Petit théorème de Fermat

Emmanuel Vieillard-Baron[1], Alain Soyeur[2], and François Capaces[3]

[1]Enseignant en CPGE, Lycée Kléber, Strasbourg
[2]Enseignant en CPGE, Lycée Pierre de Fermat, Toulouse
[3], ,

23 mars 2024

Exercice 0.1 ★ ***Petit théorème de Fermat***

Soit p un nombre premier.

1. *Montrer que* $\forall k \in [\![1, p-1]\!], \quad p \mid \binom{p}{k}$.
2. *En déduire le petit théorème de Fermat :*

$$\forall n \in \mathbb{Z}, \quad p \mid n^p - n.$$

Solution :

1. *Soit $k \in [\![1, p-1]\!]$. On sait que $A_p^k = k!\binom{p}{k}$. Mais $p \mid A_p^k = p(p-1)\dots(p-n+1)$ donc comme p est premier $p \mid k!$ ou $p \mid \binom{p}{k}$. Si $p \mid k!$ alors p divise un des entiers $1, 2, \dots, k < p$ ce qui n'est pas possible et prouve la propriété.*
2. *On effectue un raisonnement par récurrence. Si $n = 0$ alors la propriété est vérifiée. Soit $n \in \mathbb{N}$. On la suppose vraie au rang n : $p \mid n^p - n$ et on montre que $p \mid (n+1)^p - (n+1)$. On utilise la formule du binôme :*

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

Comme $p \mid n^p - n$ et que $p \mid \binom{p}{k}$ pour $k \in [\![1, p-1]\!]$, on sait que $p \mid (n+1)^p - (n+1)$ et le petit théorème de Fermat est prouvée par récurrence pour $n \geqslant 0$. Si $n < 0$ et si $p = 2$ alors $n^2 - n = n(n-1)$ est clairement divisible par 2. Si $p > 2$, comme p est premier il est impair et en notant $m = -n$, on a $n^p - n = -m^p + m = -(m^p - m)$ qui est divisible par p.

Références