# Le Petit Fermat

**Lemme.** Soit $p$ un nombre premier, et $0 < k < p$ un entier. Alors $p$ divise $\binom{p}{k}$.

**Démonstration :** On a que $\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$ est un entier. Donc $k!\,(p-k)!$ divise $p! = p\,(p-1)!$. Or, $k!\,(p-k)!$ est un produit de facteurs $< p$, et donc premier avec $p$. Ainsi $k!\,(p-k)!$ est premier avec $p$. D'après le lemme de Gauss, $k!\,(p-k)!$ divise $(p-1)!$, et $p$ divise $\frac{p\,(p-1)!}{k!\,(p-k)!} = \frac{p!}{k!\,(p-k)!} = \binom{p}{k}$. $\square$

**Théorème (Petit Théorème de Fermat).** Soit $p$ premier, et $n \in \mathbb{N}$. Alors $n^p \equiv n \mod p$. Si $\mathrm{pgcd}(n, p) = 1$, alors $n^{p-1} \equiv 1 \mod p$.

**Démonstration :** Par récurrence sur $n$. L'énoncé est trivial si $n = 0$ ou $n = 1$. On suppose donc que $n^p \equiv n \mod p$. Alors

$$(n+1)^p = 1 + \sum_{k=1}^{p-1} \binom{p}{k} n^k + n^p \equiv 1 + n^p \equiv 1 + n = n + 1 \mod p,$$

où la première équivalence découle du lemma ci-dessus, et la deuxième équivalence est l'hypothèse de récurrence.

Ainsi $n^p \equiv n \mod p$ pour tout $n \in \mathbb{N}$.

Si de plus $\mathrm{pgcd}(n, p) = 1$, alors comme $p$ divise $n^p - n = n\,(n^{p-1} - 1)$, d'après le lemme de Gauss $p$ divise $n^{p-1} - 1$, et $n^{p-1} \equiv 1 \mod p$. $\square$