

Petit théorème de Fermat : Soit n un entier.

Si p est un nombre premier ne divisant pas n , alors $n^{p-1} \equiv 1 \pmod{p}$.

Démonstration :

Pré requis : Si p est un nombre premier et n un entier, alors $n^p \equiv n \pmod{p}$.

Comme p est un nombre premier, d'après le pré requis, on peut dire que $n^p - n$ est congru à 0 modulo p . D'où p divise $n^p - n$, c'est-à-dire $n(n^{p-1} - 1)$.

Or p et n sont premiers entre eux, d'après le théorème de Gauss, p divise $(n^{p-1} - 1)$, par suite, $n^{p-1} - 1 \equiv 0 \pmod{p}$, soit $n^{p-1} \equiv 1 \pmod{p}$.