Résultat d'arithmétique

Le texte suivant est une réponse au problème 538-3 paru dans la revue *Au fil des maths* (décembre 2020) de l'APMEP.

Idée générale : On se propose de démontrer que pour tout entier premier impair p et tout entier naturel non nul k tel que k n'est pas divisble par $p-1$, on a :

$$1^k + 2^k + \ldots + (p-1)^k \quad \text{est divisible par } p$$

On commence par démontrer deux lemmes, correspondant à deux cas particuliers :
celui où $PGCD(k\,; p-1) = 1$ et celui où k divise strictement $p-1$.
La démonstration de ces deux lemmes est en fait basée sur l'étude du comportement du morphisme suivant :

$$\phi : \left\{ \begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ x & \longmapsto & x^k \end{array} \right.$$

Lemme 1

Pour tout entier p premier impair et tout entier naturel k tel que $\mathrm{PGCD}(k\,; p-1) = 1$:

$$1^k + 2^k + \ldots + (p-1)^k \text{ est divisible par } p.$$

Démonstration.
Soit p un entier premier impair et k un entier naturel non nul et premier avec $p-1$.
On considère l'application $\phi : \left\{ \begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ x & \longmapsto & x^k \end{array} \right.$
Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est commutatif, il est clair que l'application ϕ est un morphisme de groupes.
Il s'agit en fait d'un isomorphisme.
En effet, on commence par montrer que ϕ est injective :
Soit $x \in \ker \phi$, c'est-à-dire $x^k = 1$.
Cela signifie que l'ordre de x divise k dans $(\mathbb{Z}/p\mathbb{Z})^*$. Comme on sait, d'après le petit théorème de Fermat que l'ordre de x divise $p-1$ et que k et $p-1$ sont premiers entre eux, on en déduit que l'ordre de x est égal à 1.
Autrement dit, on en déduit que $x = 1$.
Finalement, cela prouve que $\ker(\phi) = \{1\}$ et donc que ϕ est injective.
Comme les ensembles de départ et d'arrivée sont de même cardinaux, ϕ est donc un isomorphisme.

On pose $S = 1^k + 2^k + \ldots + (p-1)^k \quad \text{et} \quad S' = 1 + 2 + \ldots + (p-1)$.
Le fait que ϕ soit un isomorphisme a pour conséquence que $S \equiv S'\,[p]$.
Or $S' = \frac{p(p+1)}{2} \equiv 0\,[p]$ car $\frac{p(p+1)}{2}$ est divisible par p $\left(\frac{p+1}{2}\right.$ est un entier).
Finalement, on a bien $S \equiv 0\,[p]$, ce qui signifie que p divise S. $\square$

Lemme 2

Pour tout entier p premier impair et tout entier naturel $k < p-1$ tel que k divise $p-1$:

$$1^k + 2^k + \ldots + (p-1)^k \text{ est divisible par } p.$$

Démonstration.
Comme $k|p-1$, il existe $k' \in \mathbb{N}$ tel que $p-1 = kk'$.
On considère le morphisme $\phi : \left\{ \begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* \\ x & \longmapsto & x^k \end{array} \right.$.
Le noyau de ϕ est un sous groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ et de cardinal un diviseur de $p-1$.
On note $n = \mathrm{Card}(\ker \phi)$.
Ainsi, $\mathrm{Im}(\phi)$ est de cardinal $\dfrac{p-1}{n} = n' > 1$.
Chaque élément de $\mathrm{Im}(\phi)$ admet d'ailleurs exactement n antécédents par ϕ.
De plus, on sait que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique donc en notant, b un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$, il en résulte que b^n est un générateur de $\mathrm{Im}(\phi)$.
En résumé, cela signifie que pour tout $x \in \mathrm{Im}(\phi)$, il existe $0 \leqslant l \leqslant n'-1$ tel que $x = b^{nl}$ et que x admet exactement n antécédents.
En posant $S = 1^k + 2^k + \ldots + (p-1)^k$, on en déduit que :

$$\begin{aligned}
S &\equiv n \times \left(\sum_{l=0}^{n'-1} b^{nl} \right) [p] \\
&\equiv n \times (1-b)^{-1} \times \left(1 - b^{nn'}\right) [p] \qquad ((1-b) \text{ est inversible car } b \neq 1 \text{ car } \mathrm{Card}(\mathrm{Im}(\phi)) > 1) \\
&\equiv n \times (1-b)^{-1} \times \left(1 - b^{p-1}\right) [p] \\
&\equiv n \times (1-b)^{-1} \times 0 \ [p] \qquad \text{d'après le petit théorème de Fermat} \\
&\equiv 0 \ [p]
\end{aligned}$$

Finalement, cela signifie que p divise S. $\square$

Proposition 1

Pour tout entier p premier impair et tout entier k tel que k n'est pas divisble par $p-1$:

$$1^k + 2^k + \ldots + (p-1)^k \text{ est divisible par } p.$$

Démonstration.
Soit p un entier premier impair et k un entier naturel non nul non divisible par $p-1$.
On pose $d = \mathrm{PGCD}(k, p-1)$. On a donc $d < p-1$.
De plus, il existe $k' \in \mathbb{N}^*$ tel que $k = dk'$ avec $PGCD(k' \,; p-1) = 1$. Ainsi,

$$\begin{aligned}
1^k + 2^k + \ldots + (p-1)^k &\equiv 1^{dk'} + 2^{dk'} + \ldots + (p-1)^{dk'} \ [p] \\
&\equiv \left(1^{k'}\right)^d + \left(2^{k'}\right)^d + \ldots + \left((p-1)^{k'}\right)^d [p] \\
&\equiv 1^d + 2^d + \ldots + (p-1)^d \ [p] \qquad \text{car } \mathrm{PGCD}(k' \,; p-1) = 1 \text{ (lemme 1)} \\
&\equiv 0 \ [p] \qquad \text{car } d \text{ divise } p-1 \text{ (lemme 2).}
\end{aligned}$$

Ainsi, on a bien montré que p divise $1^k + 2^k + \ldots + (p-1)^k$. $\square$