Un théorème de Wolstenhome

Gilles Auriol
auriolg@free.fr — http ://auriolg.free.fr

Théorème. — *Soit $p \geqslant 5$ un nombre premier et* $\displaystyle\sum_{k=1}^{p-1} \frac{1}{k} = \frac{A}{B}$ *écrit sous forme irréductible. Alors p^2 divise A.*

Preuve. — Pour tout tout $k \in [\![1, p-1]\!]$, on pose $p_k = \displaystyle\prod_{\substack{1 \leqslant i \leqslant p-1 \\ i \neq k, i \neq p-k}} i = \frac{(p-1)!}{k\,(p-k)}$. Une astuce classique permet d'écrire

$$\frac{A}{B} = \sum_{k=1}^{p-1} \frac{1}{k} = \frac{1}{2} \sum_{k=1}^{p-1} \left(\frac{1}{k} + \frac{1}{p-k} \right) = \frac{1}{2} \sum_{k=1}^{p-1} \frac{p}{k(p-k)} = \frac{p}{2} \sum_{k=1}^{p-1} \frac{1}{k(p-k)} = \frac{p}{2(p-1)!} \sum_{k=1}^{p-1} p_k$$

Par conséquent on arrive à

$$pB \times \sum_{k=1}^{p-1} p_k = 2A\,(p-1)! \tag{1}$$

Pour $k \in [\![1, p-1]\!]$, on a $k(p-k)p_k = (p-1)! \equiv -1\,[p]$ par le théorème de Wilson[1], d'où $-k^2 p_k \equiv -1\,[p]$, c'est-à-dire que dans $\mathbb{Z}/p\mathbb{Z}$, $\widetilde{p_k} = \widetilde{k}^{-2}$ (k étant inversible puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps). Par suite

$$\sum_{k=1}^{p-1} \widetilde{p_k} = \sum_{k=1}^{p-1} \widetilde{k}^{-2} = \sum_{k=1}^{p-1} \left(\widetilde{k}^{-1} \right)^2 = \sum_{k=1}^{p-1} \widetilde{k}^2 \tag{2}$$

la dernière égalité résultant du fait, évident, que l'application $\widetilde{k} \mapsto \widetilde{k}^{-1}$ est une permutation de $\mathbb{Z}/p\mathbb{Z} - \{0\}$.

Dans $\mathbb{N}$, on a $\displaystyle\sum_{k=1}^{p-1} k^2 = \frac{p(p-1)(2p-1)}{6}$. Or $\mathrm{pgcd}(p, 6) = 1$ car $p \geqslant 5$ est premier. Ainsi 6 divise $(p-1)(2p-1)$ et p est un diviseur du membre de droite, donc p divise $\displaystyle\sum_{k=1}^{p-1} k^2$, et d'après l'égalité (2) il divise aussi $\displaystyle\sum_{k=1}^{p-1} p_k$ et il existe $k \in \mathbb{N}$ tel que $\displaystyle\sum_{k=1}^{p-1} p_k = kp$; par suite l'identité (1) s'écrit $p^2 \times kB = A \times 2(p-1)!$ et le théorème de Gauss assure alors que p^2 divise A puisque p (donc p^2) est premier avec $2(p-1)!$. ∎

[1] Rappel du théorème de Wilson. Soit p un entier naturel, p premier $\equiv (p-1)! \equiv -1\,[p]$.