Il est conseillé aux candidat(e)s de lire le problème en entier. Les deuxième et quatrième parties peuvent être abordées indépendamment des parties précédentes.
Le crible d'Ératosthène 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, $i = 1, 2, \cdots$: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...
Dans tout le problème le lettre p est réservée aux nombres premiers. Étant donné un réel x, sa partie entière $[x]$ est l'entier n qui vérifie la double inégalité suivante : $[x] = n \leq x < n + 1$.
Étant donné un réel x, supérieur ou égal à 2, $(x \geq 2)$, il existe un entier N égal au rang du plus grand nombre premier p_N inférieur ou égal à x, $p_N = \sup\{p \mid p \leq x\}$.

PARTIE I

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 $\dfrac{1}{p_i}$, $i = 1, 2, \cdots$

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

Démontrer que la suite des nombres premiers est illimitée en considérant, par exemple, pour n nombres premiers p_1, p_2,... ,p_n donnés, l'entier Q défini à partir de ces n nombres premiers par la relation suivante : $Q = p_1 p_2 \cdots p_n + 1 = \prod_{i=1}^{n} p_i + 1$.

Dans toute la suite n est un entier supérieur ou égal à 2 $(n \geq 2)$, s un réel donné strictement positif $(s > 0)$.

I.2) **Ensemble** M_n

a) Justifier la relation suivante $\left(1 - \dfrac{1}{n^s}\right)^{-1} = \sum_{k=0}^{\infty} \dfrac{1}{n^{ks}}$.

b) Soit a et b deux entiers différents l'un de l'autre, tous les deux supérieurs ou égaux à 2 $(a \neq b, a \geq 2, b \geq 2)$; démontrer que la série double de terme général $u_{i,j}$, défini pour i et j entiers naturels par la relation suivante $u_{i,j} = \dfrac{1}{a^{is} b^{js}}$ est sommable. Déterminer sa somme S.

Soit p_1, p_2, ..., p_n les n premiers nombres premiers, M_n l'ensemble des réels obtenus en considérant tous les produits des réels p_1^s, p_2^s, ..., p_n^s élevés à des exposants α_i, $1 \leq i \leq n$, entiers positifs ou nuls.

$$M_n = \{m \mid \exists (\alpha_i)_{1 \leq i \leq n} \in \mathbf{N}^n, m = (p_1)^{s\alpha_1} (p_2)^{s\alpha_2} \ldots (p_n)^{s\alpha_n}\} \ .$$

c) Démontrer que l'application $(\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (p_1)^{s\alpha_1} (p_2)^{s\alpha_2} \ldots (p_n)^{s\alpha_n}$, de $\mathbf{N}^n$ dans M_n est injective. En déduire qu'il est possible d'indexer les réels m dans l'ordre croissant : l'application $i \mapsto m_i$ est strictement croissante de $\mathbf{N}^*$ sur M_n.

Exemple : écrire la suite des 12 premiers termes de la suite $(m_i)_{i \in \mathbf{N}^*}$ lorsque le réel s est égal à 1 et l'entier n égal à 2 puis à 3.

Il est admis que la série de terme général $\nu_i = \dfrac{1}{m_i}$, $i \in \mathbf{N}^*$ est convergente ; sa somme est désignée par le symbole $\sum_{m \in M_n} m^{-1}$. Comme le laisse présager l'alinéa b, le résultat plus général ci-après est vrai et admis : $\prod_{i=1}^{n} \left(1 - \dfrac{1}{p_i^s}\right)^{-1} = \sum_{m \in M_n} m^{-1} = \sum_{i=1}^{\infty} \dfrac{1}{m_i}$.

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 ($N = \sup\{\, i \mid p_i \leq n\}$).

d) Démontrer la relation suivante : $\displaystyle\sum_{k=1}^{n} \frac{1}{k^s} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1}$.

Retrouver, en donnant une valeur particulière au réel s, le résultat : la suite des entiers premiers est illimitée.

Déterminer en supposant le réel s inférieur ou égal à 1 ($0 < s \leq 1$), la limite lorsque l'entier n tend vers l'infini, de l'expression $f_n(s)$ introduite ci-dessus.

e) Établir, lorsque le réel s est strictement supérieur à 1 ($s > 1$), l'encadrement ci-dessous $\displaystyle\sum_{k=1}^{n} \frac{1}{k^s} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1} \leq \sum_{k=1}^{\infty} \frac{1}{k^s}$.

En déduire, pour $s > 1$, la limite de l'expression $f_n(s)$ introduite ci-dessus lorsque l'entier n tend vers l'infini.

Il est admis, puisque la suite des nombres premiers est illimitée, qu'à tout réel x supérieur ou égal à 2 ($x \geq 2$), peut-être associé un entier N tel que le réel x soit encadré par les nombres premiers p_N et p_{N+1} : $p_N \leq x < p_{N+1}$.

I.3) **Série de terme général $\dfrac{1}{p_i}$, $i = 1, 2, \ldots$**

Déduire des résultats ci-dessus la nature de la série de terme général v_i, $i = 1, 2, \ldots$, défini par la relation suivante $v_i = \ln\left(1 - \dfrac{1}{p_i}\right)$.

En déduire la nature de la série de terme général : $w_i = \dfrac{1}{p_i}$, $i = 1, 2, \ldots$ Quelle conclusion qualitative est-il possible d'en tirer sur la répartition des nombres premiers ?

I.4) **Fonction ζ**

Soit ζ la fonction limite de la suite f_n. Démontrer que cette fonction, définie d'après la question (2e) sur la demi-droite ouverte $]1, \infty[$ par la relation ci-après, est continûment dérivable.

$$\zeta(s) = \lim_{N \to \infty} \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1} = \sum_{k=1}^{\infty} \frac{1}{k^s} .$$

PARTIE II

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 entiers n.

Soit toujours n un entier supérieur ou égal à 2 ($n \geq 2$), N le rang du plus grand nombre premier inférieur ou égal à n, soit P_n le produit des nombres premiers inférieurs ou égaux à n : $p_N \leq n < p_{N+1}$, $P_n = \prod_{i=1}^{N} p_i$.

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

a) Construire un tableau donnant pour les valeurs 2, 3, 4 et 5 de l'entier n les valeurs de N, p_N, P_n, 4^n.

b) Vérifier que, si l'entier $n+1$ n'est pas premier, l'inégalité $P_n \leq 4^n$ implique l'inégalité $P_{n+1} \leq 4^{n+1}$.

c) L'entier $n+1$ est premier dans cet alinéa ; justifier l'existence d'un entier m tel que : $2m+1 = n+1$.

Démontrer que tout nombre premier p compris entre $m+2$ et $n+1$ ($m+2 \leq p \leq n+1$) divise le coefficient du binôme $\binom{2m+1}{m}$. Établir la majoration suivante : $\binom{2m+1}{m} \leq 4^m$.

En déduire que l'inégalité $P_{m+1} \leq 4^{m+1}$ implique l'inégalité $P_{n+1} \leq 4^{n+1}$.

d) En déduire, pour tout entier $n \geq 2$, la majoration : $P_n = \prod_{i=1}^{N} p_i \leq 4^n$.

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

II.2) **Une expression du ppcm d_n**

Démontrer que le ppcm d_n est égal au produit des nombres premiers p_i inférieurs ou égaux à l'entier n, élevés à des puissances α_i égales aux parties entières du rapport $\ln(n)$ sur $\ln(p_i)$; c'est à dire : $p_N \leq n < p_{N+1}$, $d_n = \prod_{i=1}^{N} p_i^{\alpha_i}$, avec $\alpha_i = \left[\frac{\ln(n)}{\ln(p_i)}\right]$.

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

Étant donné un entier n supérieur ou égal à 2 ($n \geq 2$), soit I_n l'intégrale définie par la relation suivante : $I_n = \int_0^1 x^n (1-x)^n \, \mathrm{d}x$.

a) Démonter la majoration $I_n \leq \frac{1}{4^n}$.

b) Démonter que le ppcm d_{2n+1} est divisible par tout entier $n+k+1$, lorsque l'entier k varie de 0 à n ($0 \leq k \leq n$). En déduire que le produit $d_{2n+1} I_n$ est un entier en considérant, par exemple, une expression de I_n obtenue par développement de $(1-x)^n$.

Démontrer, à l'aide de la majoration de l'intégrale I_n, une minoration du ppcm d_{2n+1}.

PARTIE III

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 ($x \geq 2$), $\pi(x)$ est égal au nombre des nombres premiers inférieurs ou égaux au réel x. $p_N \leq x < p_{N+1}$, $\pi(x) = N = \sum_{i=1}^{N} 1$.

Pour tout réel x supérieur ou égal à 2 ($x \geq 2$), $\theta(x)$ est égal à la somme des logarithmes des nombres premiers inférieurs ou égaux au réel x. $p_N \leq x < p_{N+1}$, $\theta(x) = \sum_{i=1}^{N} \ln(p_i)$.

Plus généralement : étant donné une suite réelle $A = (a_k)_{k\geq 1}$, soit H_A la fonction définie sur la demi-droite fermée $[1, +\infty[$, par la relation suivante :

$H_A(x)$ est nul sur l'intervalle $[1, 2[$, égal pour $x \geq 2$, 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 : $H_A(x) = \begin{cases} 0 & \text{si } 1 \leq x < 2 \\ \sum_{k=1}^{N} a_k & \text{si } 2 \leq x \text{ et } p_N \leq x < p_{N=1} \end{cases}$

III.1) **Un résultat auxiliaire**

Préciser, pour une suite $A = (a_i)_{i\geq 1}$ donnée, sur quels intervalles la fonction H_A est continue. Quels sont ses points de discontinuité ? Préciser en ces points x la valeur de $H_A(x) - \lim_{\substack{y\to x \\ y<x}} H_A(y)$.

Soit f une fonction réelle, définie et continûment dérivable sur la demi-droite fermée $[2, +\infty[$, et une suite réelle $A = (a_i)_{i\geq 1}$; démontrer la relation suivante : pour tout réel x compris entre p_N et p_{N+1}, ($p_N \leq x < p_{N+1}$) il vient : $\sum_{i=1}^{N} a_i f(p_i) = H_A(x)f(x) - \int_2^x H_A(t)f'(t)\,\mathrm{d}t$.

III.2) **Une majoration de la fonction π**

a) Démontrer la majoration suivante de la fonction θ : $\theta(x) \leq x\ln(4)$.

b) Établir en choisissant, dans la relation établie à la question précédente, comme suite A, la suite $\ln(p_k)$, $k = 1, 2, \ldots$, et comme fonction f la fonction $x \mapsto \dfrac{1}{\ln(x)}$, l'inégalité suivante : $\pi(x) \leq \ln(4)\left(\dfrac{x}{\ln(x)} + \displaystyle\int_2^x \frac{\mathrm{d}t}{(\ln(t))^2}\right)$.

c) Démontrer la convergence vers 0, lorsque le réel x croît vers l'infini, de la fonction $R(x)$, suivante : $R(x) = \dfrac{\ln(x)}{x}\displaystyle\int_2^x \frac{\mathrm{d}t}{(\ln(t))^2}$.

Indication : introduire, pour $x \geq 4$, les intégrales de 2 à $\sqrt{x}$ et de $\sqrt{x}$ à x.

d) En déduire l'existence d'un réel x_0 tel que, pour tout réel x supérieur ou égal à x_0, la fonction π vérifie la majoration suivante : $\pi(x) \leq 4\ln(2)\dfrac{x}{\ln(x)}$.

III.3) **Une minoration de la fonction g** En utilisant par exemple la minoration du ppcm d_{2n+1} obtenue à la question (II-3), démontrer qu'il existe un réel x_1 tel que pour tout réel x supérieur ou égal à x_1, la fonction π vérifie la minoration suivante : $\pi(x) \geq \dfrac{\ln(2)}{2}\dfrac{x}{\ln(x)}$.

Ces deux résultats sont 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 $x \mapsto \dfrac{x}{\ln(x)}$.

PARTIE IV

Soit, dans toute cette partie, un entier n donné ($n \geq 2$). L'anneau $\mathbf{Z}/n\mathbf{Z}$ est l'ensemble des classes d'équivalence pour la relation définie par « deux entiers relatifs son équivalents si leur différence est divisible par l'entier n ». Classiquement un élément de $\mathbf{Z}/n\mathbf{Z}$ 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 $\mathbf{Z}/n\mathbf{Z}$.

IV.1) Théorème d'Euler

a) Démontrer que pour que l'élément $\overline{a}$ de $\mathbf{Z}/n\mathbf{Z}$ soit inversible, il faut et il suffit que l'entier a soit premier avec n. Donner les valeurs de $\varphi(n)$ lorsque l'entier n prend toutes les valeurs de 2 à 7.

b) Démontrer que l'ensemble $(\mathbf{Z}/n\mathbf{Z})^\times$ des éléments de $\mathbf{Z}/n\mathbf{Z}$ inversibles est un groupe multiplicatif. Quel est son cardinal ?

Soit a un entier compris entre 0 et $n-1$ ($0 \leq a \leq n-1$), premier avec n. Soit $\varphi(n)$ le nombre d'éléments de $\mathbf{Z}/n\mathbf{Z}$ inversibles. Démontrer la relation : $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Indication : considérer l'application $\gamma : \overline{b} \mapsto \overline{b}\overline{a}$ de $(\mathbf{Z}/n\mathbf{Z})^\times$ dans lui-même puis l'expression c définie par la relation suivante $c = \prod_{b \in (\mathbf{Z}/n\mathbf{Z})^\times} \overline{b}\overline{a}$.

c) Application : déterminer le reste de la division de 251^{311} par 6.

IV.2) Principe de cryptographie

Soit n un entier($n \geq 2$) égal au produit de deux nombres premiers p et q ; $n = pq$.

a) Démontrer la relation : $\varphi(n) = (p-1)(q-1)$.

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

b) Établir l'existence d'un entier d tel que : $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Exemple simple : $n = 6$, $e = 5$; calculer, pour tout élément $\overline{a}$ de $\mathbf{Z}/6\mathbf{Z}$, $\overline{a}^{e.d}$.

c) Démontrer que pour tout élément $\overline{a}$ de $\mathbf{Z}/n\mathbf{Z}$, la relation : $a^{e.d} \equiv a \pmod{n}$.

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 $a^e \mapsto (a^e)^d$. Le message est retrouvé.

PARTIE I

I.1) On suppose qu'il n'y ait qu'un nombre fini de nombres premiers $p_1, \ldots, p_n$. Soit alors $Q = 1 + \prod_{i=1}^{n} p_i$. La relation de définition de Q fournit une relation de Bézout entre Q et tous les nombres premiers, à savoir $Q - \prod_{i=1}^{n} p_i = 1$. On en déduit $Q = 1$ puisqu'il est premier à tout nombre. Autrement dit $n = 0$. Or 2 est premier et donc $n \geq 1$. Il en résulte que

l'ensemble des nombres premiers est infini

I.2) a) Comme $n \geq 2$ et $s > 0$, on a $0 < n^{-s} \leq 2^{-s} < 1$ par stricte monotonie. La somme de la série géométrique de raison n^{-s} est donc l'inverse de $1 - n^{-s}$, i.e.

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

b) Pour $j \in \mathbf{N}$, la série $\sum_i u_{ij}$ est à termes positifs, de somme $\dfrac{1}{a^{is}(1 - b^{-s})}$ et donc

$$\boxed{\text{la série double est sommable et } S = \frac{1}{(1 - a^{-s})(1 - b^{-s})}.}$$

c) Puisque $s > 0$, la fonction $x \mapsto x^s$ est injective de $\mathbf{R}_+$ dans lui-même. L'application considérée est donc injective en tant que composée de deux telles fonctions car $(\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (p_1)^{\alpha_1}(p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n}$ est injective d'après le théorème fondamental de l'arithmétique. Comme $\mathbf{N}^n$ est dénombrable, M aussi et on peut donc ordonner ses éléments dans l'ordre croissant.

L'application $(\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (p_1)^{s\alpha_1}(p_2)^{s\alpha_2} \ldots (p_n)^{s\alpha_n}$, de $\mathbf{N}^n$ dans M_n est injective et il est possible d'indexer les réels m de M dans l'ordre croissant.

Si $n = 2$ et $s = 1$, M est formé de nombres donc la décomposition en facteurs premiers ne fait apparaître que 2 et 3, i.e. 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27 etc.

Si $n = 3$, on ajoute à cette liste les nombres ayant 5 dans leur décomposition en facteurs premiers, i.e. 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16 etc.

d) Soit k dans $[\![1, n]\!]$, comme $k \leq n$, sa décomposition en facteurs premiers ne fait apparaître que des nombres premiers inférieurs à n et donc à p_N. Il en résulte $k^s \in M$, si $M = \left\{ m \mid \exists (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbf{N}^N, m = (p_1)^{s\alpha_1}(p_2)^{s\alpha_2} \ldots (p_N)^{s\alpha_N} \right\}$ et donc d'après le résultat admis

$$\sum_{k=1}^{n} k^{-s} \leq \sum_{i=0}^{+\infty} m_i^{-s} = \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1}$$

et il vient donc $\boxed{\displaystyle\sum_{k=1}^{n} \frac{1}{k^s} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1}.}$

En prenant $s = 1$ et en supposant que la suite des nombres premiers est finie, de cardinal N, on en déduit que la série harmonique est bornée par $\displaystyle\prod_{i=1}^{N} (1 - p^{-1})^{-1}$. Comme elle est à termes positifs, elle serait convergente. Cette contradiction assure que

la suite des entiers premiers est illimitée.

D'après le critère de Riemann, la série $\sum k^{-s}$ est divergente pour $0 < s \leq 1$. Par ailleurs lorsque N tend vers l'infini p_N aussi, puisque la suite des nombres premiers est infinie.

D'après le résultat précédent, on a $\sum_{k=1}^{p_N} \frac{1}{k^s} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1}$ et donc, par comparaison, $\boxed{\text{pour } 0 < s \leq 1,\ \lim_n f_n(s) = +\infty.}$

e) La première partie de l'encadrement a déjà été démontrée. D'après la relation admise, on a

$$\prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1} = \sum_{i=0}^{+\infty} m_i^{-s} \leq \sum_{i=1}^{+\infty} i^{-s}$$

puisque la série de droite est convergente et majore toutes les sommes partielles de celle du milieu puisque c'est une série à termes positifs qui contient tous les termes de la série du milieu. D'où $\boxed{\sum_{k=1}^{n} \frac{1}{k^s} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1} \leq \sum_{k=1}^{\infty} \frac{1}{k^s}.}$ On en déduit

$$\sum_{k=1}^{p_N} \frac{1}{k^s} \leq \prod_{i=1}^{N} \left(1 - \frac{1}{p_i^s}\right)^{-1} \leq \sum_{k=1}^{+\infty} \frac{1}{k^s}\ .$$

Le théorème d'encadrement des limites permet de conclure $\boxed{\lim_n f_n(s) = \sum_{k=1}^{+\infty} \frac{1}{k^s}.}$

I.3) On a $f_n(1) > 0$ en tant que produit de termes strictement positifs et il vient $-\ln(f_n(1)) = \sum_{i=1}^{n} \ln(1 - p^{-1}) = \sum_{i=1}^{n} v_i$. Il résulte de I.2d) et de $\lim_{+\infty} \ln = +\infty$, que $\boxed{\sum v_i \text{ diverge vers } -\infty.}$

Comme $v_i \sim -w_i$, puisque $\lim p_i^{-1} = 0$, le théorème de comparaison des séries à termes de signes constants, permet d'en déduire que $\boxed{\sum w_i \text{ diverge vers } +\infty.}$

$\boxed{\text{Il y a donc relativement beaucoup de nombres premiers, plus que des carrés par exemple.}}$

I.4) On considère la série de fonctions $-\sum \ln(k) k^{-s}$ pour $s \in]1, \infty[$. C'est une série normalement convergente sur tout compact et même sur tout intervalle de la forme $[a, +\infty[$, avec $1 < a$. En effet

$$\sup_{a \leq s} \ln(k) k^{-s} = \ln(k) k^{-a} = o(k^{-(1+a)/2})$$

et la série des normes converge donc, par le critère de Riemann. Comme ζ converge simplement sur $]1, +\infty[$ d'après ce qui précède, le théorème de dérivation des séries de fonctions montre que ζ est de classe C^1 sur $]a, +\infty[$. Il en résulte que $\boxed{\zeta \text{ est continûment dérivable sur }]1, +\infty[.}$

PARTIE II

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'est pas premier, $P_{n+1} = P_n$. Comme $4^{n+1} > 4n$, il vient :

si l'entier $n+1$ n'est pas premier, l'inégalité $P_n \leq 4^n$ implique l'inégalité $P_{n+1} \leq 4^{n+1}$.

c) Si $n+1$ est premier, comme $n+1 \geq 2+1 = 3$, c'est un nombre premier impair et donc il existe un entier m tel que : $2m+1 = n+1$.

Soit p un nombre premier compris entre $m+2$ et $n+1$. Comme $\binom{2m+1}{m} m!$ est le produit des nombres entiers compris entre $m+2$ et $n+1$, il est divisible par p. Mais p est premier à $m!$ puisque $p > m$, donc d'après le lemme de Gauss, p divise $\binom{2m+1}{m}$.

On a $\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1} = 2.4^m$, d'après la formule du binôme de Newton. Par symétrie on a donc $\sum_{k=0}^{m} \binom{2m+1}{k} = \sum_{k=m+1}^{2m+1} \binom{2m+1}{k} = 4^m$ et en particulier, puisque c'est une somme à termes positifs, $\binom{2m+1}{m} \leq 4^m$.

Puisque tous les nombres premiers compris entre $m+2$ et $n+1$ divisent $\binom{2m+1}{m}$, et puisqu'ils sont tous premiers entre eux, leur produit divise aussi $\binom{2m+1}{m}$. Il en résulte que ce produit est inférieur à 4^m. Comme P_{2m+1} est le produit de P_{m+1} et de ce produit et que $4^{m+1}4^m = 4^{2m+1}$, l'inégalité $P_{m+1} \leq 4^{m+1}$ implique l'inégalité $P_{n+1} \leq 4^{n+1}$.

d) Les deux questions précédentes montre que la propriété $\forall k \leq n,\ P_k \leq 4^k$ est héréditaire, pour n entier supérieur à 2 (puisque $m+1 < 2m+1$ si $n+1 = 2m+1 \geq 3$). Comme elle est vraie pour $n = 2$ d'après le tableau établi en II.1a), par le principe de récurrence

pour tout entier $n \geq 2$, $P_n = \prod_{i=1}^{N} p_i \leq 4^n$.

II.2) Par définition le ppcm d_n est obtenu comme le produit de tous les nombres premiers divisant l'un des nombres entiers 1, 2, …, n, chacun étant élevé à la plus grande puissance apparaissant dans la décomposition de ces nombres en facteurs premiers. Soit p^k divisant l'un des nombres entiers 1, 2, …, n, avec p premier et $k \in \mathbf{N}^*$, alors $p \leq p^k \leq n$ et donc $p = p_i$ pour $i \leq N$ et $k \leq \dfrac{\ln(n)}{\ln(p)}$. Réciproquement $p^{[\ln(n)/\ln(p)]}$ est inférieur à n (et supérieur à 1) et se divise lui-même, donc divise d_n, i.e. $d_n = \prod_{i=1}^{N} p_i^{\left[\frac{\ln(n)}{\ln(p_i)}\right]}$.

II.3) a) Par inégalité entre moyenne géométrique et arithmétique, pour x dans $[0,1]$, $x^n(1-x)^n \leq \left(\dfrac{1}{2}\right)^{2n} = 4^{-n}$. L'inégalité de la moyenne donne donc $I_n \leq \dfrac{1}{4^n}$.

b) On a $I_n = \displaystyle\int_0^1 x^n \left(\sum_{k=0}^{n}(-1)^k\binom{n}{k}x^k\right) \mathrm{d}x$ ou encore $d_{2n+1}I_n = \displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{d_{2n+1}}{n+k+1}$, par linéarité de l'intégrale. Comme d_{2n+1} est un ppcm, il est divisible par tous les nombres entiers compris entre 1 et $2n+1$ et donc a fortiori entre $n+1$ et $2n+1$. Il en résulte

$\boxed{d_{2n+1} \text{ est divisible par tout entier } n+k+1, \text{ pour } 0 \leq k \leq n, \text{ et } d_{2n+1}I_n \text{ est un entier.}}$

Comme I_n est l'intégrale d'une fonction continue non identiquement nulle et positive sur $[0,1]$, $I_n > 0$ et donc $d_{2n+1}I_n > 0$. Il en résulte, puisqu'on affaire à un entier, $d_{2n+1}I_n \geq 1$ et il vient $\boxed{d_{2n+1} \geq 4^n.}$

PARTIE III

III.1) La fonction H_A est en escalier et constante sur les intervalles $[1,2[$, ainsi que $[p_i, p_{i+1}[$, pour $i \in \mathbf{N}^*$. Elle est donc continue sur $[1,+\infty[$ sauf peut-être en les nombres premiers. Pour i dans $\mathbf{N}^*$, on a $H_A(p_i) - \lim\limits_{\substack{y\to p_i \\ y<p_i}} H_A(y) = a_i$. D'où

$\boxed{\begin{array}{l} H_A \text{ est continue sur tous les intervalles inclus dans } [1,+\infty[\text{ privé des nombres premiers } p_i \\ \text{avec } i \in \mathbf{N}^* \text{ et } a_i \neq 0\,; \text{ les plus grands intervalles étant les composantes connexes par arcs} \\ \text{de cet ensemble. En les points de discontinuité, on a } H_A(p_i) - \lim\limits_{\substack{y\to p_i \\ y<p_i}} H_A(y) = a_i. \end{array}}$

Pour $i \in \mathbf{N}^*$ avec $i < N$, on a, puisque H_A est constante sur $[p_i, p_{i+1}[$, $\displaystyle\int_{p_i}^{p_{i+1}} H_A(t)f'(t)\,\mathrm{d}t = H_A(p_i)\left(f(p_{i+1}) - f(p_i)\right)$. Il en résulte, par la relation de Chasles,

$$\int_2^{p_N} H_A(t)f'(t)\,\mathrm{d}t = \sum_{i=1}^{N-1} H_A(p_i)\left(f(p_{i+1}) - f(p_i)\right)$$

ou encore, en effectuant une transformation d'Abel,

$$\int_2^{p_N} H_A(t)f'(t)\,\mathrm{d}t = -f(p_1)H_A(p_1) + \sum_{i=2}^{N-1} f(p_i)\left(H_A(p_{i-1}) - H_A(p_i)\right) + f(p_N)H_A(p_{N-1})\,.$$

Or $H_A(p_1) = a_1$ et donc

$$\int_2^{p_N} H_A(t)f'(t)\,\mathrm{d}t = -\sum_{i=1}^{N-1} a_i f(p_i) + f(p_N)H_A(p_{N-1})\,.$$

Enfin, comme H_A est constante sur $[p_N, x]$ et égale à $H_A(p_N)$, il vient

$$\int_2^{x} H_A(t)f'(t)\,\mathrm{d}t = -\sum_{i=1}^{N-1} a_i f(p_i) + f(p_N)H_A(p_{N-1}) + H_A(p_n)(f(x) - f(p_N))\,.$$

Comme $H_A(p_N) = H_A(x)$, il vient finalement $\boxed{\displaystyle\sum_{i=1}^{N} a_i f(p_i) = H_A(x)f(x) - \int_2^x H_A(t)f'(t)\,\mathrm{d}t.}$

III.2) a) Par définition $\theta(x)$ est le logarithme du produit des nombres premiers inférieurs à x, i.e. de $P_{[x]}$. D'après II.1d), on a donc, par croissance du logarithme, $\theta(x) \leq [x]\ln(4)$ et donc $\boxed{\theta(x) \leq x\ln(4).}$

b) Remarquons que f est de classe C^∞ sur $[2,+\infty[$ en tant qu'inverse d'une telle fonction qui ne s'annule pas. Le choix proposé par l'énoncé est donc licite. Avec ce choix, on a $\sum_{i=1}^N a_i f(p_i) = \sum_{i=1}^N 1 = \pi(x)$. De plus $H_A = \theta$. Il en résulte, par positivité sur $[1,+\infty[$, $H_A(x)f(x) \leq x\ln(4)f(x)$. De plus $f'(x) = -\dfrac{1}{x(\ln(x))^2}$ et donc l'intégrale de la question III.1 se récrit $-\displaystyle\int_2^x H_A(t)f'(t)\,\mathrm{d}t = \int_2^x \frac{\theta(t)}{t(\ln(t))^2}\,\mathrm{d}t$. Par inégalité de la moyenne, cette dernière expression est majorée par $\displaystyle\int_2^x \frac{\ln(4)}{(\ln(t))^2}\,\mathrm{d}t$ et il vient

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

c) Pour $x \geq 4$, on peut écrire, puisque f^2 est décroissante,

$$0 \leq \int_2^{\sqrt{x}} \frac{\mathrm{d}t}{(\ln(t))^2}\,\mathrm{d}t \leq \frac{\sqrt{x}-2}{(\ln(2))^2} = O(\sqrt{x}) = o\left(\frac{x}{\ln(x)}\right)$$

et

$$0 \leq \int_{\sqrt{x}}^x \frac{\mathrm{d}t}{(\ln(t))^2}\,\mathrm{d}t \leq \frac{x-\sqrt{x}}{\left(\frac{1}{2}\ln(x)\right)^2} = O\left(\frac{x}{(\ln(x))^2}\right) = o\left(\frac{x}{\ln(x)}\right)$$

et donc, par la relation de Chasles, $\boxed{\lim_{x\to+\infty} R(x) = 0.}$

d) On dispose, d'après la question précédente, de x_0 tel que, pour tout réel x supérieur ou égal à x_0, $0 \leq R(x) \leq 1$; on a alors aussi $\pi(x) \leq 2\ln(4)\dfrac{x}{\ln(x)}$, i.e. $\boxed{\pi(x) \leq 4\ln(2)\dfrac{x}{\ln(x)}.}$

III.3) Pour $x \geq 3$, soit n l'entier vérifiant $3 \leq 2n+1 \leq x < 2n+3$. Comme $2n \geq 4$, $2n$ n'est pas premier et donc $p_N \leq 2n+1 \leq x < p_{N+1}$. D'après II.3b) et II.2), on a, par croissance du logarithme,

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

Comme $x < 2n+3$ et, pour i dans $[\![1,N]\!]$, $\ln(p_i) \geq 0$ et $\left[\dfrac{\ln(2n+1)}{\ln(p_i)}\right] \leq \dfrac{\ln(2n+1)}{\ln(p_i)}$,

$$\frac{x-3}{2}\ln(4) \leq \sum_{i=1}^N \frac{\ln(2n+1)}{\ln(p_i)}\ln(p_i) = N\ln(2n+1) = \pi(x)\ln(2n+1) \leq \pi(x)\ln(x).$$

Le terme de gauche est équivalent à $x\ln(2)$ et donc supérieur à $x\dfrac{\ln(2)}{2}$ pour x suffisamment grand, i.e. en divisant par $\ln(x)$, qui est strictement positif, on dispose d'un réel x_1 tel que, pour tout réel supérieur à x_1, $\boxed{\pi(x) \geq \dfrac{\ln(2)}{2}\dfrac{x}{\ln(x)}.}$

PARTIE IV

IV.1) a) On a $\boxed{\varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2,\ \varphi(5) = 4,\ \varphi(6) = 2 \text{ et } \varphi(7) = 6.}$ La première question est du cours.

b) $\boxed{(\mathbf{Z}/n\mathbf{Z})^\times \text{ est un groupe multiplicatif de cardinal } \varphi(n).}$

D'après le théorème de Lagrange (hors-programme) $\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}.}$

c) On a $251 \equiv -1 \pmod 6$ et donc $\boxed{\text{le reste de la division de } 251^{311} \text{ par 6 est 5.}}$

IV.2) a) D'après le théorème des restes chinois $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ et on a affaire à un isomorphisme d'anneaux. En prenant les éléments inversibles de chacun puis les cardinaux, il vient, puisque $\mathbf{Z}/p\mathbf{Z}$ et $\mathbf{Z}/q\mathbf{Z}$ sont des corps, $\boxed{\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1).}$

b) Puisque e est premier à $(p-1)(q-1)$, il est inversible dans $\mathbf{Z}/(p-1)(q-1)\mathbf{Z}$, i.e. $\boxed{\text{il existe un entier } d \text{ tel que } ed \equiv 1 \pmod{(p-1)(q-1)}.}$

On a $n = 2 \times 3$ et donc $(p-1)(q-1) = 2$. On a donc $ed \equiv 1 \pmod 2$. Or l'application $\overline{a} \mapsto \overline{a}^k$ est périodique de période 2 et donc $\boxed{\overline{a}^{ed} = \overline{a}.}$

c) La relation à démontrer est, par le théorème chinois, équivalente aux deux relations obtenues en remplaçant n par p et q. Si a est inversible modulo p, $k \mapsto a^k$ est $\varphi(p)$-périodique puisque $a^{\varphi(p)} \equiv 1 \pmod p$ et donc $a^{ed} \equiv a \pmod p$. Si a n'est pas inversible modulo p, il est nul modulo p et donc $a^{ed} \equiv 0 \pmod p$. Dans tous les cas $a^{ed} \equiv a \pmod p$. En échangeant le rôle de p et q, il vient donc

$\boxed{\text{pour tout élément } \overline{a} \text{ de } \mathbf{Z}/n\mathbf{Z}, \text{ on a } a^{e.d} \equiv a \pmod{n}.}$