Le postulat de Bertrand

Notations

– On note $\mathbb{P}$ l'ensemble des nombres premiers.
Pour tout n de $\mathbb{N}$, on note $\mathbb{P}_n = \mathbb{P} \cap [2, n]$ et $\pi(n) = \text{card}(\mathbb{P}_n)$.
$\pi(n)$ désigne donc le nombre d'entiers premiers inférieurs ou égaux à n.

– Pour tout entier $n \geqslant 2$, et tout p de $\mathbb{P}$, on note $v_p(n) = \max\{k \in \mathbb{N},\ p^k \mid n\}$.
$v_p(n)$ est donc l'exposant de p dans la décomposition de n en produit de facteurs premiers.
On dit que $v_p(n)$ est la *valuation* de n suivant p.
L'égalité $v_p(n) = k$ caractérise donc les entiers n divisibles par p^k mais pas par p^{k+1}.

– Pour tout $n \geqslant 2$, on note $E_n = \{1, 2, 3, \ldots, n\}$ et $n\mathbb{N} = \{kn,\ k \in \mathbb{N}\}$.

– On note $[x]$ la partie entière de tout réel x.

L'objet de ce problème est de montrer le "postulat de Bertrand" :

Pour tout entier $n \geqslant 2$, il existe au moins un entier premier p tel que $n < p < 2n$.

Dans la suite du problème, n est un entier fixé quelconque, supérieur ou égal à 2.

Première partie

Dans cette partie et dans la suivante, p désigne un entier premier fixé quelconque.
On note m l'entier k maximum tel que $p^k \leqslant n$.

1. Donner une expression de m sous la forme d'une partie entière.
2. Pour $1 \leqslant k \leqslant m$, calculer $\text{card}(E_n \cap p^k\mathbb{N})$ et $\text{card}\{j \in E_n,\ v_p(j) = k\}$.
3. Justifier l'égalité $v_p(n!) = \sum\limits_{j=2}^{n} v_p(j)$.
4. En déduire finalement l'égalité $v_p(n!) = \sum\limits_{k=1}^{m} \left[\dfrac{n}{p^k}\right]$.

Deuxième partie

Dans cette partie, on étudie les valeurs possibles de la quantité $u_p(n) = v_p\left(\dbinom{2n}{n}\right)$.

1. Montrer que $u_p(n) = \sum\limits_{k=1}^{m'} \left(\left[\dfrac{2n}{p^k}\right] - 2\left[\dfrac{n}{p^k}\right]\right)$, avec $m' = \left[\dfrac{\ln(2n)}{\ln p}\right]$.
2. Vérifier les propriétés suivantes :
   (a) $p^{u_p(n)} \leq 2n$.
   (b) Si $\sqrt{2n} < p$, alors $u_p(n) \in \{0, 1\}$.
   (c) Si $n \geqslant 3$ et $\frac{2}{3}n < p \leq n$, alors $u_p(n) = 0$.
   (d) Si $n < p < 2n$, alors $u_p(n) = 1$.

Troisième partie

Cette partie est consacrée à la démonstration de résultats utiles dans la partie IV.

Pour tout réel $x \geqslant 2$, on note Π_x le produit des entiers premiers $p \leqslant x$.

1. Montrer que si $0 \leqslant k \leqslant 2n$ alors $\binom{2n}{k} \leq \binom{2n}{n}$. En déduire $\binom{2n}{n} \geqslant \dfrac{4^n}{2n}$.
2. (a) Pour tout $m \geqslant 1$, montrer que $\Pi_{2m+1} \leqslant \binom{2m+1}{m}\Pi_{m+1} \leqslant 4^m \Pi_{m+1}$.
   Indication : montrer que tout p de $\mathbb{P}$ tel que $m+1 < p \leqslant 2m+1$ divise $\binom{2m+1}{m}$.
   (b) En déduire que pour tout réel $x \geqslant 2$, on a $\Pi_x \leq 4^x$ (inégalité de Tchebyshev).
3. Montrer que tous les diviseurs premiers de $\binom{2n}{n}$ sont strictement inférieurs à $2n$.

Quatrième partie

Dans cette partie, on va prouver le postulat de Bertrand. On suppose, par l'absurde, l'existence d'un entier $n \geqslant 2$ tel que l'intervalle $]n, 2n[$ ne contienne aucun entier premier.

1. Montrer que l'entier n est nécessairement supérieur ou égal à 631.
   Indication : considérer les entiers premiers $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 13$, $p_5 = 23$, $p_6 = 43$, $p_7 = 83$, $p_8 = 163$, $p_9 = 317$, et $p_{10} = 631$.
2. Montrer que l'hypothèse faite sur n permet d'écrire $\binom{2n}{n} = \prod\limits_{p \in \mathbb{P}_n} p^{u_p(n)}$.
3. Utiliser les parties II et III pour établir $\binom{2n}{n} \leqslant (2n)^{\sqrt{2n}-1}\, 4^{2n/3}$.
   Indication : $p \in \mathbb{P}_n \Rightarrow (p \leqslant \sqrt{2n})$ ou $(\sqrt{2n} < p \leqslant \dfrac{2n}{3})$ ou $(\dfrac{2n}{3} < p \leqslant n)$.
4. En déduire que $4^{n/3} \leqslant (2n)^{\sqrt{2n}}$, puis $\varphi(\sqrt{2n}) \geqslant \dfrac{\ln 2}{6}$ avec $\varphi(x) = \dfrac{\ln x}{x}$.
5. Déduire que ce qui précède que n est inférieur à 450 et conclure.

Contexte historique

Le "postulat de Bertrand" fut pour la première fois conjecturé en 1845 par Joseph Bertrand (1822-1900) qui le vérifia lui-même pour tous les nombres de l'intervalle $[2, 3 \cdot 10^6]$.

La première démonstration date de 1850 et est dûe à Chebyshev (1821-1894). Ainsi le postulat est-il aussi appelé théorème de Chebyshev.

Ramanujan (1887-1920) en donna une démonstration plus simple et Paul Erdös (1913-1996) publia en 1932 une preuve élémentaire utilisant les coefficients binomiaux (c'est de cette preuve qu'est inspirée le problème ci-dessus).

Corrigé

Première partie

1. L'entier m est défini par $p^m \leqslant n < p^{m+1}$ c'est-à-dire $m \leqslant \dfrac{\ln n}{\ln p} < (m+1)$.
   Autrement dit l'entier m est donné par $m = \left[\dfrac{\ln n}{\ln p}\right]$.

2. Soit qp^k le plus grand multiple de p^k qui soit inférieur ou égal à n.
   L'entier q est caractérisé par $qp^k \leqslant n < (q+1)p^k$. On en déduit $q = \left[\dfrac{n}{p^k}\right]$.
   Avec ces notations, on a $E_n \cap p^k\mathbb{N} = \{jq^k, 1 \leqslant j \leqslant q\}$.
   Ainsi $\operatorname{card}(E_n \cap p^k\mathbb{N}) = q = \left[\dfrac{n}{p^k}\right]$.

   On remarque ensuite que $\{j \in E_n,\ v_p(j) = k\}$ est formé des éléments de E_n qui sont divisbles par p^k mais pas par p^{k+1} c'est-à-dire des éléments de $(E_n \cap p^k\mathbb{N}) \setminus (E_n \cap p^{k+1}\mathbb{N})$.

   Ainsi $\operatorname{card}\{j \in E_n,\ v_p(j) = k\} = \operatorname{card}(E_n \cap p^k\mathbb{N}) - \operatorname{card}(E_n \cap p^{k+1}\mathbb{N}) = \left[\dfrac{n}{p^k}\right] - \left[\dfrac{n}{p^{k+1}}\right]$.

   Remarque : le résultat est correct pour $k = m$.
   En effet $E_n \cap p^{m+1}\mathbb{N} = \emptyset$ et $\left[\dfrac{n}{p^{m+1}}\right] = 0$ donc $\operatorname{card}\{j \in E_n,\ v_p(j) = m\} = \left[\dfrac{n}{p^m}\right]$.

3. Pour tout $k \geqslant 2$, $v_p(k)$ est l'exposant de p dans la décomposition de k en produit de facteurs premiers.

   Il est clair alors que $v_p(jk) = v_p(j)v_p(k)$ pour tous $j, k \geqslant 2$ (c'est une conséquence de l'unicité de la décomposition en produit de facteurs premiers).

   Par une récurrence évidente, cela se généralise à un produit quelconque d'entiers.
   En particulier $v_p(n) = v_p\left(\prod\limits_{j=2}^{n} j\right) = \sum\limits_{j=2}^{n} v_p(j)$.

4. Dans la somme précédente, on se limite bien sûr aux indices j tels que $v_p(j) \geqslant 1$.

   On peut ensuite réorganiser la somme en groupant les valeurs de j pour lesquelles $v_p(j)$ a une valeur k donnée, avec $1 \leqslant k \leqslant m$, et on sait d'après la question (2) combien il existe de tels indices.

   On obtient alors $v_p(n) = \sum\limits_{j=2}^{n} v_p(j) = \sum\limits_{k=1}^{m} k\left(\left[\dfrac{n}{p^k}\right] - \left[\dfrac{n}{p^{k+1}}\right]\right)$.

   On trouve alors successivement :

$$\begin{aligned} v_p(n) &= \sum_{k=1}^{m} k\left[\frac{n}{p^k}\right] - \sum_{k=1}^{m} k\left[\frac{n}{p^{k+1}}\right] = \sum_{k=1}^{m} k\left[\frac{n}{p^k}\right] - \sum_{k=2}^{m+1}(k-1)\left[\frac{n}{p^k}\right] \\ &= \left[\frac{n}{p}\right] + \sum_{k=2}^{m}(k-(k-1))\left[\frac{n}{p^k}\right] - \underbrace{\left[\frac{n}{p^{m+1}}\right]}_{=0} = \sum_{k=1}^{m}\left[\frac{n}{p^k}\right] \end{aligned}$$

   En conclusion, on a l'égalité $v_p(n) = \sum\limits_{k=1}^{m}\left[\dfrac{n}{p^k}\right]$, avec $m = \left[\dfrac{\ln n}{\ln p}\right]$.

Deuxième partie

1. On a $(2n)! = (n!)^2\binom{2n}{n}$ donc $v_p((2n)!) = 2v_p(n) + u_p(n)$ (cf I.3)

   Ainsi $u_p(n) = v_p((2n)!) - 2v_p(n) = \sum\limits_{k=1}^{m'}\left[\dfrac{2n}{p^k}\right] - 2\sum\limits_{k=1}^{m}\left[\dfrac{n}{p^k}\right]$ (en utilisant I.4).

   Pour $k > m$, et notamment si $m < k \leqslant m'$, on a $p^k > n$ donc $\left[\dfrac{n}{p^k}\right] = 0$.

   On obtient donc $u_p(n) = \sum\limits_{k=1}^{m'}\left(\left[\dfrac{2n}{p^k}\right] - 2\left[\dfrac{n}{p^k}\right]\right)$ en regroupant les deux sommes.

2. (a) Il s'agit de montrer l'inégalité $u_p(n)\ln p \leq 2n$.

   Puisque $u_p(n)$ est un entier, cela équivaut à prouver $u_p(n) \leqslant m' = \left[\dfrac{\ln(2n)}{\ln p}\right]$.

   Mais on sait que $u_p(n) = \sum\limits_{k=1}^{m'}\left(\left[\dfrac{2n}{p^k}\right] - 2\left[\dfrac{n}{p^k}\right]\right)$.

   Il suffit donc pour conclure d'utiliser l'inégalité $[2x] - 2[x] \leqslant 1$ pour tout x de $\mathbb{R}$.

   En effet :

   $$\begin{cases} 2x - 1 < [2x] \leqslant 2x \\ 2x - 2 < 2[x] \leqslant 2x \end{cases} \Rightarrow \begin{cases} 2x - 1 < [2x] \leqslant 2x \\ -2x \leqslant -2[x] < -2x + 2 \end{cases} \Rightarrow -1 < [2x] - 2[x] < 2$$

   Ainsi, $\forall\, x \in \mathbb{R},\ [2x] - 2[x] \in \{0, 1\}$, et le résultat attendu en découle.

   (b) Si $\sqrt{2n} < p$, alors $p^k > 2n > n$ donc $\left[\dfrac{2n}{p^k}\right] = \left[\dfrac{n}{p^k}\right] = 0$ pour tout entier $k \geqslant 2$.

   Il en découle $u_p(n) = \sum\limits_{k=1}^{m'}\left(\left[\dfrac{2n}{p^k}\right] - 2\left[\dfrac{n}{p^k}\right]\right) = \left[\dfrac{2n}{p}\right] - 2\left[\dfrac{n}{p}\right] \in \{0, 1\}$.

   (c) Si $\dfrac{2n}{3} < p \leq n$, alors $2 \leqslant \dfrac{2n}{p} < 3$ et $1 \leqslant \dfrac{n}{p} < \dfrac{3}{2}$ donc $\left[\dfrac{2n}{p}\right] = 2$ et $\left[\dfrac{n}{p}\right] = 1$.

   D'autre part $3p > 2n \Rightarrow 9p^2 \geqslant (2n+1)^2 \Rightarrow 9(p^2 - 2n) \geqslant 4n(n-4) + 2n + 1$.

   Si $n \geqslant 4$ alors $p^2 > 2n$ puis, pour tout $k \geqslant 2$: $p^k \geqslant p^2 > 2n > n$.

   Donc si $n \geqslant 4$, de manière analogue à la question (b) : $u_p(n) = \left[\dfrac{2n}{p}\right] - 2\left[\dfrac{n}{p}\right] = 0$.

   Si $n = 3$, alors $\dfrac{2n}{3} < p \leq n \Leftrightarrow p = n = 3$, et $u_p(n) = v_3\left(\binom{6}{3}\right) = v_3(20) = 0$.

   On a donc montré que si $n \geqslant 3$ alors : $\dfrac{2}{3}n < p \leq n \Rightarrow u_p(n) = 0$.

   NB : c'est faux si $n = 2$ car alors $p = 2$ et $u_p(n) = v_2\left(\binom{4}{2}\right) = v_2(6) = 1$.

   (d) Si $n < p < 2n$, alors : $1 < \dfrac{2n}{p} < 2$ et $\dfrac{1}{2} < \dfrac{n}{p} < 1$. Il en découle $\left[\dfrac{2n}{p}\right] = 1$ et $\left[\dfrac{n}{p}\right] = 0$.

   Pour $k \geqslant 2$ on a $p^k \geqslant p^2 > n^2 \geqslant 2n > n$ donc $\left[\dfrac{2n}{p^k}\right] = \left[\dfrac{n}{p^k}\right] = 0$.

   On en déduit : $u_p(n) = \left[\dfrac{2n}{p}\right] - 2\left[\dfrac{n}{p}\right] = 1$.

Troisième partie

1. On peut se limiter à $0 \leqslant k \leqslant n$ car on sait que $\binom{2n}{k} = \binom{2n}{2n-k}$.

   Si $0 \leqslant k < n$ on a $\binom{2n}{k+1} = \dfrac{(2n)!}{(k+1)!(2n-k-1)!} = \dfrac{2n-k}{k+1}\dfrac{(2n)!}{k!(2n-k)!} = \dfrac{2n-k}{k+1}\binom{2n}{k}$.

   Mais $0 \leqslant k < n \Rightarrow 1 \leqslant k+1 < 2n-k \Rightarrow \dfrac{2n-k}{k+1} > 1 \Rightarrow \binom{2n}{k+1} > \binom{2n}{k}$.

   Ainsi la suite $k \mapsto \binom{2n}{k}$ est strictement croissante pour $0 \leqslant k \leqslant n$.

   On en déduit que si $0 \leqslant k \leqslant 2n$ alors $\binom{2n}{k} \leqslant \binom{2n}{n}$.

   En utilisant ce résultat pour $0 < k < 2n$, la formule du binôme et $\binom{2n}{n} \geqslant 2$, on trouve :

   $$4^n = \sum_{k=0}^{2n}\binom{2n}{k} = 2 + \sum_{k=1}^{2n-1}\binom{2n}{k} \leqslant 2 + (2n-1)\binom{2n}{n} \leqslant 2n\binom{2n}{n}.$$

2. (a) On peut écrire $\Pi_{2m+1} = \prod_{2 \leqslant p \leqslant 2m+1} p = \prod_{2 \leqslant p \leqslant m+1} p \prod_{m+1 < p \leqslant 2m+1} p = \Pi_{m+1} \prod_{m+1 < p \leqslant 2m+1} p$.

   On a l'égalité $\binom{2m+1}{m} m!\,(m+1)! = (2m+1)!$

   Soit p un entier premier tel que $m+1 < p \leqslant 2m+1$. Alors p divise $(2m+1)!$.

   Mais p est premier avec les entiers de $\{1, \ldots, m+1\}$ donc avec le produit $m!\,(m+1)!$

   Il s'ensuit (théorème de Gauss) que p divise $\binom{2m+1}{m}$.

   $\binom{2m+1}{m} m!$ est donc divisible par le produit des p de $\mathbb{P}$ tels que $m+1 < p \leqslant 2m+1$.

   Il en découle bien sûr $\prod_{m+1 < p \leqslant 2m+1} p \leqslant \binom{2m+1}{m}$ donc $\Pi_{2m+1} \leqslant \binom{2m+1}{m}\Pi_{m+1}$.

   D'autre part $\binom{2m+1}{m} = \binom{2m}{m} + \binom{2m}{m-1} \leqslant \sum_{k=0}^{2m}\binom{2m}{k}$ donc $\binom{2m+1}{m} \leqslant 4^m$.

   On a donc obtenu $\Pi_{2m+1} \leqslant \binom{2m+1}{m}\Pi_{m+1} \leqslant 4^m \Pi_{m+1}$ pour tout $m \geqslant 1$.

   (b) On prouve d'abord la propriété pour tout entier $n \geqslant 2$, par récurrence forte sur n.

   Le résultat est évident sur $n = 2$.

   On se donne $n \geqslant 3$ et on suppose que $\Pi_m \leqslant 4^m$ pour tout m tel que $2 \leqslant m < n$.

   Il s'agit donc de prouver l'inégalité $\Pi_n \leqslant 4^n$.

   Si n est pair (donc $n \geqslant 4$), alors $\Pi_n = \Pi_{n-1} \leqslant 4^{n-1} \leqslant 4^n$.

   On suppose donc que n est impair et on pose $n = 2m+1$ avec $m \geqslant 1$.

   La question précédente donne $\Pi_n = \Pi_{2m+1} \leqslant 4^m \Pi_{m+1}$.

   L'hypothèse de récurrence fournit alors $\Pi_n \leqslant 4^m 4^{m+1}$ c'est-à-dire $\Pi_n \leqslant 4^n$.

   On a donc obtenu l'inégalité $\Pi_n \leqslant 4^n$ pour tout entier $n \geqslant 2$.

   Enfin, pour tout réel $x \geqslant 2$, $\Pi_x = \Pi_{[x]} \leqslant 4^{[x]} \leqslant 4^x$.

3. Soit p un diviseur premier de $\binom{2n}{n}$. On sait que $\binom{2n}{n}(n!)^2 = (2n)!$

   Ainsi p divise $(2n)!$ donc divise un élément de $\{2, \ldots, 2n\}$, donc $p < 2n$.

Quatrième partie

1. Supposons qu'au contraire on ait l'égalité $n \leqslant 630$.

   Avec les notations de l'énoncé, notons k (avec $k \leqslant 9$) l'indice maximum tel que $p_k \leqslant n$.

   Alors $p_k \leqslant n < 2n \leqslant p_{k+1}$ puisque $]n, 2n[$ ne contient aucun entier premier.

   Mais $p_{k+1} < 2p_k$ (c'est pour assurer cette propriété qu'on a choisi $p_1, p_2, \ldots, p_{10}$).

   On trouve donc $p_k \leqslant n < 2n \leqslant p_{k+1} < 2p_k$ ce qui est absurde.

   Il en découle que l'entier n est nécessairement supérieur ou égal à 631.

2. (a) D'après (IV.2) : $\binom{2n}{n} = \prod_{p\in\mathbb{P}_{2n-1}} p^{u_p(n)}$. Mais par hypothèse $u_p(n) = 0$ si $n < p < 2n$.

   On obtient donc la décomposition en facteurs premiers : $\binom{2n}{n} = \prod_{p\in\mathbb{P}_n} p^{u_p(n)}$.

   (b) On définit les trois ensembles suivants :

   $A_n = \{p \in \mathbb{P}, p \leqslant \sqrt{2n}\}$, $B_n = \{p \in \mathbb{P}, \sqrt{2n} < p \leqslant \frac{2n}{3}\}$, $C_n = \{p \in \mathbb{P}, \frac{2n}{3} < p \leqslant n\}$.

   On a bien sûr $\mathbb{P}_n = A_n \cup B_n \cup C_n$ donc $\prod_{p\in\mathbb{P}_n} p^{u_p(n)} \leqslant \prod_{p\in A_n} p^{u_p(n)} \prod_{p\in B_n} p^{u_p(n)} \prod_{p\in C_n} p^{u_p(n)}$

   (cette dernière inégalité est justifiée par le fait que tous les facteurs sont $\geqslant 1$).

   — D'une part $\prod_{p\in C_n} p^{u_p(n)} = 1$ (cf II.2.c). En effet $n \geqslant 3$ donc $\forall\, n \in C_n,\ u_p(n) = 0$.

   — D'après (II2.b) on a $u_p(n) \leqslant 1$ pour tout p de B_n.

   Il en découle $\prod_{p\in B_n} p^{u_p(n)} \leqslant \prod_{p\in B_n} p \leqslant \prod_{p\leqslant 2n/3} p = \Pi_{2n/3} \leqslant 4^{2n/3}$.

   — Enfin, on sait que $p^{u_p(n)} \leqslant 2n$ (cf II.2.a) pour tout p, et en particulier pour $p \in A_n$.

   Or $A_n = \{p \in \mathbb{P}, 2 \leqslant p \leqslant \sqrt{2n}\}$ est bien sûr constitué d'au plus $\sqrt{2n} - 1$ éléments.

   On en déduit l'inégalité $\prod_{p\in A_n} p^{u_p(n)} \leqslant (2n)^{\sqrt{2n}-1}$.

   Finalement, on a bien obtenu l'inégalité $\binom{2n}{n} \leqslant (2n)^{\sqrt{2n}-1}\, 4^{2n/3}$.

   (c) On a $\frac{4^n}{2n} \leqslant \binom{2n}{n} \leqslant (2n)^{\sqrt{2n}-1}\, 4^{2n/3}$ donc $4^{n/3} \leqslant (2n)^{\sqrt{2n}}$ donc $\frac{2n}{3} \ln 2 \leqslant \sqrt{2n}\, \ln(2n)$.

   Cela s'écrit $\frac{\ln(2n)}{\sqrt{2n}} \geqslant \frac{\ln 2}{3}$ ou encore $\varphi(\sqrt{2n}) \geqslant \frac{\ln 2}{6}$ avec $\varphi(x) = \frac{\ln x}{x}$.

   (d) φ décroit pour $x \geqslant \mathrm{e}$ car $\varphi'(x) = \frac{1 - \ln x}{x}$. Or numériquement $\varphi(30) = \frac{\ln 30}{30} < \frac{\ln 2}{6}$.

   Il en découle $\sqrt{2n} < 30$ donc $n < 450$.

   Cela est contradictoire avec le résultat de la question IV.1.

   Conclusion : le postulat de Bertrand est vérifié pour tout entier $n \geqslant 2$.