

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.

I.2. Ensemble M_n .

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

b. Ainsi les familles de réels positifs $\left(\frac{1}{a^{is}}\right)_{i \in \mathbb{N}}$ et $\left(\frac{1}{a^{js}}\right)_{j \in \mathbb{N}}$ 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 $\frac{1}{s}$, 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 $x \mapsto x^s$ 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 $\left(\frac{1}{p_i^{s\alpha_i}}\right)_{\alpha_i \in \mathbb{N}}$ sont sommables de somme $\left(1 - \frac{1}{p_i^s}\right)^{-1}$ donc la famille produit est sommable de somme le produit des sommes.

Ainsi $\sum_{m \in M_n} \frac{1}{m} = \sum_{j=1}^{+\infty} \frac{1}{m_j} = \prod_{i=1}^n \left(1 - \frac{1}{p_i^s}\right)^{-1}$. CQFD.

d. Notons $N = N(n)$.

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

• En particulier $\sum_{k=1}^n \frac{1}{k} \leq f_{N(n)}(1)$. Supposons qu'il n'existe que N_0 entiers premiers.

Il en résulte que $\sum_{k=1}^n \frac{1}{k} \leq f_{N_0}(1)$ pour tout entier $n \geq N_0$. Ainsi la série harmonique serait convergente. CQFD.

• Pour tout réel $s > 0$, la suite $(f_k(s))_{k \in \mathbb{N}}$ 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 $\sum_{k=1}^n \frac{1}{k^s} \leq f_{N(n)}(s)$ on tire par passage à la limite que $\ell(s) = +\infty$.

Ainsi $\lim_{n \rightarrow +\infty} f_n(s) = +\infty$ pour $s \in]0, 1]$. CQFD.

e. On a évidemment $\left\{\frac{1}{m}\right\}_{m \in M_{N(n)}} \subset \left\{\frac{1}{k^s}\right\}_{k \in \mathbb{N}^*}$ donc si $s > 1$ il vient $\sum_{k=1}^n \frac{1}{k^s} \leq f_{N(n)}(s) \leq \zeta(s)$.

Par passage à la limite, il en résulte que $\ell(s) = \zeta(s)$.

Ainsi $\lim_{n \rightarrow +\infty} f_n(s) = \zeta(s)$ pour $s > 1$. CQFD.

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

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

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

I.4. Fonction ζ .

Notons $u_k(s) = \frac{1}{k^s}$. Les fonctions u_k sont de classe \mathcal{C}^1 sur $]1, +\infty[$, la série $\sum_{k=1}^{+\infty} u_k(s)$ y converge simplement et la série dérivée $\sum u'_k(s)$ y converge localement normalement car, pour $s \geq a$ avec $1 < a$, on a $|u'_k(s)| = \frac{\ln k}{k^s} \leq \frac{\ln k}{k^a}$ et $\frac{\ln k}{k^a} = o\left(\frac{1}{k^\alpha}\right)$ 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 $n \geq 2$ d'où l'existence de l'entier m .

On a $m! C_{2m+1}^m = (2m+1)(2m)\dots(m+2)$. Donc si p est un nombre entier compris entre $m+2$ et $2m+1$ il divise $m! C_{2m+1}^m$. Si en outre p est premier, il ne divise pas $m!$ d'après le théorème de Gauss (sinon il diviserait $k \leq m$ ce qui est impossible car $p > m$) donc, toujours par le théorème de Gauss, il divise C_{2m+1}^m . CQFD.

• On a $C_{2m+1}^m + C_{2m+1}^{m+1} \leq \sum_{k=0}^{2m+1} C_{2m+1}^k = 2^{2m+1} = 2 \cdot 4^m$. Or $C_{2m+1}^m = C_{2m+1}^{m+1}$. Donc $C_{2m+1}^m \leq 4^m$. CQFD.

• Supposons $P_{m+1} \leq 4^{m+1}$. 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 $q \leq C_{2m+1}^m \leq 4^m$. Ainsi $P_{n+1} \leq 4^{m+1}4^m = 4^{n+1}$. CQFD.

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

II.2 Une expression du ppcm d_n .

On a $d_n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ avec $p_i^{\alpha_i}$ divise un entier $k \leq n$ mais $p_i^{\alpha_i+1}$ n'en divise aucun.

Ainsi $p_i^{\alpha_i} \leq n$ et $p_i^{\alpha_i+1} > n$ sinon $p_i^{\alpha_i+1} = k \leq n$ donc divise $k \leq n$.

Donc $\alpha_1 = \lfloor \ln n / \ln p_i \rfloor$. CQFD.

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

a. Pour tout $x \in [0, 1]$ il vient $x(1-x) \leq \frac{1}{4}$ d'où $I_n \leq \frac{1}{4^n}$. 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 $I_n = \sum_{k=0}^n (-1)^k \frac{C_n^k}{n+k+1}$ 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 $d_{2n+1} I_n \geq 1$ donc $d_{2n+1} \geq \frac{1}{I_n} \geq 4^n$ 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 $A_n = \sum_{k=1}^n a_k$.

• 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 $a_n \neq 0$.

•
$$\begin{aligned} \int_2^x H_A(t) f'(t) dt &= \sum_{k=1}^{N-1} \int_{p_k}^{p_{k+1}} H_A(t) f'(t) dt + \int_{p_N}^x H_A(t) f'(t) dt \\ &= \sum_{k=1}^{N-1} A_k (f(p_{k+1}) - f(p_k)) + A_N (f(x) - f(p_N)) \quad \text{car } f \text{ est de classe } \mathcal{C}^1. \\ &= A_N f(x) + \sum_{k=2}^N A_{k-1} f(p_k) - \sum_{k=1}^N A_k f(p_k) \\ &= H_A(x) f(x) - \sum_{k=1}^N a_k f(p_k) \quad \text{CQFD.} \end{aligned}$$

III.2. Une majoration de la fonction π .

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

$$H_A(x) = \theta(x) \text{ et la relation établie en III.1. s'écrit, puisqu'alors } \sum_{k=1}^N a_k f(p_k) = N = N(x) = \pi(x) :$$

$$\pi(x) = \frac{\theta(x)}{\ln x} + \int_2^x \frac{\theta(t)}{t \ln^2 t} dt.$$

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

c. Il vient $\int_2^x \frac{dt}{\ln^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\ln^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2 t} \leq \frac{\sqrt{x}-2}{\ln^2 2} + \frac{4(x-\sqrt{x})}{\ln^2 x} \underset{x \rightarrow +\infty}{\sim} \frac{4x}{\ln^2 x}$.

Donc $\lim_{x \rightarrow +\infty} R(x) = 0$. CQFD.

d. En particulier pour x assez grand on a $R(x) \leq 1$ donc $\int_2^x \frac{dt}{\ln^2 t} \leq \frac{x}{\ln x}$ d'où, en vertu de l'inégalité III.2.b.,

$$\pi(x) \leq 4 \ln 2 \frac{x}{\ln x}. \quad \text{CQFD.}$$

III.3. Une minoration de la fonction π .

Soit x un réel positif et soit n tel que $2n+1 \leq x < 2n+3$.

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 $d_{2n+1} \geq 4^n$ d'après II.3.b. donc $\alpha_1 \ln p_1 + \alpha_2 \ln p_2 + \dots + \alpha_N \ln p_N \geq n \ln 4$.

Or $\alpha_i = [\ln(2n+1)/\ln p_i]$ donc a fortiori $\sum_{i=1}^N \ln(2n+1) \geq n \ln 4$ d'où $N = \pi(x) \geq \ln 4 \frac{n}{\ln(2n+1)} \geq \ln 4 \frac{(x-3)/2}{\ln x}$.

Or $\ln 4 \frac{(x-3)/2}{\ln x} \underset{n \rightarrow +\infty}{\sim} \ln 2 \frac{x}{\ln x}$ donc, pour x assez grand, $\pi(x) \geq \frac{\ln 2}{2} \frac{x}{\ln x}$. CQFD.

IV.1. Théorème d'Euler.

a. $(\bar{a} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}) \iff (\exists \bar{u} \in \mathbb{Z}/n\mathbb{Z} \text{ tel que } \bar{u} \bar{a} = \bar{1}) \iff (\exists u \in \mathbb{Z} \exists v \in \mathbb{Z} \text{ tel que } ua = 1 + vn)$

Ainsi, d'après le théorème de Bezout (ici Bachet de Méziriac en réalité), \bar{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 $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe multiplicatif de cardinal $\varphi(n)$ compte-tenu de la question précédente.

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

Donc $\bar{a}^{\varphi(n)} = \bar{a}^{r \cdot q} = \bar{1}^q = \bar{1}$. CQFD.

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

a. Soit m non premier avec pq , avec $1 \leq m \leq pq-1$. 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