Préparation aux Concours (Mines)

Sommabilité

Cet énoncé comporte 7 pages de texte.

Si, au cours de l'épreuve, un candidat repère ce qui lui semble être une erreur d'énoncé, il le signale sur sa copie et poursuit sa composition en expliquant les raisons des initiatives qu'il est amené à prendre.

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'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, $i = 1, 2, \ldots$:

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

Dans tout le problème la 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

$$p_N = \sup\{p \mid p \leq x\}$$

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 $1/p_i,\ i = 1, 2, \ldots$.

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 $p_1,\ p_2,\ \ldots,\ p_n$ donnés, l'entier Q défini à partir de ces n nombres premiers par la relation suivante :

$$Q = p_1.p_2.\ldots.p_n + 1 = \prod_{i=1}^{n} p_i + 1.$$

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 :

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

b. Soient 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 $u_{i\,j}$, $i = 0, 1, 2, \ldots,$ $j = 0, 1, 2, \ldots,$ défini par la relation suivante

$$u_{i\,j} = \frac{1}{a^{i\,s}.b^{j\,s}}, \quad i = 0, 1, 2, \ldots, \quad j = 0, 1, 2, \ldots.$$

est sommable. Déterminer sa somme S.

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

$$M_n = \left\{m \mid m = (p_1)^{s\,\alpha_1}.(p_2)^{s\,\alpha_2}.\ldots.(p_n)^{s\,\alpha_n}, \quad \alpha_i \in \mathbf{N}\right\}.$$

c. Démontrer que l'application $\left(\alpha_1,\ \alpha_2, ..., \alpha_n\right) \mapsto (p_1)^{s\,\alpha_1}.(p_2)^{s\,\alpha_2}.\ldots.(p_n)^{s\,\alpha_n}$, 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.

Exemples : 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 $v_i = 1/m_i,\ i \in \mathbf{N}^*,$ 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-dessous est vrai et est admis :

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

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 l'inégalité suivante :

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

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.

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} :

$$p_N \leq x < p_{N+1}.$$

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

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

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

I-3. Série de terme général $1/p_i$, $i = 1, 2, \ldots$:

Déduire des résultats ci-dessus la nature de la série de terme général v_i, $i = 1, 2, \ldots$, défini par la relation suivante.

$$v_i = \ln\left(1 - \frac{1}{p_i}\right).$$

En déduire la nature de la série de terme général :

$$w_i = \frac{1}{p_i}, \quad i = 1, 2, \ldots.$$

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 I-2.e sur la demi-droite ouverte $]1, \infty[$ par la relation ci-dessous, est continûment dérivable.

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

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 ($n \geq 2$), 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 :

$$p_N \leq n < p_{N+1}, \quad P_n = \prod_{i=1}^{N} p_i.$$

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 C^m_{2m+1}. Établir la majoration suivante :

$$C^m_{2m+1} \leq 4^m.$$

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 p. p. c. m. d_n :

Démontrer que le p. p. c. m. 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 :

$$p_N \leq n < p_{N+1}, \quad d_n = \prod_{i=1}^{N} p_i^{\alpha_i}, \quad \text{avec : } \alpha_i = \left[\frac{\ln n}{\ln p_i} \right].$$

II-3. Une minoration du p. p. c. m. $d_{2\,n+1}$:

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

$$I_n = \int_0^1 x^n \, (1-x)^n \, dx.$$

a. Démontrer la majoration :

$$I_n \leq \frac{1}{4^n}.$$

b. Démontrer que le p. p. c. m. $d_{2\,n+1}$ 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 $d_{2\,n+1}.I_n$ 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 p. p. c. m. $d_{2\,n+1}$.

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 ($x \geq 2$), $\pi(x)$ est égal au nombre des nombres premiers inférieurs ou égaux au réel x.

$$p_N \leq x < p_{N+1}, \quad \pi(x) = N = \sum_{i=1}^{N} 1.$$

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.

$$p_N \leq x < p_{N+1}, \quad \theta(x) = \sum_{i=1}^{N} \ln p_i.$$

Plus généralement : étant donnée 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 :

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

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 $H_A(x) - H_A(x-0)$.

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 :

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

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 $\ln p_k$, $k = 1, 2, ...,$ et comme fonction f, la fonction $x \mapsto 1/\ln x$, l'inégalité suivante :

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

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

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

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 :

$$\pi(x) \leq 4\, \ln 2\, \frac{x}{\ln x}.$$

III-3. **Une minoration de la fonction π** :

En utilisant par exemple la minoration du p. p. c. m. $d_{2\,n+1}$ 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 :

$$\pi(x) \geq \frac{\ln 2}{2}\, \frac{x}{\ln x}.$$

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 $x \mapsto x/\ln x$.

Quatrième partie

Soit, dans toute cette partie, un entier n donné ($n \geq 2$). L'anneau $\mathbf{Z}/n\mathbf{Z}$ est l'ensemble quotient de l'anneau $\mathbf{Z}$ par la relation d'équivalence : "deux entiers relatifs sont équivalents si leur différence est divisible par l'entier n". Classiquement un élément de $\mathbf{Z}/n\mathbf{Z}$, une classe d'équivalence, est notée $\bar{a}$, 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 $\bar{a}$ 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 toute valeur de 2 à 7.

b. Démontrer que l'ensemble $(\mathbf{Z}/n\mathbf{Z})^*$ 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 :

$$\bar{a}^{\varphi(n)} \equiv \bar{1}, \qquad (n).$$

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

$$c = \prod_{b \in (\mathbf{Z}/n\mathbf{Z})^*} \bar{b}.\bar{a}.$$

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 ; $n = p.q$.

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 :

$$\bar{e}.\bar{d} \equiv 1, \qquad \big((p-1)\,(q-1)\big).$$

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

c. Démontrer pour tout élément $\bar{a}$ de $\mathbf{Z}/n\mathbf{Z}$, la relation :

$$\bar{a}^{\,e.d} \equiv \bar{a}, \qquad (n).$$

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 : $a \rightarrow a^e$; déchiffrement par le destinataire : $a^e \rightarrow (a^e)^d$. Le message est retrouvé.

FIN DU PROBLÈME