DIFFERENTS RESULTATS D'ARITHMETIQUE

DM MPSI3 2024-2025 LYCÉE PIERRE DE FERMAT
CORRECTION

Préliminaires

Le crible d'Erathoshène donne un algorithme qui permet de savoir si un entier est premier ou non. Il est par suite possible d'indexer la suite des nombres premiers p_i, $i = 1, 2\dots$:

$$p_1 = 2, p_2 = 3, p_3 = 5\dots$$

Dans tous le problème la lettre p est réservée aux nombre premiers. Etant donné u réel x, sa partie entière (inférieure) $\lfloor x \rfloor$ est l'entier n qui vérifie la double inégalité suivante :

$$\lfloor x \rfloor = n \leqslant x < n + 1$$

Première partie

Le but de cette partie est de démontrer que la suite des nombres premiers est illimitée et d'étudier la nature de la série de terme général $\left(\frac{1}{p_i}\right)_{i\in\mathbb{N}^*}$.

(1) La suite des nombres premiers est illimitée.
On garde les notations de l'énoncé. On fixe $n \in \mathbb{N}$. Pour tout $i \in \mathbb{N}_n$,
$\prod_{i=1}^{n} p_i \equiv 0[p_i]$, donc $Q \equiv 1[p_i]$ et donc p_i ne divise pas Q.
Si l'ensemble des nombres premiers était limité, donc fini, le nombre $n = \text{card}(\mathcal{P})$ existerait et on aurait un nombre Q sans facteurs premiers. Contradiction !

Donc la suite des nombres premiers est illimitée.

Dans toute la suite n est un entier supérieur ou égal à 2 et s est un réel donné strictement positif.

(2) Sommabilité (somme multiple de termes positifs)

(a) On peut montrer que la suite (S_m) est croissante (somme de termes positifs, et majorée grâce aux suites géométriques), mais nous allons directement employer les suites géométriques.
Soit $m \in \mathbb{N}$, la suite $(s_k) := \left(\left(\frac{1}{n^s}\right)^k\right)$ est géométrique de raison $\frac{1}{n^s} \neq 1$, puisque $n \geqslant 2$, donc $n \neq 1$.
On a donc

$$S_m := \sum_{k=0}^{m} \frac{1}{n^{ks}} = \frac{1 - \left(\frac{1}{n^s}\right)^{m+1}}{1 - \frac{1}{n^s}}$$

Or la suite $\left(\left(\frac{1}{n^s}\right)^{m+1}\right)_m$ est une suite géométrique de raison $\frac{1}{n^s} \in [0, 1[$ donc convergente vers 0.
Par addition, puis division par une constante,

la suite (S_m) est convergente et $\lim S_m = \frac{1-0}{1-\frac{1}{n^s}} = \left(1 - \frac{1}{n^s}\right)^{-1}$.

On notera cette limite : $\sum_{k=0}^{+\infty} \frac{1}{n^{ks}} = \left(1 - \frac{1}{n^s}\right)^{-1}$

(b) Soient a et b deux entiers, différents l'in de l'autre, tous les deux supérieurs ou égaux à 2 ($a \neq b$, $a \geqslant 2$, $b \geqslant 2$).
On note pour tout $i, j \in \mathbb{N}$, $u_{i,j} = \frac{1}{a^{is}b^{js}}$. On note $\mathbb{N}_f$, l'ensemble des parties de $\mathbb{N}$ *finis*.

(i) Soient K une partie finie de $\mathbb{N}^2$ ($K \subset \mathbb{N}_f^2$). On suppose que K est non vide.
$\{i \in \mathbb{N} \mid \exists\, j \in \mathbb{N}, (i, j) \in K\}$ est un sous-ensemble fini non vide de $\mathbb{N}$. Il admet un maximum, notons le i_K. Nécessairement, pour tout $i > i_K$, pour tout $j \in \mathbb{N}$, $(i, j) \notin K$.
$\{j \in \mathbb{N} \mid \exists\, i \in \mathbb{N}, (i, j) \in K\}$ est un sous-ensemble fini non vide de $\mathbb{N}$. Il admet un maximum,

notons le j_K. Nécessairement, pour tout $j > j_K$, pour tout $i \in \mathbb{N}$, $(i,j) \notin K$.
Et ainsi : $K \subset [\![0, i_K]\!] \times [\![0, j_K]\!]$. Notons $H = [\![0, i_K]\!] \times [\![0, j_K]\!] \setminus K$.
Comme les nombres $u_{i,j}$ sont positifs :

$$\sum_{(i,j)\in K} \sum_{j\in J} u_{i,j} \leqslant \sum_{(i,j)\in K} u_{i,j} + \sum_{(i,j)\in H} \underbrace{u_{i,j}}_{\geqslant 0} = \sum_{i\in[\![0,i_K]\!]} \sum_{j\in[\![0,j_K]\!]} u_{i,j}$$

Or en exploitant la sommation par paquets :

$$\sum_{i\in[\![0,i_K]\!]} \sum_{j\in[\![0,j_K]\!]} u_{i,j} = \sum_{i=0}^{i_K i} \left(\sum_{j=0}^{j_K} \frac{1}{a^{is}} \frac{1}{b^{js}}\right) = \left(\sum_{i=0}^{i_K} \frac{1}{a^{is}}\right)\left(\sum_{j=0}^{j_K} \frac{1}{b^{js}}\right) = \frac{1-\frac{1}{a^{s(i_K+1)}}}{1-\frac{1}{a^s}} \times \frac{1-\frac{1}{b^{s(j_K+1)}}}{1-\frac{1}{b^s}}$$

Enfin, comme $\frac{1}{a^{s(i_K+1}} < 1$, et $1 - \frac{1}{a^s} > 0$ (de même pour b), par transitivité :

$$\boxed{\sum_{(i,j)\in K} \sum_{j\in J} u_{i,j} \leqslant \frac{1}{1-\frac{1}{a^s}} \times \frac{1}{1-\frac{1}{b^s}} = \left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1}}$$

(ii) Soit $\epsilon > 0$. Notons $\epsilon' = \left(1-\frac{1}{a^s}\right)\left(1-\frac{1}{b^s}\right)\epsilon > 0$
Comme $\lim \left(1-\frac{1}{a^{s(n+1)}}\right)\left(1-\frac{1}{b^{s(n+1)}}\right) = 1$.
Il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $\left(1-\frac{1}{a^{s(n+1)}}\right)\left(1-\frac{1}{b^{s(n+1)}}\right) > 1-\epsilon'$.
Avec les mêmes calculs qu'à la question précédente :

$$\sum_{i\in[\![0,N]\!]} \sum_{j\in[\![0,N]\!]} u_{i,j} = \left(\sum_{i=0}^{N} \frac{1}{a^{is}}\right)\left(\sum_{j=0}^{N} \frac{1}{b^{js}}\right) = \left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1} \times \left(1-\frac{1}{a^{s(n+1)}}\right)\left(1-\frac{1}{b^{s(n+1)}}\right)$$

$$\sum_{i\in[\![0,N]\!]} \sum_{j\in[\![0,N]\!]} u_{i,j} > \left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1} \times (1-\epsilon') = \left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1} - \epsilon$$

tous les produits ont des facteurs positifs et en exploitant la définition de ϵ'.
Par exemple, en prenant $K = [\![0, N]\!]^2$,

$$\boxed{\text{Ainsi } \forall\ \epsilon > 0,\ \exists\ K \in \mathbb{N}_f^2 \text{ tel que } \sum_{(i,j)\in K} u_{i,j} > \left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1} - \epsilon.}$$

(iii) D'après (i), l'ensemble $\left\{\sum_{(i,j)\in K} u_{i,j}, K \in \mathbb{N}_f^2\right\}$ est majoré et est non vide, donc il admet une borne supérieure.
Et $\left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1}$ est un majorant (i), il est dans l'adhérence (ii), c'est donc la borne supérieure de l'ensemble.

$$\boxed{\left\{\sum_{(i,j)\in K} u_{i,j}, K \in \mathbb{N}_f^2\right\} \text{ admet une borne supérieure } \sum_{(i,j)\in\mathbb{N}^2} u_{i,j} = \left(1-\frac{1}{a^s}\right)^{-1}\left(1-\frac{1}{b^s}\right)^{-1}}$$

(3) Ensemble M_n.
Soient p_1, p_2,$\dots p_n$ les n premiers nombres premiers. M_n est l'ensemble des réels obtenus en considérant tous les produits des réels $(p_1)^s$, $(p_2)^s \dots (p_n)^s$ élevés à des exposants $(\alpha_i)_{1\leqslant i\leqslant n}$, entiers positifs ou nuls :

$$M_n = \{m \in \mathbb{R} \mid m = (p_1)^{s\alpha_1} \times (p_2)^{s\alpha_2} \times \cdots \times (p_n)^{s\alpha_n}, \alpha_i \in \mathbb{N}\}$$

(a) Notons déjà, que par définition de M_n (en tant qu'image de l'application Ω), Ω est surjective.
Si $\Omega(\alpha_1, \alpha_2, \cdots, \alpha_n) = \Omega(\alpha_1', \alpha_2', \cdots, \alpha_n')$, alors $(p_1)^{s\alpha_1}(p_2)^{s\alpha_2} \times \cdots \times (p_n)^{s\alpha_n} = (p_1)^{s\alpha_1'}(p_2)^{s\alpha_2'} \times \cdots \times (p_n)^{s\alpha_n'}$.
Et par unicité de l'écriture en produit de nombres premiers, pour tout $i \in \mathbb{N}_n$, $s\alpha_i = s\alpha_i'$, donc $\alpha_i = \alpha_i'$.

$$\boxed{\text{L'application } \Omega : \mathbb{N}^n \to M_n,\ (\alpha_1, \alpha_2, \cdots, \alpha_n) \mapsto (p_1)^{s\alpha_1} \times (p_2)^{s\alpha_2} \times \cdots \times (p_n)^{s\alpha_n} \text{ est injective.}}$$

(b) On peut énumérer récursivement et de manière croissante les termes de la suite M_n.
- On commence par $m_1 = 1 = \Omega(0, 0, \dots 0)$

- les nombres $m_1, m_2 \dots m_k$ étant obtenus (de manière croissante dans M_n), on définit $m_{k+1} = \min M_n \setminus \{m_1, m_2, \dots, m_k\}$.
  L'ensemble M_n infini, n'est jamais épuisé.

On peut aussi tenter de trouver l'énumération croissante en faisant un tableau qui garde en mémoire, les derniers (α_i) en mémoire puisqu'il ne peut y avoir de saut. C'est comme une gestion de bordure.
Nécessairement, le nombre $m_k = \Omega(\alpha_1^k, \dots, \alpha_n^k)$ suit un m_h $(h \leqslant k)$, $\alpha_i^h = \alpha_i^k$ sauf pour un h où $\alpha_i^h = \alpha_i^k - 1$.
(A noter qu'il y a plusieurs tel m_h).
On garde donc en mémoire *seulement* les (au plus n) éléments maximaux $(\alpha_1^h, \dots \alpha_n^h)_h$ pour $h \leqslant k-1$.
Puis comparer les (au plus n^2 : n nombres pour chacun des n éléments maximaux) nombres :
$\Omega(\alpha_1^{h+1}, \dots \alpha_n^h), \dots \Omega(\alpha_1^h, \dots \alpha_n^{h+1})$ pour connaitre le suivant (le plus petit de ces n^2 nombres).
On a ainsi un procédé constructif de recherche de minimum, à partir d'un ensemble fini, à chaque étape.

Il est possible d'indexer les réels m de M_n dans l'ordre croissant.

On considère $s = 1$ (mais en fait, cela ne change rien dans le relation d'ordre car $t \mapsto t^s$ est croissante.).
Si $n = 2$, il faut donc considérer $p_1 = 2$ et $p_2 = 3$. Puis on classe les nombres $2^{\alpha_1}3^{\alpha_2}$.

$$\underbrace{2^0 3^0}_{=1} < \underbrace{2^1 3^0}_{=2} < \underbrace{2^0 3^1}_{=3} < \underbrace{2^2 3^0}_{=4} < \underbrace{2^1 3^1}_{=6} < \underbrace{2^3 3^0}_{=8} < \underbrace{2^0 3^2}_{=9} < \underbrace{2^2 3^1}_{=12} < \underbrace{2^4 3^0}_{=16} < \underbrace{2^1 3^2}_{=18} < \underbrace{2^3 3^1}_{=24} < \underbrace{2^0 3^3}_{=27} < \dots$$

Si $n = 3$, il faut donc considérer $p_1 = 2$, $p_2 = 3$ et $p_3 = 5$. Puis on classe les nombres $2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}$.

$$\underbrace{2^1 3^0 5^0}_{=1} < \underbrace{2^1 3^0 5^0}_{=2} < \underbrace{2^0 3^1 5^0}_{=3} < \underbrace{2^2 3^0 5^0}_{=4} < \underbrace{2^0 3^0 5^1}_{=5} < \underbrace{2^1 3^1 5^0}_{=6} < \underbrace{2^3 3^0 5^0}_{=8} < \underbrace{2^0 3^2 5^0}_{=9} < \underbrace{2^1 3^0 5^1}_{=10} < \underbrace{2^2 3^1 5^0}_{=12} < \underbrace{2^0 3^1 5^1}_{=15} < \underbrace{2^4 3^0 5^0}_{=16} < \dots$$

Il est admis que la suite $\left(\sum_{i=1}^{r} \frac{1}{m_i}\right)_{r \in \mathbb{N}^*}$ est convergente. Sa somme est noté par $\sum_{m \in M_n} m^{-1}$.
Comme le laisse présager la question précédente (généralisée de 2 à n), on admet le résultat suivant :

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

(c) Soit f_n, la fonction définie sur la demi-droite ouverte $]0, +\infty[$ par la relation suivante :

$$f_n(s) = \prod_{i=1}^{n} \left(1 - \frac{1}{p_i^s}\right)^{-1}$$

Soit N, le rang du plus grand nombre premier inférieur à n : $p_N \leqslant n < p_{N+1}$ ou encore $N = \max\{i \mid p_i \leqslant n\}$
On sait que $\prod_{i=1}^{n} \left(1 - \frac{1}{p_i^s}\right)^{-1} = \sum_{m \in M_N} \frac{1}{m}$.

Or pour tout $k \leqslant n$, k se décompose en un unique produit de nombre premier $k = \prod_{i=1}^{+\infty} p_i^{v_{p_i}(k)}$.

Mais pour tout $i \geqslant N+1$, $p_i >> n \geqslant k$, donc $v_{p_i}(k) = 0$ et donc $k = \prod_{i=1}^{N} p_i^{v_{p_i}(k)}$.

En élevant à la puissance s : $k^s = \prod_{i=1}^{N} p_i^{s v_{p_i}(k)} \in M_n$.

Notons $J_n = \{k^s \in \mathbb{R}, k \in [\![1, n]\!]\} \subset M_N$ et $K_n = M_N \setminus J_n$. Donc

$$\sum_{k=1}^{n} \frac{1}{k^s} = \sum_{m \in J_n} \frac{1}{m} = \sum_{m \in M_N} \frac{1}{m} - \underbrace{\sum_{m \in K_n} \frac{1}{m}}_{\geqslant 0} \leqslant \sum_{m \in M_N} \frac{1}{m} = \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1}$$

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

Puis avec $s = 1$, on trouve :

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

Le terme de gauche diverge vers $+\infty$, si la suite des nombres premiers était limitée, la somme de gauche serait fini. Absurde.

La suite des entiers premiers est illimitée.

(d) Pour $s \leqslant 1$, pour tout $k \in \mathbb{N}^*$, $k^s \leqslant k$ et donc $\dfrac{1}{k} \leqslant \dfrac{1}{k^2}$, ainsi :

$$f_n(x) = \prod_{i=1}^{n} \left(1 - \frac{1}{p_i^s}\right)^{-1} \geqslant \sum_{k=1}^{p_n} \frac{1}{k^s} \geqslant \sum_{k=1}^{p_n} \frac{1}{k} \geqslant \ln(p_n)$$

car p_n est le plus grand nombre premier inférieur ou égal à p_n.

$$\boxed{\text{Et donc par minoration, si } s \in]0,1],\ f_n(x) \underset{n\to+\infty}{\longrightarrow} +\infty.}$$

Il est admis qu'à tout réel x supérieur ou égal à 2, peut être associé un entier N tel que : $p_N \leqslant x < p_{N+1}$.

(e) L'inégalité de gauche est déjà démontré (en (c)). On rappelle que $p_N \leqslant n < p_{N+1}$
On applique la même méthode que la question (c), en cherchant un ensemble L_N contenant M_N.
Tout d'abord, on se souvient que $\displaystyle\prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1} \leqslant \sum_{m \in M_N} \frac{1}{m}$.

Puis, on considère $M'_N = \{k \in \mathbb{N} \mid k^s \in M_N\} = \sqrt[s]{M_N}$. C'est bien un ensemble d'entiers.

Par bijection de $\sqrt[s]{\cdot}$: $\displaystyle\sum_{m \in M_N} \frac{1}{m} = \sum_{k \in M'_N} \frac{1}{k^s}$

Enfin, en considérant $H \in \mathbb{N}$, $M'_N \cap [\![1, H]\!] \subset [\![0, H]\!]$

et donc par positivité des termes : $\displaystyle\sum_{k \in M'_N \cap [\![0,H]\!]} \frac{1}{k^s} \leqslant \sum_{k=1}^{H} \frac{1}{k^s}$.

Et en faisant tendre H vers $+\infty$ (on sait que les suites/séries sont convergentes) : $\displaystyle\sum_{k \in M'_N} \frac{1}{k^s} \leqslant \sum_{k=1}^{+\infty} \frac{1}{k^s}$

$$\boxed{\forall\ s > 1, \quad \sum_{k=1}^{n} \frac{1}{k^s} \leqslant \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1} \leqslant \sum_{k=1}^{+\infty} \frac{1}{k^s}}$$

Par théorème d'encadrement :

$$\boxed{\text{Pour} s > 1,\ f_n(s) = \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1}}$$

Dans l'énoncé original, on démontrait également que

$$\zeta :]1, +\infty[\to \mathbb{R}, s \mapsto \lim_{N\to+\infty} f_N(s) = \sum_{k=1}^{+\infty} \frac{1}{k^s}$$

est de classe $\mathcal{C}^1$*...*

Deuxième partie

Le but de cette partie est d'établir une majoration du produit des nombres entiers premiers inférieurs ou égaux à un entier donné n et d'encadrer le plus petit commun multiple de tous les entiers inférieurs ou égaux à cet entier n.
Soit toujours n un entier supérieur ou égal à 2 ($n \geqslant 2$), N le rang du plus grand nombre premier inférieur ou égal à n ($p_N \leqslant n < p_{N+1}$). Soit P_n le produit des nombres premiers inférieurs ou égaux à n ($P_n = \displaystyle\prod_{i=1}^{N} p_i$).

(1) Majoration du produit P_n des nombres premiers majorés par un entier n.

(a) On a le tableau suivant :

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

(b) Supposons que $n+1$ n'est pas premier.
On sait que $p_N \leqslant n < p_{N+1}$, et comme $n < n+1$ et $n+1$ n'est pas premier, de même : $p_N \leqslant n+1 < p_{N+1}$.

$$\boxed{\text{si l'entier } n+1 \text{ n'est pas premier, alors } P_{n+1} = P_n \leqslant 4^n \text{ implique l'inégalité } P_{n+1} \leqslant 4^{n+1}.}$$

(c) L'entier $n+1$ est premier dans cet alinéa.

(i) Ici, $n \geqslant 2$, donc $n+1 \geqslant 3$. Par ailleurs, il s'agit d'un nombre premier donc $n+1$ est impair. Donc n est un nombre pair.

$$\boxed{\text{Il existe } m \in \mathbb{N} \text{ tel que } n+1 = 2m+1.}$$

(ii) Soit p un nombre premier compris entre $m+2$ et $n+1$. Donc p divise $\prod_{h=m+2}^{n+1} h$. Or

$$m!\binom{2m+1}{m} = m!\binom{2m+1}{m+1} = m!\binom{n+1}{m+1} = (m+2)\cdots(n+1)$$

p divise donc $m! \times \binom{2m+1}{m}$.

Or p est un nombre premier entre $m+2$ et $n+1$, donc aucun des nombres h de $\{1, 2\cdots m\}$ divise p, donc pour tout $h \in \mathbb{N}_m$, $p \wedge h = 1$ et donc $p \wedge m! = 1$ (Corollaire de Gauss).

Et donc d'après le lemme de Gauss :

$$\boxed{\text{pour tout } p \in \mathcal{P} \cap [\![m+2, n+1]\!],\ p \text{ divise } \binom{2m+1}{m}.}$$

(iii) Un corollaire du lemme de Gauss indique que si pour tout $i, j \in I$, $b_i \wedge b_j = 1$ et $b_i | c$, alors $\prod_{i\in I} b_i | c$.

Nous appliquons ce corollaire à tous les nombres premiers de $\mathcal{P} \cap [\![m+2, n+1]\!]$.

Etant premiers, ils sont premiers entre eux et par ailleurs, chacun divise $\binom{2m+1}{m}$, donc

$$\prod_{p\in\mathcal{P}\cap[\![m+2,n+1]\!]} p \Big| \binom{2m+1}{m} \text{ donc } \prod_{p\in\mathcal{P}\cap[\![m+2,n+1]\!]} p \leqslant \binom{2m+1}{m}$$

Majorons ce dernier terme, sans trop d'effort.

On sait que $2m+1 = n+1$, puis

$$2^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k} = \binom{n+1}{m} + \binom{n+1}{m+1} + \sum_{k\neq m, m+1} \underbrace{\binom{n+1}{m+1}}_{>0} \geqslant \underbrace{2\binom{2m+1}{m}}_{\binom{2m+1}{m}=\binom{2m+1}{m+1}}$$

Ainsi : $\binom{2m+1}{m} \leqslant \frac{1}{2}2^{2m+1} = 4^m$. Puis,

$$P_{n+1} = \prod_{p\in\mathcal{P}\cap[\![1,n+1]\!]} p = P_{m+1} \times \prod_{p\in\mathcal{P}\cap[\![m+2,n+1]\!]} p \leqslant P_{m+1} \times 4^m \leqslant 4^{m+1} \times 4^m = 4^{2m+1} = 4^{n+1}$$

$$\boxed{\text{Donc si } P_{m+1} \leqslant 4^{m+1}, \text{ alors } P_{n+1} \leqslant 4^{n+1}.}$$

(d) Il s'agit de faire une récurrence.

Notons, pour tout $n \in \mathbb{N}$, et $n \geqslant 2$, $\mathcal{H}_n$: " $P_n \leqslant 4^n$."

- $P_2 \leqslant 4^2$, donc $\mathcal{H}_2$ est vraie.
- $P_3 \leqslant 4^3$, donc $\mathcal{H}_3$ est vraie.
- Soit $n \in \mathbb{N}$ et $n \geqslant 3$. Supposons que pour tout $k \leqslant n$, $\mathcal{H}_k$ est vraie.
  si $n+1$ n'est pas premier, alors comme $P_n \leqslant 4^n$ ($\mathcal{H}_n$) ; d'après (b) : $P_{n+1} \leqslant 4^{n+1}$
  si $n+1$ est premier, alors comme $P_{n+1} \leqslant 4^{m+1}$ ($\mathcal{H}_{m+1}$) ; d'après (c) : $P_{n+1} \leqslant 4^{n+1}$.
  Notons qu'ici, on a bien $n+1 \geqslant 5$ et donc $m \geqslant 2$ (c'est pourquoi on démontre $\mathcal{H}_3$ à part).

Donc $\mathcal{H}_{n+1}$ est vraie.

$$\boxed{\text{Pour tout entier } n \geqslant 2,\ P_n = \prod_{i=1}^{N} p_i \leqslant 4^n.}$$

Soit d_n le plus petit commun multiple de tous les entiers 1, 2, 3,..., n

(2) Notons $T = \prod_{i=1}^{N} p_i^{\alpha_i}$ avec $\alpha_i = \left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor$. On va montrer que $T = d_n$, donc que T est le PPCM, en montrant que c'est le plus petit des multiples de 1, 2... n.

- T est un multiple de 1, 2,... n.

Soit $k \in \mathbb{N}_n$. k se décompose un unique produit de nombres premiers, le plus grand p_K vérifie $p_K \leqslant k < p_{K+1}$.

Et comme $k \leqslant n$, nécessairement $K \leqslant N$. Ainsi $k = \prod_{i=1}^{N} p_i^{v_{p_i}(k)}$.

Puis pour tout $i \in \mathbb{N}_N$, $p_i^{v_{p_i}(k)} \leqslant k \leqslant n$, donc $v_{p_i}(k) \ln p_i \leqslant \ln n$.

Et donc, pour tout $i \in \mathbb{N}_N$, $v_{p_i}(k) \leqslant \dfrac{\ln n}{\ln p_i}$. Et comme il s'agit d'un nombre entier : $v_{p_i}(k) \leqslant \alpha_i$.

En passant au produit sur i, $k = \prod_{i=1}^{N} p_i^{v_{p_i}(k)} | \prod_{i=1}^{N} p_i^{\alpha_i} = T$.

Donc T est bien un multiple de tous les entiers de 2 à n. Autrement écrit : $d_n | T$

• Montrons que c'est le plus petit.

Fixons $i \in \mathbb{N}_N$. On sait que $\alpha_i \leqslant \dfrac{\ln n}{\ln p_i}$, donc $p_i^{\alpha_i} \leqslant n$.

Donc $p_i^{\alpha_i}$ est un facteur des nombres 1, 2,... n. Et donc $p_i^{\alpha_i} | d_n$.

Donc puisque tous les $(p_j^{\alpha_j})$ sont premiers entre eux : $T = \prod_{j=1}^{N} p_j^{\alpha_j} \Big| d_n$

$$\boxed{d_n = \prod_{i=1}^{N} p_i^{\alpha_i} \quad \text{avec} \quad p_N \leqslant n < p_{N+1} \text{ et } \alpha_i = \left\lfloor \frac{\ln n}{\ln p_i} \right\rfloor}$$

(3) Une minoration du PPCM d_{2n+1}.

Etant donné un entier n supérieur ou égal à 2 ($n \geqslant 2$), soit I_n l'intégrale définie par la relation suivante :

$$I_n = \int_0^1 x^n (1-x)^n \mathrm{d}x$$

On retrouve une étude déjà faite en partie IV du DS 4.

(a) Pour tout $x \in [0,1]$, $x(1-x) = x - x^2 = \frac{1}{4} - (x - \frac{1}{2})^2$ (avec la forme canonique)

Donc, comme $(x - \frac{1}{2})^2 \geqslant 0$, on a donc pour tout $x \in [0,1]$, $x(1-x) \leqslant \dfrac{1}{4}$ (on aurait pu étudier f').

Puis par croissance de $t \mapsto t^n$ et de l'intégrale ($0 < 1$), on a donc :

$$I_n = \int_0^1 x^n (1-x)^n \mathrm{d}x \leqslant \int_0^1 \frac{1}{4^n} \mathrm{d}x = \left[\frac{x}{4^n}\right]_0^1 = \frac{1}{4^n}$$

$$\boxed{I_n \leqslant \frac{1}{4^n}}$$

(b) d_{2n+1} est le PPCM des nombres de 1 à $2n+1$.

C'est donc un multiple des nombres de $n+1 = n+k+1$ (avec $k=0$) à $2n+1 = n+k+1$ (avec $k=n$) - entre autres.

$$\boxed{\text{De manière équivalente : } d_{2n+1} \text{ est divisible par tout entier } n+k+1 \text{ (pour } 0 \leqslant k \leqslant n).}$$

$$I_n = \int_0^1 x^n (1-x)^n \mathrm{d}x = \int_0^1 \sum_{k=0}^{n} \binom{n}{k} (-1)^k x^{n+k} \mathrm{d}x = \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{n+k+1}$$

Notons $a_k = \dfrac{d_{2n+1}}{n+k+1} \in \mathbb{N}$ d'après le résultat précédent, on a donc

$$\boxed{d_{2n+1} I_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k a_k \in \mathbb{Z}}$$

(c) On a donc $d_{2n+1} I_n \in \mathbb{Z}$.

Notons que $I_n \geqslant 0$ car $x(1-x) \geqslant 0$ sur $[0,1]$, ainsi $d_{2n+1} I_n \in \mathbb{N}$

Plus précisément, $x \mapsto x(1-x)$ est continue sans être identiquement nulle. Donc $I_n \neq 0$.

Ainsi $d_{2n+1} I_n \geqslant 1$, alors $d_{2n+1} \geqslant \dfrac{1}{I_n} \geqslant \dfrac{1}{\frac{1}{4^n}} = 4^n$, car $I_n \leqslant \dfrac{1}{4^n}$.

$$\boxed{d_{2n+1} \geqslant 4^n}$$

Troisième partie

Le but de cette partie est d'étudier les deux fonctions π et θ définies ci-dessous pour en déduire un encadrement à l'infini du réel $\pi(x)$.

Pour tout réel x supérieur ou égal à 2 ($x \geqslant 2$), $\pi(x)$ est égal au nombre de nombres premiers inférieurs ou égaux à x.

$$p_N \leqslant x < p_{N+1} \qquad \pi(x) = N = \sum_{i=1}^{N} 1$$

Pour tout réel x supérieur ou égal à 2 ($x \geqslant 2$), $\theta(x)$ est égal à la somme des logarithmes des nombres premiers inférieurs ou égaux à x.

$$p_N \leqslant x < p_{N+1} \qquad \theta(x) = \sum_{i=1}^{N} \ln(p_i)$$

Plus généralement : étant donnée une suite réelle $A = (a_k)_{k\geqslant 1}$, soit H_A la fonction définie sur la demi-droite fermée $[1, +\infty[$ par la relation suivante :
$H_A(x)$ est nulle sur l'intervalle $[1, 2[$, égal pour $x \geqslant 2$, à la somme des termes de la suite A dont les rangs sont inférieurs ou égaux au rang N du plus grand nombre entier premier inférieur ou égal à x :

$$H_A(x) = \begin{cases} 0 & \text{si } 1 \leqslant x \leqslant 2 \\ \displaystyle\sum_{k=1}^{N} a_k & \text{si } 2 \leqslant x \text{ , } p_N \leqslant x < p_{N+1} \end{cases}$$

(1) Un résultat auxiliaire.

(a) H_A est assurément continue sur $[0, 2[$ puis sur les intervalles de la forme $[p_k, p_{k+1}[$, pour tout $k \in \mathbb{N}^*$.

Et dès que $a_k \neq 0$, alors H_A est discontinue en p_k, puisque $\lim\limits_{\epsilon\to 0^+} H_A(p_k) - H_A(p_k - \epsilon) = \sum\limits_{i=1}^{k} a_i - \sum\limits_{i=1}^{k-1} a_i = a_k$.

(b) Soit f une fonction réelle, définie et continûment dérivable (i.e. de classe $\mathcal{C}^1$) sur la demi-droite fermée $[2, +\infty[$, et une suite réelle $A = (a_i)_{i\geqslant 1}$.
Soit $x \in [p_N, p_{N+1}[$.

Comme H_A est constante, égale à $\sum\limits_{i=1}^{k} a_i$ (notée σ_k pour la suite) sur tout intervalle de la forme $[p_k, p_{k+1}[$, on a avec la relation de Chasles ($p_1 = 2$) :

$$\begin{aligned}
\int_2^x H_A(t)f'(t)\mathrm{d}t &= \sum_{i=1}^{N-1} \int_{p_i}^{p_{i+1}} H_A(t)f'(t)\mathrm{d}t + \int_{p_N}^{x} H_A(t)f'(t)\mathrm{d}t \\
&= \sum_{i=1}^{N-1} \int_{p_i}^{p_{i+1}} \sum_{h=1}^{i} a_h f'(t)\mathrm{d}t + \int_{p_N}^{x} \sum_{h=1}^{N} a_h f'(t)\mathrm{d}t = \sum_{i=1}^{N-1} \sigma_i \big[f(t)\big]_{p_i}^{p_{i+1}} + \sigma_N \big[f(t)\big]_{p_N}^{x} \\
&= \sum_{i=1}^{N-1} \sigma_i (f(p_{i+1}) - f(p_i)) + \sigma_N (f(x) - f(p_N)) \\
&= \sum_{i=1}^{N-1} \sigma_i f(p_{i+1}) - \sum_{i=1}^{N-1} \sigma_i f(p_i) + \sigma_N f(x) - \sigma_N f(p_N) \\
&= \sum_{i=2}^{N} \sigma_{i-1} f(p_i) - \sum_{i=1}^{N-1} \sigma_i f(p_i) + \sigma_N f(x) - \sigma_N f(p_N) \\
&= \sum_{i=2}^{N-1} (\underbrace{\sigma_{i-1} - \sigma_i}_{=-a_i}) f(p_i) + \sigma_{N-1} f(p_N) - \sigma_1 f(p_1) + \sigma_N f(x) - \sigma_N f(p_N) \\
&= -a_1 f(p_1) - \sum_{i=2}^{N-1} a_i f(p_i) - (\underbrace{\sigma_N - \sigma_{N-1}}_{=a_N}) f(p_N) + \sigma_N f(x) = -\sum_{i=1}^{N} a_i f(p_i) + \underbrace{\sigma_N}_{=H_A(x)} f(x)
\end{aligned}$$

Ainsi, $\displaystyle\sum_{i=1}^{N} a_i f(p_i) = H_A(x)f(x) - \int_2^x H_A(t)f'(t)\mathrm{d}t$

(2) Une majoration de la fonction π.

(a) Soit $x \geqslant 2$ et $p_N \leqslant x < p_{N+1}$, on note $n = \lfloor x \rfloor$, on a donc $p_N \leqslant n < p_{N+1}$ (puisque $p_N \in \mathbb{N}$) :

$$\theta(x) = \sum_{i=1}^{N} \ln(p_i) = \ln\left(\prod_{i=1}^{N} p_i\right) = \ln P_n \leqslant \ln 4^n = n \ln 4 \leqslant x \ln 4$$

car ln est croissante, en exploitant la majoration $P_n \leqslant 4^n$ et $p_N \leqslant n \leqslant x$.

$$\boxed{\theta(x) \leqslant x \ln 4}$$

(b) Prenons, selon la demande, $a_k = \ln p_k$ donc $H_A(x) = \sum_{k=1}^{N} \ln(p_k) = \theta(x)$ et $f : x \mapsto \dfrac{1}{\ln x}$:

$$\begin{aligned}\sum_{i=1}^{N} a_i f(p_i) &= \sum_{i=1}^{N} \ln(p_k)\frac{1}{\ln p_k} = N \\ &= H_A(x)\frac{1}{\ln x} - \int_2^x H_A(t) f'(t)\mathrm{d}t\end{aligned}$$

Or pour tout $x \geqslant 2$, $f'(x) = \dfrac{-1}{x(\ln x)^2}$ et donc :

$$N = \frac{\theta(x)}{\ln x} + \int_2^x \frac{\theta(x)}{x(\ln x)^2}\mathrm{d}x \leqslant \frac{x \ln 4}{\ln x} + \int_2^x \frac{x \ln 4}{x(\ln x)^2}\mathrm{d}x$$

car $\theta(x) \leqslant x \ln 4$ pour tout $x \geqslant 2$:

$\ln x > 0$ pour majorer le premier terme puis $x(\ln x)^2 > 0$ et $x > 2$ pour majorer l'intégrale.
Ce qui donne bien après simplification et factorisation :

$$\boxed{N = \pi(x) \leqslant \ln 4 \left(\frac{x}{\ln x} + \int_2^x \frac{\mathrm{d}t}{(\ln t)^2}\right)}$$

(c) On note pour tout $x \geqslant 2$, $R(x) = \dfrac{\ln x}{x} \times \displaystyle\int_2^x \frac{\mathrm{d}t}{(\ln t)^2}$.

Et donc pour $x \geqslant 4$ (et donc $\sqrt{x} \geqslant 2$) :

$$R(x) = \frac{\ln x}{x}\left(\int_2^{\sqrt{x}} \frac{\mathrm{d}t}{(\ln t)^2} + \int_{\sqrt{x}}^x \frac{\mathrm{d}t}{(\ln t)^2}\right) = \frac{\ln x}{x}\int_2^{\sqrt{x}} \frac{\mathrm{d}t}{(\ln t)^2} + \frac{\ln x}{x}\int_{\sqrt{x}}^x \frac{\mathrm{d}t}{(\ln t)^2}$$

Sur $[2, \sqrt{x}]$, $t \mapsto \dfrac{1}{(\ln t)^2}$ est décroissante et positive, donc

$$0 \leqslant \frac{\ln x}{x}\int_2^{\sqrt{x}} \frac{1}{(\ln t)^2}\mathrm{d}t \leqslant \frac{\ln x}{x(\ln 2)^2}\int_2^{\sqrt{x}} \mathrm{d}t = \frac{\ln x(\sqrt{x}-2)}{x(\ln 2)^2} \leqslant \frac{1}{(\ln 2)^2}\frac{\ln x}{\sqrt{x}} \underset{x\to+\infty}{\longrightarrow} 0$$

Sur $[\sqrt{x}, x]$, $t \mapsto \dfrac{1}{(\ln t)^2}$ est décroissante et positive, donc

$$0 \leqslant \frac{\ln x}{x}\int_{\sqrt{x}}^{x} \frac{1}{(\ln t)^2}\mathrm{d}t \leqslant \frac{\ln x}{x(\ln \sqrt{x})^2}\int_{\sqrt{x}}^{x} \mathrm{d}t = \frac{4\ln x(x-\sqrt{x})}{x(\ln x)^2} \leqslant \frac{4}{\ln x} \underset{x\to+\infty}{\longrightarrow} 0$$

Ainsi, par théorème de convergence par encadrement, puis par addition :

$$\boxed{\text{avec } R(x) = \frac{\ln x}{x} \times \int_2^x \frac{\mathrm{d}t}{(\ln t)^2}, \text{ on a } \lim_{x\to+\infty} R(x) = 0.}$$

(d) En reprenant la majoration de la question (b)

$$\pi(x) \leqslant \ln 4 \left(\frac{x}{\ln x} + \frac{x}{\ln x}R(x)\right)$$

Or $R(x) \underset{x\to+\infty}{\longrightarrow} 0$. Donc il existe $x_0 > 4$ tel que $\forall\, x \geqslant x_0$, $R(x) \leqslant 1$.

Ainsi :

$$\boxed{\text{pour tout } x \geqslant x_0, \text{ (puisque } \tfrac{x}{\ln x} > 0) : \pi(x) \leqslant 2\ln 2\left(\frac{x}{\ln x} + 1\frac{x}{\ln x}\right) = 4\ln 2 \times \frac{x}{\ln x}}$$

(3) Un minoration de la fonction π.

Soit $x \in \mathbb{R}$ et $n = \lfloor x \rfloor$, puis $N = \pi(x)$, donc $p_N \leqslant n \leqslant x < n+1 \leqslant p_{N+1}$.

On peut supposer $x > 3$, et donc p_N est impair. Donc il existe $m \in \mathbb{N}$ tel que $p_N \leqslant 2m+1 \leqslant n < p_{N+1}$.
Enfin, on rappelle que d_n est le PPCM des entiers compris entre 1 et n.

On a vue question II.(3)(c), que $d_{2m+1} \geqslant 4^m$ et que $d_{2m+1} = \displaystyle\prod_{i=1}^{N} p_i^{\alpha_i}$ puisqu'on a bien $p_N \leqslant 2m+1 < p_{N+1}$

et où $\alpha_i = \left\lfloor \dfrac{\ln(2m+1)}{\ln p_i} \right\rfloor \leqslant \dfrac{\ln(2m+1)}{\ln p_i}$.

En composant avec la fonction logarithme (croissante) : $\displaystyle\sum_{i=1}^{N} \alpha_i \ln(p_i) \geqslant 2m \ln 2$.

Comme tout est positif ($\ln p_i > 0 \dots$), on a donc :

$$N \ln x \geqslant N \times \ln(2m+1) = \sum_{i=1}^{N} \frac{\ln 2m+1}{\ln p_i} \ln p_i \geqslant \sum_{i=1}^{N} \alpha_i \ln(p_i) \geqslant m \ln 4 = 2m \ln 2$$

$$\pi(x) = N \geqslant \ln 2 \frac{x-3}{\ln x} = \ln 2 \frac{x}{\ln x} - 3 \ln 2 \frac{1}{\ln x}$$

car $2m+1 \leqslant x < 2m+3$, donc $2m > x-3$.
Ainsi :

$$\frac{\ln x}{x}\pi(x) \geqslant \ln 2 - \frac{3\ln 2}{x} \underset{x\to+\infty}{\longrightarrow} \ln 2$$

Par conséquent, à partir d'un certain rang (noté x_1), $\dfrac{\ln x}{x}\pi(x) \geqslant \dfrac{\ln 2}{2}$ et donc en multipliant par $\frac{x}{\ln x} > 0$:

$$\boxed{\exists\ x_1 > 0 \text{ tel que, } \forall\ x \geqslant x_1 :\ \pi(x) \geqslant \frac{\ln 2}{2} \times \frac{x}{\ln x}}$$

En application numérique, on a $4 \ln 2 \approx 2,77$ et $\frac{\ln 2}{2} \approx 0,35$.

Donc on trouve $\pi(x) = \Omega\left(\dfrac{x}{\ln x}\right)$. C'est en effet cohérents avec le " théorème des nombres premiers" établi par Hadamard et de La Vallée Poussin en 1896, qui affirme que la fonction π est équivalente à l'infini à la fonction $x \mapsto \dfrac{x}{\ln x}$.

Quatrième partie

Soit, dans toute cette partie, un entier n donnée ($n \geqslant 2$). L'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est l'ensemble quotient de l'anneau $\mathbb{Z}$ par la relation $a \equiv b[n]$. Classiquement un élément de $\frac{\mathbb{Z}}{n\mathbb{Z}}$, une classe d'équivalence, est noté $\overline{a}$, a étant un représentant de cette classe.
Soit φ, la fonction qui, à l'entier n, associe le nombre d'éléments inversibles de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

(1) Théorème d'Euler.

(a) Soit $a \in \mathbb{Z}$, on a les équivalences (Bézout) :

$$\begin{aligned} a \text{ est premiers avec } n &\iff \exists\ u, v \in \mathbb{Z} \text{ tel que } ua + vn = 1 \quad \textit{Identité de Bézout} \\ &\iff \exists\ u \in \mathbb{Z} \text{ tel que } ua \equiv 1[n] \\ &\iff \exists\ u \in \mathbb{Z} \text{ tel que } \overline{ua} = \overline{u} \cdot \overline{a} = \overline{1} \\ &\iff \overline{a} \text{ est inversible dans } \frac{\mathbb{Z}}{n\mathbb{Z}} \end{aligned}$$

$$\boxed{\text{L'élément } \overline{a} \text{ de } \frac{\mathbb{Z}}{n\mathbb{Z}} \text{ est inversible, si et seulement si que } a \text{ est premier avec } n.}$$

Faisons un tableau de valeurs :

n	2	3	4	5	6	7
$\varphi(n)$	1	2	2	4	2	6
Inversibles	$\overline{1}$	$\overline{1}, \overline{2}$	$\overline{1}, \overline{3}$	$\overline{1}, \overline{2}, \overline{3}, \overline{4}$	$\overline{1}, \overline{5}$	$\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$

(b) C'est un résultat du cours (officiellement au programme).
Visiblement, on attend une démonstration ici. Je vous renvoie à celui-ci...

$$\boxed{\text{Les inversibles de } \frac{\mathbb{Z}}{n\mathbb{Z}} \text{ forment bien un groupe, son cardinal est simplement } \varphi(n).}$$

Peut-être faut-il préciser la valeur de $\varphi(n)$.
• Notons que $\varphi(1) = 1$.
• Si $n = p^\alpha$, où p est un nombre premier.
Comme p est un nombre premier, pour tout $m \in \mathbb{Z}$, on a $m \wedge p^a \neq 1$ si et seulement si $p|m$.
Ainsi sur $[\![1, n]\!] = [\![1, p^a]\!]$, les nombres non premier avec n sont : p, $2p$, $3p \dots p^{a-1}p$.
Il y a donc p^{a-1} nombres non premiers avec p^a parmi les p^a nombres de 1 à n.
Dans ce cas $\varphi(n) = \varphi(p^a) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right)$.
• φ est multiplicative, i.e. elle vérifie si $a \wedge b = 1$, $\varphi(a \times b) = \varphi(a) \times \varphi(b)$.

Je renvoie au DS 5 2018-2019 - Question A.3.(b).
Une autre option : montrer que l'application

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \to \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}, \quad \overline{a}^{mn} \mapsto (\overline{a\%n}^{m}, \overline{a\%m}^{n}) \text{ est un isomorphime d'anneaux.}$$

En particulier les groupes des inversibles $\left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right)^*$ est isomorphe à $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$.
Ils ont le même cardinal : $\varphi(mn) = \varphi(m) \times \varphi(n)$.
(Vu la question IV.(2)(a) demandée plus loin, je pense qu'on n'attend vraiment pas de démonstration ici).
On a alors (pour $\mathcal{P}_n$ est l'ensemble des nombres premiers divisant strictement n) :

$$\boxed{n = \prod_{p \in \mathcal{P}_n} p^{v_p(n)} \Rightarrow \varphi(n) = n \prod_{p \in \mathcal{P}_n} \frac{p_i - 1}{p_i}}$$

(c) Nouvelle démonstration du petit théorème de Fermat, adapté directement ici... (cf exercice N°277)
Soit a un entier compris entre 0 et $n-1$ ($0 \leqslant a \leqslant n-1$) premier avec n. Donc $\overline{a}$ est inversible.
On peut alors définir $G =< \overline{a} >$, le sous-groupe monogène de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$, engendré par $\overline{a}$.
Il contient au moins un élément, puisque $a \wedge n = 1$.
Notons $r = \text{card}(G)$. D'après le théorème de Lagrange : $r \big| \text{card}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = \varphi(n)$.
Puis, $k \mapsto \overline{a}^k$ ne peut être surjective de $\mathbb{N}$ sur G, puisque G est fini ;
il existe donc $k > h > 0$ tel que $\overline{a}^k = \overline{a}^h$, et donc en multipliant par $\left(a^h\right)^{-1}$: $\overline{a}^{k-h} = \overline{1}$
Donc $\{\ell \in \mathbb{N}^* \mid a^\ell = 1\}$ est non vide ($k-h$ en est un élément) et admet un plus petit élément ℓ_0.
Alors $\overline{a}^{\ell_0} = 1$ et $\forall\ k \in \{1, 2, \dots \ell_0\} = \mathbb{N}_{\ell_0}$, $\overline{a}^k \neq \overline{1}$.
Nécessairement si $k > h \in \mathbb{N}_{\ell_0}$, $\overline{a}^k \neq \overline{a}^h$, sinon on aurait $\overline{a}^{k-h} = \overline{1}$ avec $0 < k-h < \ell_0$.
Et par conséquent, $\text{card}\{\overline{a}^k, k \in \mathbb{N}_{\ell_0}\} = \ell_0$.
Et enfin, $\{\overline{a}^k, k \in \mathbb{N}_{\ell_0}\} \subset G$ (clairement),
Mais l'inclusion réciproque est vraie : si $\overline{a}^k \in G$, alors $\overline{a}^k = \overline{a}^{q\ell_0 + r}$ avec $k = q\ell_0 + r$ DE de k par ℓ_0.
On a donc $\overline{a}^k = (\overline{a}_0^\ell)^q \overline{a}^r = \overline{a}^r \in \{\overline{a}^k, k \in \mathbb{N}_{\ell_0}\}$.
Et donc $G \subset \{\overline{a}^k, k \in \mathbb{N}_{\ell_0}\}$.
Par double inclusion : $G = \{\overline{a}^k, k \in \mathbb{N}_{\ell_0}\}$ et donc $r = \text{card}G = \text{card}\{\overline{a}^k, k \in \mathbb{N}_{\ell_0}\} = \ell_0$.
Par conséquent, $\ell_0 = r | \varphi(n)$ et ainsi, $\overline{a}^{\varphi(n)} = (\overline{a}^{\ell_0})^s = \overline{1}^s = \overline{1}$ en notant $s \times \ell_0 = \varphi(n)$.

$$\boxed{\text{Si } a \text{ un entier compris entre 0 et } n-1 \text{ et } a \wedge n = 1, \text{ alors } \overline{a}^{\varphi(n)} = \overline{1}.}$$

On notera que si $n = p$ est un nombre premier, alors tous les nombres a de 1 à $p-1$ sont premiers avec p et $\varphi(p) = p-1$. On retrouve exactement la formulation du théorème de Fermat (qui est donc un cas particulier du théorème d'Euler).

(d) $251 = 246 + 5 = 41 \times 6 + 5$, donc $A = 251 \equiv 5[6]$ et ainsi $A^{311} \equiv 5^{311}[6]$.
Puisque $5 \wedge 6 = 1$, on peut appliquer la formule précédente.
Or $\varphi(6) = 2$, donc

$$A^{311} \equiv 5^{311} \equiv 5^{2\times 155+1} \equiv (5^2)^{155} \times 5 \equiv 1^{155} \times 5 \equiv 5[6]$$

$$\boxed{\text{Le reste de la division de } 251^{311} \text{ par 6 est donc 5.}}$$

(2) Principe de cryptographie
Soit n un entier ($n \geqslant 2$) égal au produit de deux nombres premiers p et q : $n = p \times q$.

(a) p et q sont des nombres premiers.
Les nombres de 1 à pq qui sont premiers avec p sont ceux qui ne sont ni dans $p\mathbb{Z}$, ni dans $q\mathbb{Z}$.
Il s'agit des nombres de $[\![1, pq]\!] \setminus (p\mathbb{Z} \cup q\mathbb{Z})$.
Notons $A_p = p\mathbb{Z} \cap [\![1, pq]\!]$. On a $A_p = \{p, 2p, \dots qp\}$, donc $\text{card}(A_p) = q$.
Notons $A_q = q\mathbb{Z} \cap [\![1, pq]\!]$. On a $A_q = \{q, 2q, \dots pq\}$, donc $\text{card}(A_q) = p$.
Remarquons que $A_p \cap A_q = \{pq\}$.
En effet, si $a \in A_p \cap A_q$, alors $\exists\ r \in \mathbb{Z}$ tel que $a = rp$. Or $q|a$, donc $q|rp$, mais $q \wedge p = 1$, donc $q|r$.
Donc $a \in pq\mathbb{Z}$, et nécessairement $a = pq$ car par ailleurs : $a \in [\![1, pq]\!]$.
Notons $I = \{m \in [![1, pq]\!] \mid m \wedge pq = 1\}$.

$$\text{card}(I) = \text{card}(\mathbb{N}_{pq}) - \text{card}(A_p \cup A_q) = pq - [\text{card}A_p + \text{card}A_q - \text{card}(A_p \cap A_q) = pq - p - q + 1 = (p-1)(q-1)$$

On rappelle qu'on a vu que pour p premier, $\varphi(p) = p-1$. Et donc

$$\boxed{\varphi(n) = \text{card}(I) = (p-1)(q-1) = \varphi(p) \times \varphi(q)}$$

Soit e un nombre entier premier avec $(p-1)(q-1)$

(b) Toujours avec le théorème de Bézout : $\exists\, c, d \in \mathbb{Z}$ tels que $c(p-1)(q-1) + de = 1$.
On a alors

$$\boxed{e \times d \equiv 1 \quad [(p-1)(q-1)]}$$

(c) Avec $n = 6$, on a $p = 2$ et $q = 3$, $\varphi(6) = 1 \times 2 = 2$ (mais on le savait déjà).
Puis $e = 5$ est bien premier avec 2, on a alors $1 \times 5 \equiv 1[2]$. On choisit donc $d = 1$.
Ensuite, $ed = 5$. On a vu que si $a \wedge 6 = 1$, $a^2 \equiv 1[6]$. Ce qui donne le tableau suivant :

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

Car $2^2 \equiv -2[6]$, puis $2^5 \equiv 2[6]$, $3^2 = 3[6]$, $4^2 \equiv 4[6]$

(d) Soit $\overline{a} \in \dfrac{\mathbb{Z}}{n\mathbb{Z}}$. On peut supposer que $a \in [\![0, n-1]\!]$

- Ou bien, si $a \wedge n = 1$, alors on a vu plus haut que $a^{\varphi(n)} \equiv 1[n]$.
  Puis $de + c\varphi(n) = 1$, donc $a = a^1 = a^{de+c\varphi(n)} \equiv a^{de}(a^{\varphi(n)})^c \equiv a^{de} \times 1^c \equiv a^{de}\ [n]$
- Ou bien, si $a = 0$, alors, pour tout h, $a^h \equiv 0 \equiv a[n]$.
- Ou bien, si $a \wedge n \neq 1$.
  Puisque $n = pq$ (décomposition en nombre premier), $a \wedge n = p$ ou q (pas n).
  Supposons sans perte de généralité que $a = ps$, avec $s \in \mathbb{Z}$ et finalement $s \wedge q = 1$.
  Alors $a \equiv 0[p]$ et donc $a^{ed} \equiv 0 \equiv a[p]$.
  Ainsi $p | a^{ed} - a$.
  Par ailleurs : $a^{ed} = a^{1-c(p-1)(q-1)} = a \times (a^{q-1})^{c(p-1)} \equiv a \times 1[q]$ car $a \wedge q = 1$ et $\varphi(q) = q - 1$.
  Ainsi $q | a^{ed} - a$.
  Et donc, comme $p \wedge q = 1$, d'après un corollaire du lemme de Gauss : $pq | a^{ed} - a$.

Dans tous les cas :

$$\boxed{\text{pour tout élément } \overline{a} \text{ de } \frac{\mathbb{Z}}{n\mathbb{Z}} \text{ on a bien la relation } a^{ed} \equiv a[n].}$$

En fait, l'entier e est connu de l'expéditeur, l'entier d du destinataire. L'entier d est très difficile à calculer si la factorisation de l'entier n n'est pas connue (les entiers p et q sont grands).

- Chiffrement du message a par l'expéditeur : $a \mapsto a^e$;
- Déchiffrement par le destinataire : $b(= a^e) \mapsto b^d = a^{ed} = a$.
- Le message est trouvé.