

Question 2010

Vincent Devinck

Question. Quels sont les couples (q, n) d'entiers strictement positifs pour lesquels $n!$ divise

$$\prod_{k=0}^{n-1} (q^n - q^k) ?$$

Dans le cas où q est une puissance d'un nombre premier, le couple (q, n) vérifie pour tout n cette propriété car $\text{GL}_n(\mathbb{F}_q)$, où \mathbb{F}_q est le corps ayant q éléments, contient le sous-groupe des matrices de permutation.

(Vincent Devinck)

Une réponse. Nous allons montrer que tous les couples $(n, q) \in (\mathbb{N}^*)^2$ sont solutions.

Théorème 1. Pour tous $n, q \in \mathbb{N}^*$, on a $n! \mid \prod_{k=0}^{n-1} (q^n - q^k)$.

Il n'y a rien à faire si $n = 1$ ou $q = 1$. Si n et q sont des entiers supérieurs ou égaux à 2, on pose dans la suite $P_{n,q} = \prod_{k=0}^{n-1} (q^n - q^k)$. En notant classiquement \mathcal{P} l'ensemble des nombres premiers, il s'agit de montrer que :

$$\forall p \in \mathcal{P}, \quad v_p(n!) \leq v_p(P_{n,q})$$

Les deux lemmes suivants vont nous permettre de faire cette comparaison.

Lemme 1 (formule de Legendre). Pour tous $n \in \mathbb{N}^*$ et $p \in \mathcal{P}$, on a :

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

Démonstration. Pour tout entier $k \geq 1$, notons a_k le nombre de facteurs du produit $n! = n(n-1) \times \dots \times 1$ qui sont exactement divisibles par p^k . Comme le nombre d'entiers $\ell \in \llbracket 1, n \rrbracket$ divisibles par p^k est égal à $\left\lfloor \frac{n}{p^k} \right\rfloor$, on a (il n'y a pas de problème de convergence des séries mises en jeu) :

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{+\infty} k a_k = \sum_{k=1}^{+\infty} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) \\ &= \sum_{k=1}^{+\infty} k \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=1}^{+\infty} (k-1) \left\lfloor \frac{n}{p^k} \right\rfloor, \end{aligned}$$

ce qu'il fallait démontrer. □

Le deuxième résultat est une conséquence du petit théorème de Fermat.

Lemme 2. Soient $p \in \mathcal{P}$ et q un entier positif premier avec p . Alors :

$$\forall k \in \mathbb{N}^*, \quad q^{p^k - p^{k-1}} \equiv 1 \pmod{p^k}$$

Démonstration. On procède par récurrence. Le cas $k = 1$ est précisément le petit théorème de Fermat. Supposons que la relation soit vraie au rang $k \in \mathbb{N}^*$. On en déduit qu'il existe $\alpha \in \mathbb{N}$ tel que $q^{p^k - p^{k-1}} = 1 + \alpha p^k$. Ainsi :

$$q^{p^{k+1} - p^k} = (1 + \alpha p^k)^p = 1 + \alpha p^{k+1} + \sum_{\ell=2}^p \binom{p}{\ell} \alpha^\ell p^{k\ell},$$

La relation au rang $k + 1$ s'ensuit. □

Démonstration du théorème. Tout d'abord, en factorisant par q^k dans le produit puis en changeant d'indice, on a :

$$P_{n,q} = q^{\frac{n(n-1)}{2}} \prod_{\ell=1}^n (q^\ell - 1)$$

Soit $p \in \mathcal{P}$. On distingue deux cas.

★ **Premier cas :** p est un facteur premier de q

L'égalité précédente entraîne que $v_p(P_{n,q}) = \frac{n(n-1)}{2} v_p(q)$. Par ailleurs, la formule de Legendre nous donne la majoration :

$$v_p(n!) \leq n \sum_{k=1}^{+\infty} \frac{1}{p^k} = \frac{n}{p-1} \leq n \leq \frac{n(n-1)}{2}$$

pour $n \geq 3$. On vérifie facilement que $P_{2,q}$ est pair donc on a bien, pour tout $n \geq 2$, l'inégalité $v_p(n!) \leq v_p(P_{n,q})$.

★ **Deuxième cas :** p n'est pas un facteur premier de q

On a alors $v_p(P_{n,q}) = v_p \left(\prod_{\ell=1}^n (q^\ell - 1) \right)$. Nous allons nous contenter de minorer cette valuation. D'après le Lemme 2 (et la compatibilité de la relation de congruence avec l'exponentiation positive entière), pour que p^k divise $q^\ell - 1$, il suffit que ℓ soit un multiple de $p^k - p^{k-1}$. En se contentant de tels facteurs $q^\ell - 1$ et en imitant la preuve de la formule de Legendre, il vient :

$$v_p(P_{n,q}) \geq \sum_{k=1}^{+\infty} k \left(\left\lfloor \frac{n}{p^k - p^{k-1}} \right\rfloor - \left\lfloor \frac{n}{p^{k+1} - p^k} \right\rfloor \right) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k - p^{k-1}} \right\rfloor$$

Or il est clair que :

$$\forall k \in \mathbb{N}^*, \quad \left\lfloor \frac{n}{p^k} \right\rfloor \leq \left\lfloor \frac{n}{p^k - p^{k-1}} \right\rfloor,$$

donc $v_p(n!) \leq v_p(P_{n,q})$.

Le théorème est démontré.