqslant f_{N_0}(1)$ pour tout entier $n \geqslant N_0$. Ainsi la série harmonique serait convergente. CQFD.

- Pour tout réel $s > 0$, la suite $\big(f_k(s)\big)_{k\in\mathbb{N}}$ est clairement croissante donc admet une limite $\ell(s) \in \overline{\mathbb{R}}$.
  Lorsque n tend vers $+\infty$, il en va de même de $N(n)$ donc $f_{N(n)}(s)$ tend vers $\ell(s)$.
  Supposons désormais que $s \in]0, 1]$. De $\displaystyle\sum_{k=1}^{n} \frac{1}{k^s} \leqslant f_{N(n)}(s)$ on tire par passage à la limite que $\ell(s) = +\infty$.
  Ainsi $\displaystyle\lim_{n\to+\infty} f_n(s) = +\infty$ pour $s \in]0, 1]$. CQFD.

e. On a évidemment $\left\{\dfrac{1}{m}\right\}_{m\in M_{N(n)}} \subset \left\{\dfrac{1}{k^s}\right\}_{k\in\mathbb{N}^*}$ donc si $s > 1$ il vient $\displaystyle\sum_{k=1}^{n} \frac{1}{k^s} \leqslant f_{N(n)}(s) \leqslant \zeta(s)$.
Par passage à la limite, il en résulte que $\ell(s) = \zeta(s)$.
Ainsi $\displaystyle\lim_{n\to+\infty} f_n(s) = \zeta(s)$ pour $s > 1$. CQFD.

I.3. Série de terme général $\dfrac{1}{p_i}$.

Il vient $\displaystyle\sum_{i=1}^{n} v_i = \ln\Big(\prod_{i=1}^{n} (1 - \frac{1}{p_1})\Big) = -\ln f_n(1)$ tend vers $-\infty$ d'après I.2.d. Donc la série de terme général v_i diverge donc également la série de terme général $\dfrac{1}{p_i}$ puisque $-v_i \sim \dfrac{1}{p_i} > 0$.

Ainsi la série $\sum \dfrac{1}{p_i}$ diverge ce qui prouve qu'il a "beaucoup" de nombres premiers. CQFD.

I.4. Fonction ζ.

Notons $u_k(s) = \dfrac{1}{k^s}$. Les fonctions u_k sont de classe $\mathcal{C}^1$ sur $]1, +\infty[$, la série $\sum\limits_{k=1}^{+\infty} u_k(s)$ y converge simplement et la série dérivée $\sum u'_k(s)$ y converge localement normalement car, pour $s \geqslant a$ avec $1 < a$, on a $|u'_k(s)| = \dfrac{\ln k}{k^s} \leqslant \dfrac{\ln k}{k^a}$ et $\dfrac{\ln k}{k^a} = o\Big(\dfrac{1}{k^\alpha}\Big)$ avec $1 < \alpha < a$. Ainsi la fonction ζ est de classe $\mathcal{C}^1$ sur $]1, +\infty[$. CQFD.

II.1. Majoration du produit P_n.

a. $\begin{bmatrix} n & N & p_N & P_n & 4^n \\ 2 & 1 & 2 & 2 & 16 \\ 3 & 2 & 3 & 6 & 64 \\ 4 & 2 & 3 & 6 & 256 \\ 5 & 3 & 5 & 30 & 1024 \end{bmatrix}$

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

c. Si $n+1$ est premier il est impair car $n \geqslant 2$ d'où l'existence de l'entier m.
On a $m!\,\mathrm{C}_{2m+1}^m = (2m+1)(2m)\ldots(m+2)$. Donc si p est un nombre entier compris entre $m+2$ et $2m+1$ il divise $m!\,\mathrm{C}_{2m+1}^m$. Si en outre p est premier, il ne divise pas $m!$ d'après le théorème de Gauss (sinon il diviserait $k \leqslant m$ ce qui est impossible car $p > m$) donc, toujours par le théorème de Gauss, il divise C_{2m+1}^m. CQFD.

- On a $\mathrm{C}_{2m+1}^m + \mathrm{C}_{2m+1}^{m+1} \leqslant \sum\limits_{k=0}^{2m+1} \mathrm{C}_{2m+1}^k = 2^{2m+1} = 2\ 4^m$. Or $\mathrm{C}_{2m+1}^m = \mathrm{C}_{2m+1}^{m+1}$. Donc $\mathrm{C}_{2m+1}^m \leqslant 4^m$. CQFD.

- Supposons $P_{m+1} \leqslant 4^{m+1}$. Il vient $P_{n+1} = P_{m+1}q$ où q est le produit des nombres premiers compris entre $m+2$ et $n+1 = 2m+1$. D'après ci-dessus chacun de ces facteurs divise C_{2m+1}^m donc leur produit q également d'après le théorème de Gauss. Il en résulte que $q \leqslant \mathrm{C}_{2m+1}^m \leqslant 4^m$. Ainsi $P_{n+1} \leqslant 4^{m+1}4^m = 4^{n+1}$. CQFD.

d. Pour $n \geqslant 2$ soit le prédicat $\mathcal{P}(n) =$ « $P_k \leqslant 4^k$ pour $2 \leqslant k \leqslant n$». $\mathcal{P}(2)$ est vrai et il résulte de ce qui précède que $\mathcal{P}(n)$ est vrai pour tout $n \geqslant 2$ par récurrence. CQFD.

II.2 Une expression du ppcm d_n.

On a $d_n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$ avec $p_i^{\alpha_i}$ divise un entier $k \leqslant n$ mais $p_i^{\alpha_i+1}$ n'en divise aucun.
Ainsi $p_i^{\alpha_i} \leqslant n$ et $p_i^{\alpha_i+1} > n$ sinon $p_i^{\alpha_i+1} = k \leqslant n$ donc divise $k \leqslant n$.
Donc $\alpha_1 = [\ln n / \ln p_i]$. CQFD.

II.3. Une minoration du ppcm d_{2n+1}.

a. Pour tout $x \in [0,1]$ il vient $x(1-x) \leqslant \dfrac{1}{4}$ d'où $I_n \leqslant \dfrac{1}{4^n}$. CQFD.

b. d_{2n+1} est évidemment divisible par tout entier inférieur ou égal à $2n+1$ donc en particulier par $n+k+1$ pour k variant de 0 à n.
Or $I_n = \sum\limits_{k=0}^{n} (-1)^k \dfrac{\mathrm{C}_n^k}{n+k+1}$ donc $d_{2n+1}I_n \in \mathbb{Z}$. Par ailleurs $d_{2n+1}I_n > 0$ donc c'est un entier naturel non nul.
Ainsi $d_{2n+1}I_n \geqslant 1$ donc $d_{2n+1} \geqslant \dfrac{1}{I_n} \geqslant 4^n$ d'après II.3.a. CQFD.

III.1. Un résultat auxiliaire.

- Notons que $\pi(x) = N([x])$, $\theta(x) = \ln P_{[x]}$ et $H_A(x) = A_{\pi(x)}$ en notant $A_n = \sum\limits_{k=1}^{n} a_k$.
- H_A est constante donc continue sur l'ouvert $]1, 2[$ et sur tout intervalle $]p_n, p_{n+1}[$ où elle vaut A_n.
On a donc $H_A(p_n) - H_A(p_n - 0) = a_n$ et donc H_A est discontinue en p_n si et seulement si $a_n \neq 0$.
- $$\begin{aligned} \int_2^x H_A(t)f'(t)\,\mathrm{d}\,t &= \sum_{k=1}^{N-1} \int_{p_k}^{p_{k+1}} H_A(t)f'(t)\,\mathrm{d}\,t + \int_{p_N}^{x} H_A(t)f'(t)\,\mathrm{d}\,t \\ &= \sum_{k=1}^{N-1} A_k\big(f(p_{k+1}) - f(p_k)\big) + A_N\big(f(x) - f(p_N)\big) \quad \text{car } f \text{ est de classe } \mathcal{C}^1. \\ &= A_N f(x) + \sum_{k=2}^{N} A_{k-1}f(p_k) - \sum_{k=1}^{N} A_k f(p_k) \\ &= H_A(x)f(x) - \sum_{k=1}^{N} a_k f(p_k) \quad \text{CQFD.} \end{aligned}$$

III.2. Une majoration de la fonction π.

a. On a $\theta(x) = \ln\left(P_{[x]}\right) \leqslant \ln\left(4^{[x]}\right)$ d'après II.1.d. Donc $\theta(x) \leqslant [x]\ln 4 \leqslant x\ln 4$. CQFD.

b. En choisissant la suite (a_k) et la fonction f (qui est bien de classe $\mathcal{C}^1$ sur $[2, +\infty[$) indiquées dans l'énoncé, il vient $H_A(x) = \theta(x)$ et la relation établie en III.1. s'écrit, puisqu'alors $\sum\limits_{k=1}^{N} a_k f(p_k) = N = N(x) = \pi(x)$:

$\pi(x) = \dfrac{\theta(x)}{\ln x} + \displaystyle\int_2^x \frac{\theta(t)}{t\ln^2 t}\,\mathrm{d}\,t.$

D'où la majoration proposée compte tenu de l'inégalité $\theta(x) \leqslant x\ln 4$ établie ci-dessus. CQFD.

c. Il vient $\displaystyle\int_2^x \frac{\mathrm{d}\,t}{\ln^2 t} = \int_2^{\sqrt{x}} \frac{\mathrm{d}\,t}{\ln^2 t} + \int_{\sqrt{x}}^x \frac{\mathrm{d}\,t}{\ln^2 t} \leqslant \frac{\sqrt{x}-2}{\ln^2 2} + \frac{4(x-\sqrt{x})}{\ln^2 x} \underset{x\to+\infty}{\sim} \frac{4x}{\ln^2 x}$.
Donc $\lim\limits_{x\to+\infty} R(x) = 0$. CQFD.

d. En particulier pour x assez grand on a $R(x) \leqslant 1$ donc $\displaystyle\int_2^x \frac{\mathrm{d}\,t}{\ln^2 t} \leqslant \frac{x}{\ln x}$ d'où, en vertu de l'inégalité III.2.b., $\pi(x) \leqslant 4\ln 2 \dfrac{x}{\ln x}$. CQFD.

III.3. Une minoration de la fonction π.

Soit x un réel positif et soit n tel que $2n+1 \leqslant x < 2n+3$.
Il vient $d_{2n+1} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ avec $N = N(2n+1) = \pi(x)$ car $N(2n+1) = N(2n+2)$.
Or $d_{2n+1} \geqslant 4^n$ d'après II.3.b. donc $\alpha_1 \ln p_1 + \alpha_2 \ln p_2 + \cdots + \alpha_N \ln p_N \geqslant n\ln 4$.
Or $\alpha_i = [\ln(2n+1)/\ln p_i]$ donc a fortiori $\sum\limits_{i=1}^{N} \ln(2n+1) \geqslant n\ln 4$ d'où $N = \pi(x) \geqslant \ln 4 \dfrac{n}{\ln(2n+1)} \geqslant \ln 4 \dfrac{(x-3)/2}{\ln x}$.
Or $\ln 4 \dfrac{(x-3)/2}{\ln x} \underset{n\to+\infty}{\sim} \ln 2 \dfrac{x}{\ln x}$ donc, pour x assez grand, $\pi(x) \geqslant \dfrac{\ln 2}{2}\, \dfrac{x}{\ln x}$. CQFD.

IV.1. Théorème d'Euler.

a. $\left(\ \overline{a} \text{ est inversible dans } \mathrm{Z}/n\mathrm{Z}\ \right) \iff \left(\ \exists \overline{u} \in \mathbb{Z}/n\mathbb{Z} \text{ tel que } \overline{u}\,\overline{a} = \overline{1}\ \right) \iff \left(\ \exists u \in \mathbb{Z}\ \exists v \in \mathbb{Z} \text{ tel que } ua = 1 + vn\right)$
Ainsi, d'après le théorème de Bezout (ici Bachet de Méziriac en réalité), $\overline{a}$ est inversible si et seulement si a est premier avec n. CQFD.

b. D'une manière générale si $\mathcal{A}$ est un anneau, il est immédiat de vérifier que l'ensemble $\mathcal{A}^*$ des éléments inversibles est un groupe multiplicatif. En particulier $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ est un groupe multiplicatif de cardinal $\varphi(n)$ compte-tenu de la question précédente.

- Soit a premier avec n. Alors $\overline{a} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ et son ordre r divise $\varphi(n)$ d'après le théorème de Lagrange.

Donc $\overline{a}^{\varphi(n)} = \overline{a}^{rq} = \overline{1}^q = \overline{1}$. CQFD.
Autre démonstration : l'application proposée est, puisque $\overline{a}$ est inversible, bien une application de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ dans lui-même et elle est injective. Donc elle est surjective puisque $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ est fini. Ainsi c est le produit de tous les éléments de $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Or, puisque le groupe est commutatif, $c = \overline{a}^{\varphi(n)}c$ avec c inversible. CQFD.

c. $251 = 41 \times 6 + 5$ donc, modulo 6, $251^{311} \equiv 5^{311} \equiv (-1)^{311} \equiv -1$. Le reste cherché est donc 5. Le théorème d'Euler est totalement inutile pour traiter cet exemple !

IV.2. Principe de criptographie.

a. Soit m non premier avec pq, avec $1 \leqslant m \leqslant pq-1$. Alors m est divisible par p ou q donc de la forme pr avec $r < q$ ou de la forme qs avec $s < p$. Or ces deux ensemble sont disjoints. Donc le nombre des entiers m est $(p-1)+(q-1)$. Il en découle que $\varphi(pq) = pq - 1 - (p+q-2) = (p-1)(q-1)$. CQFD.

b. Ce n'est rien d'autre qu'un cas particulier de IV.1.a.

c. Soit a un entier quelconque.
Nous avons $a^{1+k(p-1)(q-1)} \equiv a \pmod{p}$. En effet c'est clairement vrai si a est divisible par p et sinon, comme p est premier, a est premier avec p et le théorème d'Euler fournit $a^{p-1} \equiv 1 \pmod{p}$.
De même puisque q est premier, $a^{1+k(p-1)(q-1)} \equiv a \pmod{q}$.
p et q étant évidemment premiers entre eux, le théorème de Gauss prouve que $a^{1+k(p-1)(q-1)} \equiv a \pmod{pq}$.
Comme $ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$, il vient donc $a^{ed} \equiv a \pmod{pq}$. CQFD.

FIN