

DEVOIR SURVEILLÉ N°5
CORRECTION

Sujet donné le samedi 17 janvier 2025, 4h.

QUELQUES RÉSULTATS SUR LES NOMBRES PREMIERS

Dans tout le problème, $\mathcal{P}$ désigne l'ensemble des nombres premiers. Pour tout n entier naturel non nul, on note $\mathcal{P}_n$ l'ensemble des nombres premiers inférieurs ou égaux à n . Par exemple, $\mathcal{P}_8 = \{2, 3, 5, 7\}$ et $\mathcal{P}_{11} = \{2, 3, 5, 7, 11\}$.

On utilise les conventions habituelles : une somme indexée par un ensemble vide est nulle, un produit indexé par un ensemble vide vaut 1.

Dans tout le problème, pour tout ensemble fini X , la notation $|X|$ désigne le cardinal de l'ensemble X , c'est-à-dire le nombre de ses éléments.

Partie I - Résultats préliminaires d'analyse

1. Soient u, v et w trois suites réelles telles que $u_n \underset{n \rightarrow +\infty}{\sim} v_n$ et $v_n \underset{n \rightarrow +\infty}{=} O(w_n)$.

Redémontrer alors que $u_n \underset{n \rightarrow +\infty}{=} O(w_n)$.

Par hypothèse, il existe deux suites (a_n) et (b_n) telles que à partir d'un certain rang :

$$u_n = v_n \times a_n \text{ avec } (a_n) \rightarrow 1 \text{ et } v_n = w_n \times b_n \text{ avec } (b_n) \text{ bornée.}$$

Donc, à partir d'un certain rang, $u_n = w_n \times (a_n \times b_n)$, avec $(a_n \times b_n)$ bornée,

car (a_n) est une suite convergente donc bornée et rappelons que le produit de deux suites bornées est une suite bornée.

donc $u_n \underset{n \rightarrow +\infty}{=} O(w_n)$.

2. Soient λ, μ deux réels strictement positifs et $\varphi_{\lambda, \mu} \left| \begin{array}{l}]0, +\infty[\rightarrow \mathbb{R} \\ x \mapsto x \ln x - \lambda x + \mu \end{array} \right.$.

a) Étudier les variations de $\varphi_{\lambda, \mu}$ et donner le tableau correspondant avec les limites aux bords du domaine de définition.

La fonction $\varphi_{\lambda, \mu}$ est continue et dérivable sur $\mathbb{R}_+^*$ et

$$\forall x \in \mathbb{R}_+^*, \varphi'_{\lambda, \mu}(x) = \ln x + 1 - \lambda = \ln x + \ln e^{1-\lambda} = \ln \left(\frac{x}{e^{\lambda-1}} \right)$$

d'où le tableau des variations

x	0	$e^{\lambda-1}$	$+\infty$
$\varphi'_{\lambda, \mu}(x)$	-	0	+
$\varphi_{\lambda, \mu}$	μ	$\searrow$ $\mu - e^{\lambda-1}$	$\nearrow$ $+\infty$

car

— $\varphi_{\lambda, \mu}(e^{\lambda-1}) = (\lambda - 1)e^{\lambda-1} - \lambda e^{\lambda-1} + \mu = \mu - e^{\lambda-1}$.

— $\lim_{x \rightarrow 0} \varphi_{\lambda, \mu}(x) = \mu$ car $\lim_{x \rightarrow 0} x \ln x = 0$ (croissances comparées),

— $\varphi_{\lambda, \mu}(x) = x \ln x \left(1 - \frac{\lambda}{\ln x} + \frac{\mu}{x \ln x} \right)$ donc $\lim_{x \rightarrow +\infty} \varphi_{\lambda, \mu}(x) = +\infty$.

b) Montrer que, pour tout entier naturel $n > e^\mu$ il existe une unique solution à l'équation d'inconnue $x \in \mathbb{R}_+^*$

$$\varphi_{\lambda,\mu}(x) = \ln(n)$$

On notera x_n cette solution pour $n \geq n_0 = \lfloor e^\mu \rfloor + 1$.

Soit un entier naturel $n > e^\mu$ fixé quelconque.

- L'étude des variations de $\varphi_{\lambda,\mu}$ a montré que,

$$\forall x \in [0, e^{\lambda-1}] , \varphi_{\lambda,\mu}(x) \leq \mu < \ln(n)$$

donc l'équation n'admet aucune solution dans l'intervalle $[0, e^{\lambda-1}]$.

- $\star \varphi_{\lambda,\mu}$ est continue sur $[e^{\lambda-1}, +\infty[$,
- $\star \varphi_{\lambda,\mu}$ est strictement croissante sur $[e^{\lambda-1}, +\infty[$,
- $\star \varphi_{\lambda,\mu}(e^{\lambda-1}) = \mu - \underbrace{e^{\lambda-1}}_{\geq 0} \leq \mu < \ln(n)$ et $\lim_{x \rightarrow +\infty} \varphi_{\lambda,\mu}(x) = +\infty$,

donc $\varphi_{\lambda,\mu}$ réalise une bijection de $[e^{\lambda-1}, +\infty[$ sur $[\varphi_{\lambda,\mu}(e^{\lambda-1}), +\infty[$ si bien que l'équation $\varphi_{\lambda,\mu}(x) = \ln(n)$ a une unique solution dans l'intervalle $[e^{\lambda-1}, +\infty[$.

Ainsi, l'équation $\varphi_{\lambda,\mu}(x) = \ln(n)$ d'inconnue $x \in \mathbb{R}_+^*$ admet une unique solution.

c) Montrer que la suite $(x_n)_{n \geq n_0}$ est croissante puis déterminer sa limite.

Notons g la restriction de $\varphi_{\lambda,\mu}$ à $[e^{\lambda-1}, +\infty[$ et corestrictée à $[\mu - e^{\lambda-1}, +\infty[$. La fonction g est ainsi bijective et

$$\forall n \in \mathbb{N}, x_n = g^{-1}(n).$$

De plus, comme g est strictement croissante, alors g^{-1} est strictement croissante.

Soit $n \in \mathbb{N}$.

$$\begin{aligned} n &< n+1 \\ g^{-1}(n) &< g^{-1}(n+1) \\ x_n &< x_{n+1}. \end{aligned}$$

Ainsi,

la suite (x_n) est croissante.

De plus, $\lim_{x \rightarrow +\infty} g^{-1}(x) = +\infty$, donc

$$\lim_{n \rightarrow +\infty} x_n = +\infty.$$

d) Justifier que $x_n \ln(x_n) \underset{n \rightarrow +\infty}{\sim} \ln(n)$. En déduire un équivalent de $\ln(x_n)$ et conclure que $x_n \underset{n \rightarrow +\infty}{\sim} \frac{\ln(n)}{\ln(\ln(n))}$.

- Par définition de x_n ,

$$\ln(n) = x_n \ln x_n - \lambda x_n + \mu$$

or, puisque $\lim_{n \rightarrow +\infty} x_n = +\infty$,

$$\frac{\lambda x_n + \mu}{x_n \ln x_n} = \frac{\lambda}{\ln x_n} + \frac{\mu}{x_n \ln x_n} \xrightarrow{n \rightarrow +\infty} 0$$

donc $\lambda x_n + \mu \underset{n \rightarrow +\infty}{=} o(x_n \ln x_n)$. Ainsi

$$\ln(n) \underset{n \rightarrow +\infty}{=} x_n \ln x_n + o(x_n \ln x_n)$$

$$\boxed{\text{donc } x_n \ln x_n \underset{n \rightarrow +\infty}{\sim} \ln(n)}$$

- L'équivalent ci-dessus est équivalent à l'écriture asymptotique

$$\ln(n) \underset{n \rightarrow +\infty}{=} x_n \ln x_n + o(x_n \ln x_n) \underset{n \rightarrow +\infty}{=} x_n \ln(x_n)(1 + o(1))$$

sur laquelle nous pouvons prendre le logarithme dont on utilise la propriété de morphisme :

$$\ln(\ln(n)) \underset{n \rightarrow +\infty}{=} \ln x_n + \ln \ln x_n + \ln(1 + o(1))$$

Or,

— d'après les croissances comparées, $\frac{\ln X}{X} \xrightarrow{X \rightarrow +\infty} 0$ et $\ln x_n \xrightarrow{n \rightarrow +\infty} +\infty$ donc, par composition des limites, $\frac{\ln \ln x_n}{\ln x_n} \xrightarrow{n \rightarrow +\infty} 0$ si bien que

$$\ln \ln x_n \underset{n \rightarrow +\infty}{=} o(\ln x_n)$$

— $\ln(1 + o(1)) \xrightarrow{n \rightarrow +\infty} 0$ et $\ln x_n \xrightarrow{n \rightarrow +\infty} +\infty$ donc $\frac{\ln(1 + o(1))}{\ln x_n} \xrightarrow{n \rightarrow +\infty} 0$ si bien que

$$\ln(1 + o(1)) \underset{n \rightarrow +\infty}{=} o(\ln x_n)$$

donc

$$\ln(\ln(n)) \underset{n \rightarrow +\infty}{=} \ln x_n + o(\ln x_n)$$

$$\boxed{\text{donc } \ln x_n \underset{n \rightarrow +\infty}{\sim} \ln(n).}$$

- La relation $x_n \ln x_n \underset{n \rightarrow +\infty}{\sim} \ln(n)$ donne, sachant que $\ln x_n \underset{n \rightarrow +\infty}{\sim} \ln(\ln(n))$, $x_n \ln \ln(n) \underset{n \rightarrow +\infty}{\sim} \ln(n)$

$$\boxed{\text{Ainsi, } x_n \underset{n \rightarrow +\infty}{\sim} \frac{\ln(n)}{\ln(\ln(n))}.}$$

3.a) Montrer que, pour tout $k \in \mathbb{N}$ tel que $k \geq 2$, $\int_{k-1}^k \ln(t) dt \leq \ln(k)$ puis en déduire que, pour tout $n \in \mathbb{N}$ supérieur ou égal à 1 :

$$n \ln(n) - n + 1 \leq \ln(n!) \leq n \ln(n)$$

- La fonction logarithme est croissante sur $]0, +\infty[$ donc, pour tout $k \geq 2$,

$$\forall t \in [k-1, k], \ln t \leq \ln k.$$

Comme $k-1 \leq k$, par croissance de l'intégrale,

$$\int_{k-1}^k \ln t dt \leq \int_{k-1}^k \ln k dt = \ln k.$$

- Soit $n \geq 1$ fixé quelconque.

★ Si $n = 1$, $n \ln(n) - n + 1 = \ln 1 - 1 + 1 = 0$ et $\sum_{k=2}^1 \ln k = 0$ (par convention pour une somme indexée par un ensemble vide) donc l'égalité cherchée est vraie.

★ Sinon, $n \geq 2$, sommons les inégalités établies dans le premier point pour $k \in \llbracket 2, n \rrbracket$, afin d'obtenir d'après la relation de Chasles,

$$\begin{aligned} \sum_{k=2}^n \int_{k-1}^k \ln(t) dt &\leq \sum_{k=2}^n \ln(k) \\ \int_1^n \ln(t) dt &\leq \ln(n!) \\ [t \ln(t) - t]_1^n &= n \ln(n) - n + 1 \leq \ln(n!). \end{aligned}$$

$$\boxed{\text{Ainsi, } \forall n \in \mathbb{N}^*, n \ln(n) - n + 1 \leq \ln(n!).}$$

- ★ Si $n = 1$, $n \ln(n) - n + 1 = 0$, $\ln(n!) = \ln 1 = 0$ et $n \ln(n) = \ln 1 = 0$ donc les 3 membres sont égaux,

★ Sinon, $n \geq 2$.

Par ailleurs, une somme de termes est toujours majorée par le plus grand d'entre eux fois le nombre de termes donc

$$\ln(n!) = \sum_{k=1}^n \ln(k) \leq n \ln(n).$$

$$\boxed{\text{Ainsi, } \forall n \in \mathbb{N}^*, n \ln(n) - n + 1 \leq \ln(n!) \leq n \ln(n).}$$

b) En déduire un équivalent de $(\ln(n!))$.

On divise par $n \ln n > 0$ pour $n > 1$:

$$1 - \frac{n-1}{n \ln n} \leq \frac{\ln n!}{n \ln n} \leq 1$$

Le deux termes extrêmes de cette relation converge vers 1. Le théorème de convergence par encadrement (dit des gendarmes), permet d'affirmer que $\left(\frac{\ln n!}{n \ln n}\right)_n$ converge et sa limite vaut 1.

$$\boxed{\ln n! \sim n \ln n}$$

Partie II - Résultats préliminaires d'arithmétique

On considère un entier $n \geq 2$ et un nombre premier p . On rappelle que, pour tout a entier, $v_p(a)$ désigne la valuation p -adique de a , c'est-à-dire le plus grand entier naturel k tel que p^k divise a .

4. Pour tout entier $k \geq 0$, on considère les sous-ensembles finis U_k , $\overline{U_k}$ et Ω_k de $\mathbb{N}$ définis par :

$$U_k = \{a \in \{1, 2, \dots, n\} \mid p^k \text{ divise } a\} \text{ et } \overline{U_k} = \{a \in \{1, 2, \dots, n\} \mid p^k \text{ ne divise pas } a\}$$

$$\Omega_k = \{a \in \{1, 2, \dots, n\} \mid v_p(a) = k\}$$

a) Justifier qu'il existe un plus grand entier $k_p \geq 0$ tel que $p^{k_p} \leq n$. Montrer que $k_p \geq 0$ et expliciter k_p en fonction de n et p . On exploitera la fonction partie entière.

La suite $(p^k)_{k \in \mathbb{N}}$ diverge vers $+\infty$. Donc pour tout A , $\exists N \in \mathbb{N}$ tel que $\forall n \geq N$, $p^n \geq A + 1 > A$.

En donnant à A la valeur n , on a donc $\{k \in \mathbb{N} \mid p^k \leq n\}$ est majoré par $N - 1$.

Ainsi, comme $p^0 = 1 \leq n$, l'ensemble $\{k \in \mathbb{N} \mid p^k \leq n\}$ est inclus dans $\mathbb{N}$, non vide et majoré.

Il admet un plus grand élément k_p et donc $p^{k_p} \leq n < p^{k_p+1}$.

En composant par le logarithme, fonction croissante (ces nombres sont positifs), puis en divisant par $\ln p > 0$ (car $p > 1$), on trouve :

$$k_p \leq \frac{\ln(n)}{\ln p} < k_p + 1$$

Or k_p est un nombre entier, il s'agit exactement de la définition de la partie entière :

$$k_p \text{ existe bien et } k_p = \left\lfloor \frac{\ln(n)}{\ln p} \right\rfloor.$$

b) Montrer que pour tout $k \in \{0, \dots, k_p\}$, l'ensemble U_{k+1} est strictement inclus dans U_k et que pour $k > k_p$, $U_k = \emptyset$.

Soit $k \in \{0, \dots, k_p\}$.

Soit $x \in U_{k+1}$, donc $x \in \{1, 2, \dots, n\}$ et $p^{k+1} | x$, ainsi $p^k | x$ par transitivité car $p^k | p^{k+1}$.

Donc $x \in U_k$. Et ainsi $U_{k+1} \subset U_k$.

Par ailleurs, puisque $p^{k_p} \leq n$, alors pour tout $k \leq k_p$, $p^k \leq p^{k_p} \leq n$, et comme $p^k | p^k$, on a : $p^k \in U_k$.

Alors que p^{k+1} ne divise pas p^k , donc $p^k \notin U_{k+1}$ et donc

$$\text{pour tout } k \in \{0, 1, \dots, k_p\}, U_{k+1} \text{ est strictement inclus dans } U_k.$$

Enfin, si $k > k_p$, alors comme ce sont des nombres entiers $k \geq k_p + 1$ et donc $p^k \geq p^{k_p+1} > n$.

Il n'y a donc aucun nombre compris entre 1 et n , divisible par p^k .

$$\text{Ainsi pour } k > k_p, U_k \text{ est vide.}$$

c) Prouver que la famille des parties $(\Omega_0, \Omega_1, \dots, \Omega_{k_p})$ forme une partition de l'ensemble $\{1, 2, \dots, n\}$.

Soit $(k, h) \in \{1, \dots, k_p\}^2$.

Si $a \in \Omega_k \cap \Omega_h$, alors $v_p(a) = k = h$.

Ainsi si $k \neq h$, alors $\Omega_k \cap \Omega_h = \emptyset$. La réunion est donc disjointe.

Soit $a \in \{1, 2, \dots, n\}$, alors $a \leq n$. Or $p^{v_p(a)} | a$, donc $p^{v_p(a)} \leq n$ et nécessairement $v_p(a) \leq k_p$.

Ainsi, il existe $\ell (= v_p(a)) \leq k_p$ tel que $a \in \Omega_\ell$.

$$\text{Ainsi } \{1, 2, \dots, n\} \subset \bigcup_{\ell=0}^{k_p} \Omega_\ell$$

Enfin, pour tout $\ell \leq k_p$, si $a \in \Omega_\ell$, alors $a \in \{1, 2, \dots, n\}$. Donc $\bigcup_{\ell=0}^{k_p} \Omega_\ell \subset \{1, 2, \dots, n\}$

$$\text{La famille des parties } (\Omega_0, \Omega_1, \dots, \Omega_{k_p}) \text{ forme une partition de l'ensemble } \{1, 2, \dots, n\}.$$

d) Montrer que pour tout $k \in \mathbb{N}$, $\Omega_k = U_k \cap \overline{U_{k+1}}$.

Soit $k \in \mathbb{N}$.

Soit $a \in \{1, 2, \dots, n\}$. On a les équivalences :

$$a \in \Omega_k \iff v_p(a) = k \iff p^k | a \text{ et } p^{k+1} \nmid a \iff a \in U_k \text{ et } a \notin U_{k+1}$$

$$\text{Ainsi, pour tout } k \in \mathbb{N}, \Omega_k = U_k \cap \overline{U_{k+1}}.$$

e) Calculer, pour tout $k \in \mathbb{N}$, $|U_k|$, $|\overline{U_k}|$, puis $|\Omega_k|$ en fonction de n et de p .

Soit $k \in \mathbb{N}$.

— On décrit $U_k : U_k = \{p^k, 2p^k \dots rp^k\}$ où $r \in \mathbb{N}$ vérifie : $rp^k \leq n$ et $(r+1)p^k > n$.

Cela donne $r \leq \frac{n}{p^k} < r+1$ et donc $r = \left\lfloor \frac{n}{p^k} \right\rfloor$. Or le cardinal de U_k est, par description, égal à

$$r. \text{ Donc } |U_k| = \left\lfloor \frac{n}{p^k} \right\rfloor.$$

— $\overline{U_k}$ est le complémentaire de U_k dans $\{1, 2, \dots, n\}$, donc

$$|\overline{U_k}| + |U_k| = |\{1, 2, \dots, n\}| = n.$$

$$\text{Ainsi, } |\overline{U_k}| = n - \left\lfloor \frac{n}{p^k} \right\rfloor.$$

— Enfin, $\Omega_k = U_k \cap \overline{U_{k+1}}$, donc $\Omega_k \cup U_{k+1} = (U_k \cap \overline{U_{k+1}}) \cup (U_k \cap U_{k+1})$,

car $U_{k+1} \subset U_k$, donc $U_k \cap U_{k+1} = U_{k+1}$.

Ainsi, en factorisant : $\Omega_k \cup U_{k+1} = U_k \cap (\overline{U_{k+1}} \cup U_{k+1}) = U_k$.

Et comme $\Omega_k \cap U_{k+1} = \emptyset$, donc a donc $|\Omega_k| + |U_{k+1}| = |U_k|$ et donc $|\Omega_k| = \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$.

Pour tout $k \in \mathbb{N}$, $|U_k| = \left\lfloor \frac{n}{p^k} \right\rfloor$, $|\overline{U_k}| = n - \left\lfloor \frac{n}{p^k} \right\rfloor$ et $|\Omega_k| = \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$.

f) Montrer que $v_p(n!) = \sum_{k=0}^{k_p} k |\Omega_k|$ et en déduire la formule de LEGENDRE

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Il s'agit d'une somme finie, car les termes sont nuls à partir du rang $k_p + 1$.

La fonction v_p est un morphisme logarithmique (cours), donc

$$v_p(n!) = v_p\left(\prod_{i=1}^n i\right) = \sum_{i=1}^n v_p(i) = \sum_{i \in \{1, 2, \dots, n\}} v_p(i) = \sum_{i \in \Omega_0 \cup \Omega_1 \cup \dots \cup \Omega_{k_p}} v_p(i)$$

On retrouve la formule de la sommation par paquets, car la réunion figurant en dernière somme est disjointe :

$$v_p(n!) = \sum_{k=0}^{k_p} \sum_{i \in \Omega_k} v_p(i) = \sum_{k=0}^{k_p} \sum_{i \in \Omega_k} k = \sum_{k=0}^{k_p} k |\Omega_k|$$

En remplaçant par la valeur trouvée précédemment (on commence la somme à 1 car pour $k=0$, $k|\Omega_k| = 0$) :

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{k_p} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) \\ &= \sum_{k=1}^{k_p} k \left\lfloor \frac{n}{p^k} \right\rfloor - k \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \\ &= \sum_{k=1}^{k_p} \left\lfloor \frac{n}{p^k} \right\rfloor + \sum_{k=1}^{k_p} (k-1) \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=1}^{k_p} k \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \\ &= \sum_{k=1}^{k_p} \left\lfloor \frac{n}{p^k} \right\rfloor + 0 \times \left\lfloor \frac{n}{p^1} \right\rfloor - \underbrace{k_p \left\lfloor \frac{n}{p^{k_p+1}} \right\rfloor}_{=0} \end{aligned}$$

où on aura reconnu un télescopage. Finalement, on retrouve la formule de LEGENDRE :

$$v_p(n!) = \sum_{k=1}^{k_p} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Remarque On peut aussi exploiter le symbole d'Iverson et une double somme.

On commence par noter que

$$v_p(i) = h \iff p|i, p^2|i, \dots, p^h|i, p^{h+1} \nmid i \dots \iff \sum_{k=1}^{+\infty} [p^k|i] = \underbrace{1+1+\dots+1}_{h \text{ termes}} + 0 + \dots = h$$

Donc $v_p(i) = \sum_{k=1}^{+\infty} [p^k|i]$ (en respectant la convention sur la somme vide). On notera qu'en réalité la somme est finie.

$$v_p(n!) = \sum_{i=1}^n v_p(i) = \sum_{i=1}^n \left(\sum_{k=1}^{+\infty} [p^k|i] \right) = \sum_{k=1}^{+\infty} \left(\sum_{i=1}^n [p^k|i] \right)$$

$$v_p(n!) = \sum_{k=1}^{+\infty} |U_i| = \sum_{k=1}^{+\infty} |\{p^k, 2p^k, \dots, rp^k\}| = \sum_{k=1}^{+\infty} r$$

$$\text{où } rp^k \leq n < (r+1)p^k \iff r = \left\lfloor \frac{n}{p^k} \right\rfloor.$$

5. On s'intéresse maintenant à la valuation du coefficient binomial : $v_p \left(\binom{2n}{n} \right)$.

a) En utilisant les questions précédentes, déterminer une expression de $v_p \left(\binom{2n}{n} \right)$ faisant intervenir une somme de parties entières.

On exploite toujours la propriété de morphisme, ainsi que l'écriture sous forme de produit de factorielles

$$v_p \left(\binom{2n}{n} \right) = v_p \left(\frac{(2n)!}{n!n!} \right) = v_p((2n)!) - 2v_p(n!)$$

$$v_p \left(\binom{2n}{n} \right) = \sum_{k=1}^{+\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor$$

b) Montrer que $v_p \left(\binom{2n}{n} \right) \leq \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor$

Notons d'abord, comme précédemment $k'_p = \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor$ de sorte que $p^{k'_p} \leq 2n < p^{k'_p+1}$.

On sait que $a-1 < [a] \leq a$, on exploite donc ces inégalités :

On a pour tout $k \leq k'_p$,

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \left(\frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) \right) = 2$$

Or, le membre de gauche de l'inégalité précédente est un nombre entier, strictement plus petit que 2 ; il est donc inférieur ou égal à 1 :

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \leq 1$$

En sommant :

$$v_p \left(\binom{2n}{n} \right) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) = \sum_{k=1}^{k'_p} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq \sum_{k=1}^{k'_p} 1 = k'_p = \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor$$

Ainsi,

$$v_p \left(\binom{2n}{n} \right) \leq \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor.$$

c) Soit k tel que p^k divise $\binom{2n}{n}$. Montrer alors que $p^k \leq 2n$.

Puisque p^k divise $\binom{2n}{n}$, alors nécessairement $k \leq v_p \left(\binom{2n}{n} \right)$.

On exploite alors la question précédente et donc $k \leq \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor \leq \frac{\ln(2n)}{\ln p}$.

Donc $p^k \leq p^{\ln(2n)/\ln p} = e^{\ln(2n) \ln p / \ln p} = e^{\ln(2n)} = 2n$ par croissance de la suite $(p^m)_{m \in \mathbb{N}}$.

$$\text{Si } p^k \text{ divise } \binom{2n}{n}, \text{ alors que } p^k \leq 2n.$$

Partie III - Estimation du nombre de diviseurs premiers

Pour tout entier naturel non nul n , on note $\omega(n)$ le nombre d'entiers premiers distincts qui divisent n .

On a $\omega(1) = 0$, $\omega(2) = 1$, $\omega(3) = 1$, $\omega(4) = 1$, $\omega(6) = 2$, ...

6. Donner le tableau des valeurs $\omega(n)$ pour $n \in \llbracket 10, 19 \rrbracket$.

Donner sans justification les plus petits entiers n tels que $\omega(n) = 3$ et $\omega(n) = 4$.

n	10	11	12	13	14	15	16	17	18	19
$\omega(n)$	2	1	2	1	2	2	1	1	2	1

Le plus petit entier tel que $\omega(n) = 3$ est $2 \times 3 \times 5 = 30$, celui tel que $\omega(n) = 4$ est $2 \times 3 \times 5 \times 7 = 210$.

7. Montrer que $\omega : \mathbb{N}^* \rightarrow \mathbb{N}$ est surjective et que toutes les valeurs de $\mathbb{N}$ admettent une infinité d'antécédents sauf une à préciser.

Soit $m \in \mathbb{N}$ fixé quelconque.

Étudions l'équation d'inconnue $n \in \mathbb{N}^*$, $\omega(n) = m$.

— Si $m = 0$,

$$\omega(n) = 0 \iff n \text{ n'a aucun diviseur premier } \iff n = 1$$

ce qui prouve que 0 possède un unique antécédent.

— Sinon, $m \geq 1$, posons $a = \prod_{k=1}^m p_k$ (produit des m premiers nombres premiers) et observons que,

$$\forall j \in \mathbb{N}^*, \omega(a^j) = \omega \left(\prod_{k=1}^m p_k^j \right) = m$$

donc $\{a^j \mid j \in \mathbb{N}^*\} \subset \omega^{-1}(\{m\})$, ce qui prouve que m possède une infinité d'antécédents.

Ainsi, $\omega : \mathbb{N}^* \rightarrow \mathbb{N}$ est surjective et toutes les valeurs non nulles admettent une infinité d'antécédents.

8. Soit $n \in \mathbb{N}^*$. Justifier que $n \geq 2^{\omega(n)}$ (pour le cas $n \geq 2$, on pourra introduire $q_1 < q_2 < \dots < q_{\omega(n)}$ les $\omega(n)$ facteurs premiers de n et les utiliser pour exprimer n).

En déduire une majoration de $\omega(n)$ explicite en fonction de n .

Écrire ce résultat sous la forme $\omega(n) \underset{n \rightarrow +\infty}{=} O(u_n)$, où u_n est une suite simple qui s'exprime à l'aide des fonctions usuelles. Ce résultat est une estimation asymptotique de $\omega(n)$.

★ — Si $n = 1$, $\omega(1) = 0$ donc $n = 1 \geq 1 = 2^0 = 2^{\omega(1)}$.

— Sinon $n \geq 2$, donc il admet au moins un facteur premier ce qui permet d'introduire $q_1 < q_2 < \dots < q_{\omega(n)}$ les $\omega(n)$ facteurs premiers intervenant dans la décomposition de n . Notons $(\alpha_1, \dots, \alpha_{\omega(n)}) \in (\mathbb{N}^*)^{\omega(n)}$ les exposants de ces facteurs dans la décomposition de n de sorte que

$$n = \prod_{k=1}^{\omega(n)} q_k^{\alpha_k} \underset{\substack{\forall k \in \llbracket 1, \omega(n) \rrbracket, \\ \alpha_k \geq 1}}{\geq} \prod_{k=1}^{\omega(n)} q_k \underset{\substack{\forall k \in \llbracket 1, \omega(n) \rrbracket, \\ q_k \geq 2}}{\geq} \prod_{k=1}^{\omega(n)} 2 = 2^{\omega(n)}$$

★ $n \geq 2^{\omega(n)}$ donc, par croissance de la fonction $\ln$ sur $\mathbb{R}_+^*$, $\ln(n) \geq \omega(n) \ln 2$ donc

$$\omega(n) \leq \frac{\ln(n)}{\ln 2}.$$

★ Cette inégalité implique $\omega(n) \underset{n \rightarrow +\infty}{=} O(\ln(n))$ (prendre $N = 1$ et $C = \frac{1}{\ln 2} > 0$ dans la définition).

9. En déduire un encadrement du nombre de diviseurs premiers distincts d'un entier n compris entre 2 et $2^{20} = 1\,048\,576$.

Soit $n \in \llbracket 2, 2^{20} \rrbracket$ fixé.

Comme $n \geq 2$, il admet au moins un diviseur premier, donc $\omega(n) \geq 1$.

D'après la question précédente, $\omega(n) \leq \frac{\ln(n)}{\ln 2} \leq \frac{\ln 2^{20}}{\ln 2} \leq \frac{20 \ln 2}{\ln 2} = 20$.

$$\boxed{\forall n \in \llbracket 2, 2^{20} \rrbracket, 1 \leq \omega(n) \leq 20 \text{ (} n \text{ possède entre 1 et 20 facteurs premiers distincts).}$$

Remarque : si l'on utilise le fait que pour tout entier $n \geq 2$, en notant $q_1 < q_2 < \dots < q_{\omega(n)}$ les $\omega(n)$ facteurs premiers intervenant dans la décomposition de n et $(\alpha_1, \dots, \alpha_{\omega(n)}) \in (\mathbb{N}^*)^{\omega(n)}$ les exposants de ces facteurs dans la décomposition de n de sorte que

$$n = \prod_{k=1}^{\omega(n)} q_k^{\alpha_k} \underset{\substack{\forall k \in \llbracket 1, \omega(n) \rrbracket, \\ \alpha_k \geq 1}}{\geq} \prod_{k=1}^{\omega(n)} q_k \underset{\substack{\forall k \in \llbracket 1, \omega(n) \rrbracket, \\ q_k \geq p_k}}{\geq} \prod_{k=1}^{\omega(n)} p_k$$

On observe que si $\omega(n) = 7$, $\prod_{k=1}^7 p_k = 510510 < 2^{20}$ et si $\omega(n) = 8$, $\prod_{k=1}^8 p_k = 9699690 > 2^{20}$,

donc $\forall n \in \llbracket 2, 2^{20} \rrbracket, 1 \leq \omega(n) \leq 7$ (n possède entre 1 et 7 facteurs premiers distincts).

10. Amélioration de l'estimation asymptotique de $\omega(n)$.

a) Soit $n \in \mathbb{N}^*$ tel que $n \geq 2$. Soient $q_1 < q_2 < \dots < q_{\omega(n)}$ les $\omega(n)$ facteurs premiers de n . Montrer que

$$n \geq \prod_{k=1}^{\omega(n)} q_k \geq 2 \prod_{k=2}^{\omega(n)} (2k-1)$$

D'après le théorème de décomposition en facteurs premiers,

$$n = \prod_{k=1}^{\omega(n)} q_k^{\nu_{q_k}(n)}$$

où, pour tout $k \in \llbracket 1, \omega(n) \rrbracket$, $\nu_{q_k}(n) \geq 1$ est la valuation q_k -adique de n (= la multiplicité de q_k comme facteur premier de n),

donc, $\forall k \in \llbracket 1, \omega(n) \rrbracket$, $q_k^{\nu_{q_k}(n)} \geq q_k$, donc

$$n = \prod_{k=1}^{\omega(n)} q_k^{\nu_{q_k}(n)} \geq \prod_{k=1}^{\omega(n)} q_k$$

Par construction,

- q_1 est le plus petit facteur premier de n donc $q_1 \geq p_1 = 2$ (le plus petit nombre premier),
- $q_{\omega(n)} > \dots > q_3 > q_2 > q_1 \geq 2$ donc $3 \leq q_2 < q_3 < \dots < q_{\omega(n)}$ est une suite strictement croissante de nombres premiers supérieurs ou égaux à 3 donc tous impairs donc $3 \leq q_2, 5 \leq q_3, 7 \leq q_4, \dots, 2\omega(n) - 1 \leq q_{\omega(n)}$.

Montrons par récurrence que, pour tout $k \in \llbracket 2, \omega(n) \rrbracket$, $q_k \geq 2k - 1$ en considérant la propriété définie pour tout $k \in \llbracket 2, \omega(n) \rrbracket$:

$$\mathcal{P}(k) : \llcorner q_k \geq 2k - 1 \rceil$$

- ★ q_2 est un nombre premier strictement supérieur à 2 donc $q_2 \geq 3$ ce qui prouve que $\mathcal{P}(2)$ est vraie.
- ★ Soit $k \in \llbracket 2, \omega(n) - 1 \rrbracket$ fixé quelconque tel que $\mathcal{P}(k)$ est vraie.
Alors $q_{k+1} > q_k \geq 2k - 1$ (car $\mathcal{P}(k)$ est vraie) donc $q_{k+1} \geq 2k$, or $k \geq 2$ donc $q_{k+1} > q_1 \geq 2$ et $q_{k+1} \in \mathcal{P}$ donc q_{k+1} est impair donc $q_{k+1} \geq 2k + 1$ ce qui établit $\mathcal{P}(k + 1)$.

Par conséquent,

$$n \geq \prod_{k=1}^{\omega(n)} q_k = \underbrace{q_1}_{\geq 2} \prod_{k=2}^{\omega(n)} \underbrace{q_k}_{\geq 2k-1} \geq 2 \prod_{k=2}^{\omega(n)} (2k - 1)$$

$$\text{Ainsi, } n \geq \prod_{k=1}^{\omega(n)} q_k \geq 2 \prod_{k=2}^{\omega(n)} (2k - 1).$$

b) En exprimant le minorant de n obtenu dans la question précédente comme un quotient de deux factorielles, montrer que

$$\ln(n) \geq \ln((2\omega(n))!) - \ln(\omega(n)!) - (\omega(n) - 1) \ln 2$$

Observons que

$$\prod_{k=2}^{\omega(n)} (2k - 1) = \frac{\prod_{k=2}^{\omega(n)} (2k - 1) \prod_{k=2}^{\omega(n)} (2k)}{\prod_{k=2}^{\omega(n)} (2k)} = \frac{\prod_{\substack{1 \leq k \leq 2\omega(n) \\ k \equiv 1 \pmod{2}}} k \times \frac{1}{2} \prod_{\substack{1 \leq k \leq 2\omega(n) \\ k \equiv 0 \pmod{2}}} k}{2^{\omega(n)-1} \times \prod_{k=2}^{\omega(n)} k} = \frac{\frac{1}{2} (2\omega(n))!}{2^{\omega(n)-1} (\omega(n))!} = \frac{(2\omega(n))!}{2^{\omega(n)-2} (\omega(n))!}$$

donc en reprenant la minoration de n établie dans la question précédente,

$$n \geq 2 \prod_{k=2}^{\omega(n)} (2k - 1) = \frac{(2\omega(n))!}{2^{\omega(n)-1} (\omega(n))!}$$

si bien qu'en prenant le logarithme (fonction croissante donc préservation du sens de l'inégalité),

$$\ln(n) \geq \ln((2\omega(n))!) - \ln(\omega(n)!) - (\omega(n) - 1) \ln 2$$

c) En utilisant les estimations de la question 1, montrer que

$$\ln(n) \geq \varphi_{\lambda, \mu}(\omega(n))$$

pour des valeurs de λ et μ que l'on précisera.

★ Appliquons la minoration de la question 1 pour $n \leftarrow 2\omega(n)$ (autorisé car $\omega(n) \geq 1$ puisque $n \geq 2$) :

$$\ln((2\omega(n))!) \geq 2\omega(n) \ln(2\omega(n)) - 2\omega(n) + 1$$

★ Appliquons la majoration de la question 1 pour $n \leftarrow \omega(n)$ (autorisé car $\omega(n) \geq 1$ puisque $n \geq 2$) :

$$\ln(\omega(n)!) \leq \omega(n) \ln(\omega(n))$$

donc

$$-\ln(\omega(n)!) \geq -\omega(n) \ln(\omega(n))$$

★ Injectons ces estimations dans la minoration établie dans la question précédente :

$$\begin{aligned} \ln(n) &\geq \ln((2\omega(n))!) - \ln(\omega(n)!) - (\omega(n) - 1) \ln 2 \\ &\geq \underbrace{2\omega(n) \ln(2\omega(n))}_{= 2\omega(n) \ln(\omega(n)) + 2\omega(n) \ln 2} - 2\omega(n) + 1 - \omega(n) \ln(\omega(n)) - (\omega(n) - 1) \ln 2 \\ &\geq \underbrace{\omega(n) \ln(\omega(n)) - (2 - \ln 2)\omega(n) + 1 + \ln 2}_{= \varphi_{2 - \ln 2, 1 + \ln 2}(\omega(n))} \end{aligned}$$

Ainsi, $\ln(n) \geq \varphi_{\lambda, \mu}(\omega(n))$ pour $\lambda = 2 - \ln 2$ et $\mu = 1 + \ln 2$.

d) En déduire que $\omega(n) \underset{n \rightarrow +\infty}{=} O\left(\frac{\ln(n)}{\ln(\ln(n))}\right)$.

Posons $N = \lfloor 2e \rfloor + 1$.

★ Soit $n \in \mathbb{N}$ fixé quelconque tel que $n \geq N$.

Les valeurs $2 - \ln 2$ et $1 + \ln 2$ sont strictement positives donc les résultats de la partie 1 s'appliquent à la fonction $\varphi_{2 - \ln 2, 1 + \ln 2}$.

Pour $\mu = 1 + \ln 2$, $e^\mu = 2e < N \leq n$, en utilisant les notations de la question 2,

$$\begin{aligned} \ln(n) &\geq \varphi_{\lambda, \mu}(\omega(n)) \\ \varphi_{\lambda, \mu}(x_n) &\geq \varphi_{\lambda, \mu}(\omega(n)). \end{aligned}$$

D'après le tableau de variations de $\varphi_{\lambda, \mu}$, comme $\ln(n) \geq \mu$, alors $0 \leq \omega(n) \leq x_n$.

Ainsi, la suite $\left(\frac{\omega(n)}{x_n}\right)$ est bornée, soit

$$\omega(n) \underset{n \rightarrow +\infty}{=} O(x_n).$$

★ Par ailleurs, d'après la question 4 que $x_n \underset{n \rightarrow +\infty}{\sim} \frac{\ln(n)}{\ln(\ln(n))}$.

Donc, d'après la question 1, $\omega(n) \underset{n \rightarrow +\infty}{=} O\left(\frac{\ln(n)}{\ln(\ln(n))}\right)$.

Ainsi,

$$\omega(n) \underset{n \rightarrow +\infty}{=} O\left(\frac{\ln(n)}{\ln(\ln(n))}\right).$$

Partie IV - Majoration du PPCM des n premiers entiers

11. Soit $r \in \mathbb{N}^*$. Soient $a_1, a_2, \dots, a_r$ des entiers naturels non nuls.

a) Justifier qu'il existe un unique entier naturel $d \in \mathbb{N}^*$ tel que

$$a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_r\mathbb{Z} = d\mathbb{Z}$$

On pourra étudier la nature de la structure algébrique $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_r\mathbb{Z}$.

Notons $I_r = a_1\mathbb{Z} \cap \dots \cap a_r\mathbb{Z}$.

Pour tout $i \in \mathbb{N}_r$, $a_i\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Puis par stabilité par intersection : I_r est un idéal de $\mathbb{Z}$.

Or $\mathbb{Z}$ est un anneau euclidien donc principal. Il existe donc $d \in \mathbb{Z}$ tel que $I_r = d\mathbb{Z}$.

Nécessairement $d \neq 0$, sinon, $I_r = \{0\}$, alors que $\delta := \prod_{i=1}^r a_i \in I_r$ (multiple de tous les a_i) donc $I_r \neq \{0\}$.

Comme $(-d)\mathbb{Z} = d\mathbb{Z}$, on peut supposer que $d > 0$ donc $d \in \mathbb{N}^*$.

Enfin, s'il existe $c \in \mathbb{N}^*$ tel que $I_r = c\mathbb{Z} = d\mathbb{Z}$, alors $d|c$ et $c|d$ donc c et d sont associés.

Ainsi $|c| = |d|$. Or $|c| = c$ et $|d| = d$, donc $c = d$. Et d est unique.

Il existe un unique entier naturel $d \in \mathbb{N}^*$ tel que $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_r\mathbb{Z} = d\mathbb{Z}$.

b) Montrer que le nombre μ est le plus petit entier naturel non nul qui est divisible par tous les entiers $a_1, a_2, \dots, a_r$.

Le nombre μ s'appelle le plus petit commun multiple de $a_1, a_2, \dots, a_r$, on le note $\text{PPCM}(a_1, a_2, \dots, a_r)$.

Comme $\mu \in I_r$, alors μ est un entier divisible par chacun des a_i .

Soit m un entier divisible par chacun des $a_1, \dots, a_r$. Alors, pour tout $i \in \{1, \dots, r\}$, $m \in a_i\mathbb{Z}$. Donc, $m \in I_r$ et, d'après la question précédente, $m \in \mu\mathbb{Z}$. Ainsi, $\mu|m$. Alors, $\mu \leq m$.

Remarque. On a même montré que μ est le plus petit commun multiple à $a_1, \dots, a_r$ pour la relation divise.

12. Soit n un entier naturel non nul. On note $M_n = \text{PPCM}(1, 2, \dots, n)$. On rappelle que, pour tout entier p premier, en utilisant les définitions de la Partie II, $k_p = \max \left\{ k \in \mathbb{N} \mid p^k \leq n \right\}$.

a) Calculer M_2 , M_3 et M_4 .

— D'après la définition, $\mathbb{Z} \cap 2\mathbb{Z} = 2\mathbb{Z}$, donc $M_2 = 2$.

— Le plus petit entier multiple de 2 et 3 est 6. Ainsi, $M_3 = 6$.

— Le plus petit entier multiple de 2, 3 et 4 est 12. Ainsi, $M_4 = 12$.

b) Montrer que

$$M_n \leq n! \tag{1}$$

L'entier $n!$ est un multiple de chacun des entiers $1, 2, \dots, n$. Comme M_n est le plus petit de ces multiples, alors

$$M_n \leq n! \quad (\text{Mieux : } M_n | n!)$$

Cette majoration est relativement grossière et les questions suivantes permettront de l'améliorer.

c) Montrer que $M_n = \prod_{\substack{p \leq n \\ p \in \mathcal{P}}} p^{k_p}$.

Comme p^{k_p} est inférieur à n , alors $p^{k_p} \in \{1, 2, \dots, n\}$ et donc $p^{k_p} | M_n$.

Or, lorsque $p \neq q$ est premier, alors $p^{k_p} \wedge q^{k_q} = 1$. Ainsi (corollaire du lemme de Gauss),

$$\prod_{\substack{p \leq n \\ p \in \mathcal{P}}} p^{k_p} | M_n.$$

Réciproquement, soit $m \in \{2, \dots, n\}$. Notons $m = \prod_{p \in \mathcal{P}} p^{v_p(m)}$ sa décomposition en facteurs premiers.

Comme $p^{v_p(m)} \leq m \leq n$, alors $v_p(m) \leq k_p$. Ainsi, $p^{v_p(m)} | p^{k_p}$. Alors,

$$m = \prod_{p \in \mathcal{P}} p^{v_p(m)} | \prod_{\substack{p \leq n \\ p \in \mathcal{P}}} p^{k_p}.$$

Ainsi, $\prod_{\substack{p \leq n \\ p \in \mathcal{P}}} p^{k_p}$ est un multiple commun à tous les entiers $1, \dots, n$. Comme il est inférieur à M_n et que M_n est le plus petit, alors

$$M_n = \prod_{\substack{p \leq n \\ p \in \mathcal{P}}} p^{k_p}.$$

On note $\pi(n)$ le cardinal de l'ensemble $\mathcal{P}_n$ des nombres premiers inférieurs ou égaux à n .

d) En déduire que

$$M_n \leq n^{\pi(n)} \quad (2)$$

D'après la définition de k_p , $p^{k_p} \leq n$. Ainsi,

$$M_n \leq \prod_{\substack{p \leq n \\ p \in \mathcal{P}}} n = n^{\pi(n)}$$

Partie V - Encadrement de la fonction π

Dans toute la suite, n désigne un entier naturel non nul. On rappelle que $\pi(n)$ est le cardinal de l'ensemble $\mathcal{P}_n$ des nombres premiers inférieurs ou égaux à n .

13. L'objectif de cette question est de majorer $\prod_{\substack{p \in \mathcal{P} \\ p \leq n}} p$ en fonction de n .

a) Soient a et b deux entiers tels que $0 < \frac{b}{2} \leq a < b$. Montrer que le produit $\prod_{\substack{p \in \mathcal{P} \\ a < p \leq b}} p$ divise l'entier $\binom{b}{a}$.

$$\binom{b}{a} = \frac{b!}{a!(b-a)!} = \frac{b(b-1) \dots (b-a+1)}{a!} \text{ donc } a! \binom{b}{a} = \prod_{k=b-a+1}^b k.$$

Notons $a < q_1 < q_2 < \dots < q_N \leq b$ les $N \in \mathbb{N}$ nombres premiers situés dans l'intervalle $]a, b] = [a+1, b]$.

— Si $N = 0$, alors $\prod_{\substack{p \in \mathcal{P} \\ a < p \leq b}} p = 1$ donc $\prod_{\substack{p \in \mathcal{P} \\ a < p \leq b}} p \mid \binom{b}{a}$.

— Si $N \geq 1$, alors pour tout $i \in \llbracket 1, N \rrbracket$, q_i est un nombre premier de l'intervalle $\llbracket a+1, b \rrbracket$, or $\frac{b}{2} \leq a$ donc $b \leq 2a$ donc $b - a + 1 \leq a + 1$ donc $\llbracket a+1, b \rrbracket \subset \llbracket b-a+1, b \rrbracket$ si bien que q_i est un facteur du produit $\prod_{k=b-a+1}^b k$ donc

$$\prod_{k=b-a+1}^b k = q_i \underbrace{\prod_{\substack{k=b-a+1 \\ k \neq q_i}}^b k}_{\text{entier noté } A_i} = q_i A_i$$

donc

$$q_i A_i = a! \binom{b}{a} \quad \text{donc} \quad q_i \mid a! \binom{b}{a}$$

or $q_i > a$ donc q_i ne divise aucun des entiers de l'intervalle $\llbracket 1, a \rrbracket$ donc $\forall k \in \llbracket 1, a \rrbracket$, $q_i \wedge k = 1$ (un nombre premier est premier avec tout entier qu'il ne divise pas) donc $q_i \wedge a! = 1$ (tout entier premier avec une famille d'entiers est premier avec leur produit) si bien que le théorème de Gauss permet d'affirmer que $q_i \mid \binom{b}{a}$.

Nous venons d'établir que $\forall i \in \llbracket 1, N \rrbracket$, $q_i \mid \binom{b}{a}$, or $q_1, \dots, q_N$ sont deux à deux premiers entre eux (car ce sont des nombres premiers deux à deux distincts) donc $\prod_{i=1}^N q_i \mid \binom{b}{a}$ (Corollaire - Lemme de Gauss).

Ainsi, $\prod_{\substack{p \in \mathcal{P} \\ a < p \leq b}} p \mid \binom{b}{a}$.

b) En déduire que pour tout $m \geq 1$, $\prod_{\substack{p \in \mathcal{P} \\ m+1 < p \leq 2m+1}} p$ divise $\binom{2m+1}{m+1}$.

Soit $m \geq 1$.

Appliquons le résultat de la question précédente pour $a \leftarrow m+1$ et $b \leftarrow 2m+1$ ce qui est autorisé car

$$0 < \frac{3}{2} \leq \underbrace{\frac{2m+1}{2}}_{\substack{b \\ \frac{b}{2}}} = m + \frac{1}{2} \leq \underbrace{m+1}_a \overset{m \geq 1}{<} \underbrace{2m+1}_b$$

pour obtenir $\prod_{\substack{p \in \mathcal{P} \\ m+1 < p \leq 2m+1}} p$ divise $\binom{2m+1}{m+1}$.

c) Comparer, pour $m \geq 1$, les entiers $\binom{2m+1}{m}$ et $\binom{2m+1}{m+1}$ puis en développant $(1+1)^{2m+1}$, montrer que $\binom{2m+1}{m} \leq 4^m$.

★ Par symétrie des coefficients binomiaux

$$\boxed{\binom{2m+1}{m} = \binom{2m+1}{(2m+1)-m} = \binom{2m+1}{m+1}.}$$

★ D'une part, $(1+1)^{2m+1} = 2^{2m+1} = 2 \times 4^n$. D'autre part, en développant cette somme avec la formule du binôme de Newton, on obtient une somme de termes positifs qui est donc minorée par deux d'entre eux « bien choisis » :

$$\begin{aligned} 2 \times 4^n &= (1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k} 1^k 1^{2m+1-k} = \binom{2m+1}{m} + \binom{2m+1}{m+1} + \underbrace{\sum_{k \notin \{m, m+1\}} \binom{2m+1}{k}}_{\geq 0} \\ &\geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2 \binom{2m+1}{m}. \end{aligned}$$

$$\boxed{\text{Ainsi } \binom{2m+1}{m} \leq 4^m.}$$

d) Montrer que, pour tout $m \geq 1$, $\prod_{\substack{p \in \mathcal{P} \\ m+1 < p \leq 2m+1}} p \leq 4^m$.

Soit $m \geq 1$ fixé quelconque.

D'après la question 2, $\prod_{\substack{p \in \mathcal{P} \\ m+1 < p \leq 2m+1}} p$ divise $\binom{2m+1}{m+1} = \binom{2m+1}{m}$.

Or, $\binom{2m+1}{m} \neq 0$,

donc $\prod_{\substack{p \in \mathcal{P} \\ m+1 < p \leq 2m+1}} p \leq \binom{2m+1}{m}$ si bien que la majoration de la question 3 donne par transitivité

$$\boxed{\forall m \geq 1, \prod_{\substack{p \in \mathcal{P} \\ m+1 < p \leq 2m+1}} p \leq 4^m.}$$

e) Montrer que $\prod_{\substack{p \in \mathcal{P} \\ p \leq n}} p \leq 4^n$.

On pourra prouver par récurrence la propriété $\mathcal{Q}(\cdot)$ définie pour tout $n \in \mathbb{N}^*$ par

$$\mathcal{Q}(n) : \ll \forall k \in \llbracket 1, 2n \rrbracket, \prod_{\substack{p \in \mathcal{P} \\ p \leq k}} p \leq 4^k \gg$$

Considérons la propriété $\mathcal{Q}(\cdot)$ de l'énoncé.

- D'après la convention concernant un produit indexé par un ensemble vide, $\prod_{\substack{p \in \mathcal{P} \\ p \leq 1}} p = 1 \leq 4 = 4^1$. De

plus, $\prod_{\substack{p \in \mathcal{P} \\ p \leq 2}} p = 2 \leq 16 = 4^2$ donc $\mathcal{Q}(1)$ est vraie.

- Soit $n \in \mathbb{N}^*$ fixé quelconque tel que $\mathcal{Q}(n)$ est vraie.
Soit $k \in \llbracket 1, 2n+2 \rrbracket$ fixé quelconque.

★ Si $k \in \llbracket 1, 2n \rrbracket$, la véracité de $\mathcal{Q}(n)$ donne $\prod_{\substack{p \in \mathcal{P} \\ p \leq k}} p \leq 4^k$.

★ Sinon, $k = 2n + 1$ ou $k = 2n + 2$.

D'une part ($k = 2n + 1$),

$$\prod_{\substack{p \in \mathcal{P} \\ p \leq 2n+1}} p = \underbrace{\prod_{\substack{p \in \mathcal{P} \\ p \leq n+1}} p}_{\leq 4^{n+1} \text{ car } \mathcal{Q}(n) \text{ vraie appliquée pour } k \leftarrow n+1 \in \llbracket 1, 2n \rrbracket}} \times \underbrace{\prod_{\substack{p \in \mathcal{P} \\ n+1 < p \leq 2n+1}} p}_{\leq 4^n \text{ quest. 4 pour } m \leftarrow n, n \geq 1}} \leq 4^{n+1} \times 4^n = 4^{2n+1}$$

(3)

D'autre part ($k = 2n + 2$),

$$\prod_{\substack{p \in \mathcal{P} \\ p \leq 2n+2}} p = \underbrace{\prod_{\substack{p \in \mathcal{P} \\ p \leq 2n+1}} p}_{\text{car } 2n+2 = 2(n+1) \notin \mathcal{P} (n \geq 1)} \leq 4^{2n+1} \leq 4^{2n+2} \quad \text{inégalité (3)}$$

Ainsi, $\mathcal{Q}(n+1)$ est vraie.

Ainsi, pour tout $n \in \mathbb{N}^*$, $\prod_{\substack{p \in \mathcal{P} \\ p \leq n}} p \leq 4^n$.

14. Justifier que $\prod_{\substack{p \leq n \\ p \text{ premier}}} p \geq \prod_{\substack{\sqrt{n} < p \leq n \\ p \text{ premier}}} p$.

D'après la définition, $]\sqrt{n}, n] \subset [1, n]$ donc $\{p \in \mathcal{P} | \sqrt{n} < p \leq n\} \subset \{p \in \mathcal{P} | p \leq n\}$.

Comme tous les nombres premiers sont plus grands que 1 et que $\{p \in \mathcal{P} | p \leq n\}$ est la réunion disjointe de $\{p \in \mathcal{P} | \sqrt{n} < p \leq n\}$ et $\{p \in \mathcal{P} | p \leq \sqrt{n}\}$,

$$\prod_{\substack{p \leq n \\ p \text{ premier}}} p = \underbrace{\prod_{\substack{p \leq \sqrt{n} \\ p \text{ premier}}} p}_{\geq 1} \times \underbrace{\prod_{\substack{\sqrt{n} < p \leq n \\ p \text{ premier}}} p}_{\geq 0} \geq \prod_{\substack{\sqrt{n} < p \leq n \\ p \text{ premier}}} p.$$

Ainsi, $\prod_{\substack{p \leq n \\ p \text{ premier}}} p \geq \prod_{\substack{\sqrt{n} < p \leq n \\ p \text{ premier}}} p$.

15. Dédurre des questions 13 et 14 que,

$$n^{(\pi(n) - \pi(\sqrt{n}))/2} \leq 4^n.$$

En reprenant l'inégalité établie dans la question précédente et en minorant les facteurs du membre de droite de l'inégalité par $\sqrt{n}$, on obtient

$$\prod_{\substack{p \leq n \\ p \text{ premier}}} p \geq \prod_{\substack{\sqrt{n} < p \leq n \\ p \text{ premier}}} \underbrace{p}_{\geq \sqrt{n}} \geq \sqrt{n}^{|\{p \in \mathcal{P} | \pi(n) < p \leq n\}|} = \sqrt{n}^{\pi(n) - \pi(\sqrt{n})} = n^{\frac{\pi(n) - \pi(\sqrt{n})}{2}}$$

car la réunion $\{p \in \mathcal{P} | p \leq n\} = \{p \in \mathcal{P} | \sqrt{n} < p \leq n\} \cup \{p \in \mathcal{P} | p \leq \sqrt{n}\}$ étant disjointe,

$$\pi(n) = |\{p \in \mathcal{P} | p \leq n\}| = |\{p \in \mathcal{P} | \sqrt{n} < p \leq n\}| + \pi(\sqrt{n}) \quad \text{donc} \quad |\{p \in \mathcal{P} | p \leq n\}| = \pi(n) - \pi(\sqrt{n})$$

D'après la question 13, $\prod_{\substack{p \leq n \\ p \text{ premier}}} p \leq 4^n$,

$$\text{donc } \boxed{n^{(\pi(n)-\pi(\sqrt{n}))/2} \leq 4^n.}$$

16. On suppose que $n \geq 2$ et on admet que $\ln(2) \leq \frac{3}{4}$. Justifier que $\pi(\sqrt{n}) \leq \sqrt{n} \leq \frac{n}{\ln(n)}$, puis établir que

$$\pi(n) \leq 4 \frac{n}{\ln(n)}.$$

★ $\{p \in \mathcal{P} | p \leq \sqrt{n}\} = \mathcal{P} \cap [1, \sqrt{n}] \subset \mathcal{P} \cap \llbracket 1, \lfloor \sqrt{n} \rfloor \rrbracket \underset{\mathcal{P} \subset \mathbb{N}^*}{\subset} \mathbb{N}^* \cap [1, \sqrt{n}] \subset \llbracket 1, \lfloor \sqrt{n} \rfloor \rrbracket$ donc

$$|\{p \in \mathcal{P} | p \leq \sqrt{n}\}| \leq |\llbracket 1, \lfloor \sqrt{n} \rfloor \rrbracket| = \lfloor \sqrt{n} \rfloor$$

or, pour tout $x \in \mathbb{R}$, $\lfloor \sqrt{x} \rfloor \leq x$, et par croissance de π :

$$\boxed{\pi(\sqrt{n}) \leq \sqrt{n}}.$$

★ Montrons que $\forall x \in [2, +\infty[$, $\sqrt{x} \leq \frac{x}{\ln x}$.
Pour cela observons que, pour tout $x \geq 2$,

$$\sqrt{x} \leq \frac{x}{\ln(x)} \iff \ln(x) \leq \sqrt{x} \iff \sqrt{x} - \ln x \geq 0$$

ce qui nous incite à considérer la fonction $f : x \mapsto \sqrt{x} - \ln x$ sur $[2, +\infty[$.
 f est dérivable sur $[2, +\infty[$ et

$$\forall x \in [2, +\infty[, f'(x) = \frac{1}{2\sqrt{x}} - \frac{1}{x} = \frac{\sqrt{x} - 2}{2x} = \frac{x - 4}{2x(\sqrt{x} + 2)}$$

d'où le tableau des variations de f

x	2	4	∞
$f'(x)$	-	0	+
f	$\searrow$ $2 - \ln 4$ $\nearrow$		

or l'énoncé nous permet de minorer $f(4)$:

$$f(4) = 2 - \ln 4 = 2 - 2 \ln 2 \geq 2 - 2 \times \frac{3}{4} = \frac{1}{2} > 0$$

si bien que

$$\forall x \in [2, +\infty[, \sqrt{x} - \ln x = f(x) \geq 0$$

et cette inégalité est équivalente à l'inégalité annoncée, qui particularisée pour un entier $n \geq 2$, donne

$$\boxed{\sqrt{n} \leq \frac{n}{\ln(n)}}.$$

★ Prenons le logarithme sur l'inégalité établie dans la question précédente :

$$\frac{\pi(n) - \pi(\sqrt{n})}{2} \ln(n) \leq n \ln(4)$$

donc, puisque $n \geq 2$, $\ln(n) > 0$ ce qui permet de multiplier par $\frac{2}{\ln(n)} > 0$ tout en préservant le sens de l'inégalité

$$\pi(n) - \pi(\sqrt{n}) \leq \frac{2n \ln(4)}{\ln n} \quad \text{donc} \quad \pi(n) \leq \pi(\sqrt{n}) + 4 \ln(2) \frac{n}{\ln n}.$$

La majoration de $\pi(\sqrt{n})$ établie dans les points précédents permet d'en déduire que

$$\pi(n) \leq (1 + 4 \ln(2)) \frac{n}{\ln n}.$$

Enfin,

$$1 + 4 \ln(2) \leq 4 \iff \ln(2) \leq \frac{3}{4} \text{ ce qui est une inégalité vraie,}$$

$$\text{donc } \pi(n) \leq 4 \frac{n}{\ln(n)}.$$

17. À l'aide des inégalités établies dans les question 1 et 16, déterminer la limite de $\left(\frac{n^{\pi(n)}}{n!}\right)$. Des deux majorations (1) et (2) de M_n obtenues dans la partie précédente, laquelle est asymptotiquement la meilleure ?

Observons que $\frac{n^{\pi(n)}}{n!} = \exp(\pi(n) \ln(n) - \ln(n!))$ ce qui permet de se ramener à la recherche de la limite de la suite $(\pi(n) \ln(n) - \ln(n!))$.

D'après la question 16, puisque $\ln(n) \geq 0$,

$$\pi(n) \ln(n) \leq 4 \frac{n}{\ln n} \times \ln(n) = 4n$$

et d'après la question 1,

$$-\ln(n!) \leq -n \ln(n) + n - 1 \leq -n \ln n + n$$

donc, pour tout $n \geq 2$ (on exclut le cas $n = 1$ pour justifier la factorisation par $\ln(n)$)

$$\pi(n) \ln(n) - \ln(n!) \leq 4n - n \ln(n) + n \leq \underbrace{\overbrace{-n \ln(n)}_{\xrightarrow{n \rightarrow +\infty} -\infty}}_{\xrightarrow{n \rightarrow +\infty} -\infty} \underbrace{\left(1 - \frac{5}{\ln n}\right)}_{\xrightarrow{n \rightarrow +\infty} 1}$$

donc, par théorème de divergence vers $-\infty$ par majoration, $\lim_{n \rightarrow +\infty} \pi(n) \ln(n) - \ln(n!) = -\infty$,

donc, par composition des limites,

$$\lim_{n \rightarrow +\infty} \frac{n^{\pi(n)}}{n!} = \lim_{x \rightarrow -\infty} e^x = 0 \text{ donc } \frac{n^{\pi(n)}}{n!} = o(n!).$$

Asymptotiquement, la meilleure des deux majorations de M_n est la majoration (2) : $M_n \leq n^{\pi(n)}$.

On termine ce sujet en montrant que la majoration obtenue pour $\pi(n)$ est le bon ordre de grandeur.

18. Montrer que

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

On pourra procéder par récurrence pour la minoration, et utiliser la question 3 pour la majoration.

- Considérons la propriété $\mathcal{P}(\cdot)$ définie pour tout $n \in \mathbb{N}^*$

$$\mathcal{P}(n) : \ll \frac{4^n}{2n} \leq \binom{2n}{n} \gg.$$

$$\star \frac{4^1}{2 \times 1} = 2 \text{ et } \binom{2 \times 1}{1} = 2 \text{ donc } \frac{4^1}{2 \times 1} \leq \binom{2 \times 1}{1} \text{ donc } \mathcal{P}(1) \text{ est vraie.}$$

★ Soit $n \in \mathbb{N}^*$ fixé quelconque tel que $\mathcal{P}(n)$ est vraie.

$$\begin{aligned}
 \binom{2(n+1)}{n+1} &= \frac{(2n+2)!}{(n+1)!^2} = \frac{(2n+2)(2n+1)}{(n+1)^2} \frac{(2n)!}{n!^2} = \frac{2(2n+1)}{n+1} \binom{2n}{n} \\
 &\geq \frac{2(2n+1)}{n+1} \times \frac{4^n}{2n} \quad \text{car } \mathcal{P}(n) \text{ est vraie} \\
 &\geq \frac{(2n+1)}{2n} \times \frac{4^{n+1}}{2(n+1)} \\
 &\geq \frac{4^{n+1}}{2(n+1)} \quad \text{car } \frac{(2n+1)}{2n} = 1 + \frac{1}{2n} \geq 1.
 \end{aligned}$$

donc $\mathcal{P}(n+1)$ est vraie.

- Le résultat établi dans la question 3, appliqué pour $k \leftarrow 1$, implique que tout diviseur premier de $\binom{2n}{n}$ est inférieur ou égal à $2n$.

Par conséquent, la décomposition en facteurs premiers de $\binom{2n}{n}$ s'écrit

$$\binom{2n}{n} = \prod_{\substack{p \in \mathcal{P} \\ p \leq 2n}} p^{\nu_p(\binom{2n}{n})}$$

De plus, le résultat établi dans la question 3, appliqué pour un nombre premier q quelconque et $k \leftarrow \nu_q\left(\binom{2n}{n}\right)$, implique $q^{\nu_p(\binom{2n}{n})} \leq 2n$ si bien que

$$\binom{2n}{n} = \prod_{\substack{p \in \mathcal{P} \\ p \leq 2n}} \underbrace{p^{\nu_p(\binom{2n}{n})}}_{\leq 2n} \leq (2n)^{|\{p \in \mathcal{P} | p \leq 2n\}|} = (2n)^{\pi(2n)}$$

Ainsi, $\frac{4^n}{2n} \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}.$

19. Vérifier que

$$\frac{2n \ln(2)}{\ln(2n)} - 1 \geq \frac{n \ln(2)}{\ln(2n)},$$

puis en déduire que

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

•

$$\begin{aligned}
 \frac{2n \ln(2)}{\ln(2n)} - 1 \geq \frac{n \ln(2)}{\ln(2n)} &\iff 2n \ln(2) - \ln(2n) \geq n \ln(2) && \text{car } \ln(2n) \geq 0 \\
 &\iff n \ln(2) - \ln(2n) \geq 0 && \iff \ln(2^n) \geq \ln(2n) \\
 &\iff 2^n \geq 2n && \iff 2^{n-1} \geq n
 \end{aligned}$$

Montrons la propriété $\mathcal{P}(\cdot)$ définie pour tout $n \in \mathbb{N}^*$

$$\mathcal{P}(n) : \ll 2^{n-1} \geq n \gg.$$

★ $2^{1-1} = 2^0 = 1 \geq 1$ donc $\mathcal{P}(1)$ est vraie.

★ Soit $n \in \mathbb{N}^*$ fixé quelconque tel que $\mathcal{P}(n)$ est vraie.

Alors $2^{(n+1)-1} = 2 \times 2^{n-1} \geq 2 \times 2n = 4n$, or

$\mathcal{P}(n)$ est vraie

$$4n \geq 2(n+1) \iff 4n \geq 2n+2 \iff 2n \geq 2 \iff n \geq 1 \quad \text{ce qui est vrai donc } 4n \geq 2(n+1)$$

si bien que $2^{(n+1)-1} \geq 2(n+1)$ ce qui établit $\mathcal{P}(n+1)$.

Ainsi, $2^{n-1} \geq n$ donc les équivalences du début de la réponse à la question permettent de conclure que

$$\frac{2n \ln(2)}{\ln(2n)} - 1 \geq \frac{n \ln(2)}{\ln(2n)}.$$

• Prenons le logarithme sur l'encadrement établi dans la question précédente

$$\begin{aligned} \underbrace{\ln \frac{4^n}{2n}} &\leq \ln \left(\binom{2n}{n} \right) \leq \pi(2n) \ln(2n) \\ &= n \ln(4) - \ln(2n) \end{aligned}$$

donc, après multiplication par $\frac{1}{\ln(2n)} > 0$, $\frac{n \ln(4)}{\ln(2n)} - 1 \leq \pi(2n)$, si bien qu'en utilisant l'inégalité prouvée dans la première partie de la réponse,

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

20. En déduire, en distinguant selon la parité de n , que

$$\pi(n) \geq \frac{\ln(2)}{3} \frac{n}{\ln(n)}.$$

Soit $n \in \mathbb{N}$ tel que $n \geq 2$.

★ Si $n \equiv 0[2]$, il existe $k \in \mathbb{N}^*$ tel que $n = 2k$ ce qui permet d'appliquer la minoration de la question précédente :

$$\pi(n) = \pi(2k) \geq k \frac{\ln(2)}{\ln(2k)} \geq \frac{\ln(2)}{2} \times \frac{2k}{\ln(2k)} = \frac{\ln(2)}{2} \times \frac{n}{\ln(n)} \geq \frac{\ln(2)}{3} \times \frac{n}{\ln(n)}$$

★ Si $n \equiv 1[2]$, il existe $k \in \mathbb{N}^*$ (car $n \geq 2$) tel que $n = 2k+1$ ce qui permet d'appliquer la minoration de la question précédente après avoir utilisé la croissance de la suite $(\pi(n))$:

$$\pi(n) = \pi(2k+1) \geq \pi(2k) \geq k \frac{\ln(2)}{\ln(2k)} \geq \frac{k}{2k+1} \ln(2) \times \frac{2k+1}{\ln(2k)}$$

et en utilisant que $\ln(2k+1) \geq \ln(2k)$,

$$\pi(n) \geq \frac{k}{2k+1} \ln(2) \times \frac{2k+1}{\ln(2k+1)} = \frac{k}{2k+1} \ln(2) \times \frac{n}{\ln(n)}$$

De plus

$$\frac{k}{2k+1} \geq \frac{1}{3} \iff 3k \geq 2k+1 \iff k \geq 1 \quad \text{ce qui est vrai}$$

donc

$$\pi(n) \geq \frac{\ln(2)}{3} \times \frac{n}{\ln(n)}$$

En

$$\text{Ainsi, pour tout } n \geq 2, \pi(n) \geq \frac{\ln(2)}{3} \frac{n}{\ln(n)}.$$

Ces inégalités ont été asymptotiquement améliorées en 1896. Ce résultat, appelé théorème des nombres premiers, indique

$$\pi(n) \underset{x \rightarrow +\infty}{\sim} \frac{n}{\ln(n)}.$$