DIFFERENTS RESULTATS D'ARITHMETIQUE

DM MPSI3 2024-2025 LYCÉE PIERRE DE FERMAT
A FAIRE À DEUX. A RENDRE POUR LE 10 JANVIER

Préliminaires

Ce sujet est très largement inspiré de l'épreuve du concours Mines-Pont MP 2002 - Seconde épreuve.
Il y était écrit : *Il est conseillé aux Candidats de lire le problème en entier. Les deuxième et quatrième parties peuvent être abordées indépendamment des parties précédentes.*

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, $i = 1, 2\ldots$:

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

On note $\mathcal{P}$, l'ensemble des nombres premiers. Comme $\mathcal{P}$ est infin (Question I.1.), il est admis qu'à tout réel x supérieur ou égal à 2, peut être associé un entier $N(x)$ (simplifié si cela ne crée aucune confusion en N) tel que : $p_{N(x)} \leqslant x < p_{N(x)+1}$.
Dans tous le problème la lettre p est réservée aux nombre premiers. Etant donné un réel x, sa partie entière (inférieure) $\lfloor x \rfloor$ est l'entier n qui vérifie la double inégalité suivante :

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

On pourra être amené à exploiter la relation $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \geqslant \ln n$.

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.
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 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 et s est un réel donné strictement positif.

(2) Sommabilité (somme multiple de termes positifs)

(a) Justifier que la suite $\left(\displaystyle\sum_{k=0}^{m} \frac{1}{n^{ks}}\right)_m$ est convergente et que sa limite vaut $\left(1 - \frac{1}{n^s}\right)^{-1}$.
On notera cette limite : $\displaystyle\sum_{k=0}^{+\infty} \frac{1}{n^{ks}}$. On a donc $\displaystyle\sum_{k=0}^{+\infty} \frac{1}{n^{ks}} = \left(1 - \frac{1}{n^s}\right)^{-1}$.

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

(i) Montrer que pour tout $K \in \mathbb{N}_f^2$, $\displaystyle\sum_{(i,j)\in K} u_{i,j} \leqslant \left(1 - \frac{1}{a^s}\right)^{-1} \left(1 - \frac{1}{b^s}\right)^{-1}$.

Indication : on pourra montrer que si $K \neq \emptyset$, il existe i_K et j_K tel que $K \subset [\![0, i_K]\!] \times [\![0, j_K]\!]$.

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

(iii) En déduire que $\left\{ \sum_{(i,j)\in K} u_{i,j} \ ; \ K \subset \mathbb{N}_f^2 \right\}$ admet une borne supérieure notée $\sum_{(i,j)\in\mathbb{N}^2} u_{i,j}$, et on dit que la famille $(u_{i,j})_{(i,j)\in\mathbb{N}^2}$ à termes positifs est sommable.
Que vaut $\sum_{(i,j)\in\mathbb{N}^2} u_{i,j}$?

(3) Ensemble M_n.
Soient p_1, p_2,... 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) Démontrer que l'application $\Omega : (\alpha_1, \alpha_2, \cdots, \alpha_n) \mapsto (p_1)^{s\alpha_1} \times (p_2)^{s\alpha_2} \times \cdots \times (p_n)^{s\alpha_n}$, de $\mathbb{N}^n$ dans M_n est injective.

(b) Pourquoi est-il possible d'indexer les réels m de M_n dans l'ordre croissant ? Ainsi, on considère l'application $i \mapsto m_i$, strictement croissante de $\mathbb{N}^*$ dans M_n.
Exemple : écrire la suite des 12 premiers termes de la suite $(m_i)_{i\in\mathbb{N}^*}$ lorsque le réel s est égal à 1 et l'entier n à 2 puis à 3.

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 $N = \max\{i \mid p_i \leqslant n\}$
Démontrer l'inégalité suivante :

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

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

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

(e) Etablir lorsque le réel s est strictement supérieur à 1 ($s > 1$), l'encadrement ci-dessous :

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

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

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 ($P_n = \prod_{i=1}^{N} p_i$).

(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 la valeurs de N, p_N, P_n et 4^n.

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

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

(i) Justifier l'existence d'un entier m tel que : $2m + 1 = n + 1$

(ii) Démontrer que tout nombre premier p compris entre $m+2$ et $n+1$ divise le coefficient $\binom{2m+1}{m}$.

(iii) Etablir que l'inégalité $P_{m+1} \leqslant 4^{m+1}$ implique l'inégalité $P_{n+1} \leqslant 4^{n+1}$

(d) En déduire, pour tout entier $n \geqslant 2$, la majoration

$$P_n = \prod_{i=1}^{N} p_i \leqslant 4^n$$

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

(2) 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 :

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

(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 :

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

(a) Démontrer la majoration :

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

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

(c) Démontrer, à l'aide de la majoration de l'intégrale I_n une minoration du PPCM d_{2n+1}

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) Préciser, pour une suite $A = (a_i)_{i \geqslant 1}$ donnée, sur quels intervalles la fonction H_A est continue.
Quels sont ses points de discontinuité ? Préciser en ces points x la valeurs de $\lim\limits_{\epsilon \to 0^+} H_A(x) - H_A(x-\epsilon)$.

(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 $A = (a_i)_{i \geqslant 1}$.
Démontrer la relation suivante : pour tout réel x compris entre p_N et p_{N+1} ($p_N \leqslant x < p_{N+1}$), il vient :

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

(2) Une majoration de la fonction π.
(a) Démontrer la majoration suivante de la fonction θ :

$$\theta(x) \leqslant x \ln 4$$

(b) Etablir en choisissant, dans la relation établie à la question précédente, comme suite A, la suite $(\ln(p_k))_{k\geqslant 1}$ et comme fonction f la fonction $x \mapsto \frac{1}{\ln x}$, l'inégalité suivante :

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

(c) Démontrer la convergence vers 0, lorsque la réel x croît vers l'infini, de la fonction $R(x)$ suivante :

$$R(x) = \frac{\ln x}{x} \times \int_2^x \frac{\mathrm{d}t}{(\ln t)^2}$$

Indication : introduire, pour $x \geqslant 4$, 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 :

$$\pi(x) \leqslant 4 \ln 2 \times \frac{x}{\ln x}$$

(3) Un minoration de la fonction π.
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 :

$$\pi(x) \geqslant \frac{\ln 2}{2} \times \frac{x}{\ln x}$$

Ces 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 $x \mapsto \frac{x}{\ln x}$.

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) Démontrer que, pour que l'élément $\overline{a}$ de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ 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 $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ des éléments de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ inversibles est un groupe multiplicatif.
Quel est son cardinal ?

(c) Soit a un entier compris entre 0 et $n-1$ ($0 \leqslant a \leqslant n-1$) premier avec n. Démontrer la relation

$$\overline{a}^{\varphi(n)} = \overline{1} \qquad (\text{ou } a^{\varphi(n)} \equiv 1[n])$$

On pourra au choix adapter la démonstration vue en cours pour démontrer le petit théorème de Fermat, ou bien exploiter le sous-groupe monogène $< \overline{a} >$ de $\left(\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*, \times\right)$...

(d) Application. Déterminer le reste de la division de 251^{311} par 6.

(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) Démontrer la relation $\varphi(n) = (p-1)(q-1)$.
Soit e un nombre entier premier avec $(p-1)(q-1)$

(b) Etablir l'existence d'un entier d tel que

$$e \times d \equiv 1 \qquad [(p-1)(q-1)]$$

(c) Exemple simple : $n = 6$, $e = 5$. Calculer, pour tout élément $\overline{a}$ de $\dfrac{\mathbb{Z}}{6\mathbb{Z}}$, $\overline{a}^{ed}$.

(d) Démontrer pour tout élément $\overline{a}$ de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ 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.