Exercices de khôlle - semaine 2, groupe 11

Exercice 1 Soit $(p_n)_{n\in\mathbf{N}}$ la suite des nombres premiers. Pour tout nombre premier p, on définit l'application :

$$v_p : \begin{array}{ccc} \mathbf{N}^* & \longrightarrow & \mathbf{N} \\ n = p_1^{\alpha_1}\cdots p_k^{\alpha_k} & \longmapsto & \alpha_p \end{array}$$

L'existence et l'unicité de la décomposition en nombres premiers de tout entier naturel non nul garantit que v_p est correctement définie sur $\mathbf{N}^*$. On dit que $v_p(n)$ est la p-valuation de n.

Pour tout entier n, on désigne par $\lfloor n\rfloor$ la partie entière de n.

Montrer que pour tout entier naturel n, on a :

$$v_p(n!) = \sum_{i\geq 1}\left\lfloor \frac{n}{p^i}\right\rfloor$$

Première démonstration Démontrons d'abord le lemme suivant.

Lemme - Pour tout réel positif a et tout entier naturel n, on a $\left\lfloor \frac{\lfloor a\rfloor}{n}\right\rfloor = \left\lfloor \frac{a}{n}\right\rfloor$.

Démonstration - Notons ϵ le réel positif strictement inférieur à 1 tel que $a = \lfloor a\rfloor + \epsilon$. Écrivons la division euclidienne de $\lfloor a\rfloor$ par n : on a $\lfloor a\rfloor = nq+r$, où q est un entier naturel et r un entier naturel vérifiant $0\leq r<n$. On a également $r+\epsilon<n$; en effet, comme r est un entier naturel, on a $r\leq n-1$ d'où $r+\epsilon\leq n-1+\epsilon<n$ car $\epsilon<1$. Ainsi, on a $\left\lfloor \frac{\lfloor a\rfloor}{n}\right\rfloor = \left\lfloor \frac{\lfloor nq+r+\epsilon\rfloor}{n}\right\rfloor = \left\lfloor \frac{nq+r}{n}\right\rfloor = q + \left\lfloor \frac{r}{n}\right\rfloor = q$ car $r<n$, et $\left\lfloor \frac{a}{n}\right\rfloor = \left\lfloor \frac{nq+r+\epsilon}{n}\right\rfloor = q + \left\lfloor \frac{r+\epsilon}{n}\right\rfloor = q$ car $r+\epsilon<n$, d'où le résultat demandé.

On vérifie que la propriété à démontrer est vraie pour $n=0$.

Soit n un entier naturel non nul. Supposons la propriété vérifiée pour tout entier strictement inférieur à n. Remarquons que $n! = \prod_{i=1}^{n} i$ contient exactement $\left\lfloor \frac{n}{p}\right\rfloor$ facteurs qui sont des multiples de p. En comptant ces facteurs, on peut écrire :

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

Cependant, remarquons que l'on a :

$$v_p\left(\frac{n!}{p^{\left\lfloor \frac{n}{p}\right\rfloor}}\right) = v_p\left(\left\lfloor \frac{n}{p}\right\rfloor !\right)$$

En effet, diviser par $p^{\left\lfloor \frac{n}{p}\right\rfloor}$ revient à diviser par p les $\left\lfloor \frac{n}{p}\right\rfloor$ multiples de p apparaissant dans l'écriture de la factorielle comme produit des entiers de 1 à n. Les éventuelles puissances de p restantes correspondaient avant division à des multiples de p^2, qui apparaissent maintenant de la même manière que dans l'écriture de $\left\lfloor \frac{n}{p}\right\rfloor !$. On peut le représenter de la manière suivante :

$$\begin{array}{lccccccccccccccccc}
n! & = 1\cdots & p\cdots & 2p\cdots & 3p\cdots & p^2\cdots & (p+1)p\cdots & 2p^2\cdots & (2p+1)p\cdots & p^3\cdots & \left\lfloor \frac{n}{p}\right\rfloor p\cdots & n \\
\frac{n!}{p^{\left\lfloor \frac{n}{p}\right\rfloor}} & = 1\cdots & 1\cdots & 2\cdots & 3\cdots & p\cdots & (p+1)\cdots & 2p\cdots & (2p+1)\cdots & p^2\cdots & \left\lfloor \frac{n}{p}\right\rfloor \cdots & n \\
\left\lfloor \frac{n}{p}\right\rfloor ! & = 1\cdots & \cdots & \cdots & \cdots & p\cdots & \cdots & \cdots & \cdots & p^2\cdots & \cdots & \left\lfloor \frac{n}{p}\right\rfloor
\end{array}$$

Or, par application de l'hypothèse de récurrence puis du lemme, on a :

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

Ainsi, en décalant l'indice i, on obtient :

$$v_p(n!) = \left\lfloor\frac{n}{p}\right\rfloor + \sum_{i\geq 2}\left\lfloor\frac{n}{p^i}\right\rfloor = \sum_{i\geq 1}\left\lfloor\frac{n}{p^i}\right\rfloor$$

La propriété est donc vérifiée pour n.
Par récurrence avec prédécesseurs, la propriété est vérifiée pour tout entier naturel n.

Seconde démonstration Soit $(\chi_{i,j})_{i,j\in\mathbf{N}}$ la suite telle que $\chi_{i,j}$ vaille 1 si p^i divise j et zéro sinon. Étudions la somme $S_n = \sum_{i\geq 1}\sum_{j=1}^{n}\chi_{i,j}$. Comme $\chi_{i,j}$ est nul pour tout couple (i,j) vérifiant $j \leq n$ et $i \geq n$, S_n est en fait une somme finie. On peut donc la calculer en permutant les deux symboles de sommation, et sa valeur restera identique. On peut représenter les valeurs de χ de la manière suivante :

χ	1	2	$\cdots$	p	$\cdots$	$2p$	$\cdots$	$3p$	$\cdots$	p^2	$\cdots$	$(p+1)p$	$\cdots$	$2p^2$	$\cdots$	$(2p+1)p$	$\cdots$	p^3	$\cdots$	$\left\lfloor\frac{n}{p}\right\rfloor p$	$\cdots$	n	$n+1$	$\cdots$
1	0	0	$\cdots$	1	$\cdots$	1	$\cdots$	1	$\cdots$	1	$\cdots$	1	$\cdots$	1	$\cdots$	1	$\cdots$	1	$\cdots$	1	$\cdots$	0	0	$\cdots$
2	0	0	$\cdots$	0	$\cdots$	0	$\cdots$	0	$\cdots$	1	$\cdots$	0	$\cdots$	1	$\cdots$	0	$\cdots$	1	$\cdots$	0	$\cdots$	0	0	$\cdots$
3	0	0	$\cdots$	0	$\cdots$	0	$\cdots$	0	$\cdots$	0	$\cdots$	0	$\cdots$	0	$\cdots$	0	$\cdots$	1	$\cdots$	0	$\cdots$	0	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

La somme $\sum_{j=1}^{n}\chi_{i,j}$ correspond au nombre de multiples de p^i entre 1 et n. Elle vaut donc $\left\lfloor\frac{n}{p^j}\right\rfloor$. Ainsi, $S(n) = \sum_{i\geq 1}\left\lfloor\frac{n}{p^i}\right\rfloor$.

Mais, si l'on somme d'abord selon i, on voit que la somme $\sum_{i\geq 1}\chi_{i,j}$ est la p-valuation de j, car elle revient à compter le nombre de facteurs p qui interviennent dans la décomposition en facteurs premiers de j. On obtient donc $S(n) = \sum_{j=1}^{n} v_p(j)$. Mais pour tout couple (a,b) d'entiers naturels non nuls, on a $v_p(a\cdot b) = v_p(a) + v_p(b)$. De ce fait, $S(n) = v_p\left(\prod_{j=1}^{n} j\right) = v_p(n!)$. D'où le résultat demandé.

Exercice 2 On désigne par ϕ la fonction indicatrice d'Euler. Soit a un entier naturel non nul différent de 1. Montrer que pour tout entier naturel k, k divise $\phi\left(a^k-1\right)$.

Démonstration rédigée par Gautier Démontrons d'abord le lemme suivant.

Lemme - Soient p, q des entiers naturels non nuls. Si a^p-1 divise a^q-1, alors p divise q.
Démonstration - Écrivons la division euclidienne de q par p : on a $q = np + r$, où n est un entier naturel et r un entier naturel vérifiant $0 \leq r < p$. Comme a^p-1 divise a^q-1, on a $a^{np+r} \equiv 1 \pmod{a^p-1}$. Mais comme $a^p \equiv 1 \pmod{a^p-1}$, on a $a^{np} \equiv 1 \pmod{a^p-1}$, d'où $a^{np+r} - a^{np} \equiv 0 \pmod{a^p-1}$. Ainsi a^p-1 divise $a^{np}\left(a^r-1\right)$.

Cependant, comme a^p-1 et a^{np} sont premiers entre eux, par application du théorème de Gauß, a^p-1 divise a^r-1. Mais comme $r<p$ du fait de l'écriture de la division euclidienne, on a $a^r-1 < a^p-1$, d'où l'on déduit que $a^r-1=0$, soit $r=0$ car $a>1$. Ainsi, on a $r=0$, et $q=np$, ce qui permet d'affirmer que p divise q, le résultat demandé.

Comme a et a^k-1 sont premiers entre eux, on a par application du théorème d'Euler $a^{\phi\left(a^k-1\right)} \equiv 1 \pmod{a^k-1}$. De cela, on déduit que a^k-1 divise $a^{\phi\left(a^k-1\right)}-1$, et donc que k divise $\phi\left(a^k-1\right)$, le résultat demandé.