1/ Soit p un nombre premier et a un entier naturel non divisible par p .
Alors : $a^{p-1} - 1$ est divisible par p .

Preuve :
Soit $S = \{a , 2a , 3a , \dots , ka , \dots , (p-1)a \}$.
p , nombre premier, est premier avec tout entier qu'il ne divise pas exactement.
Donc p est premier avec a , noté $p \wedge a = 1$.

D'après le Théorème de Gauss : Si p , qui est premier avec a , divise le produit ka , alors p divise k , ce qui est impossible, puisque $k < p$.
En conséquence, p ne divise aucun des produits ka , qui admettent chacun un reste r_k dans la division par p .

Supposons $0 < k < k' < p$. Montrons que $k \neq k' \Rightarrow r_k \neq r_{k'}$.
$r_k = r_{k'} \Leftrightarrow ka \equiv k'a\ [p] \Leftrightarrow (k-k')a \equiv 0[p]$. Donc p divise exactement le produit $(k-k')a$.
Le Théorème de Gauss affirme à nouveau que p divise $k'-k$, ce qui est impossible car $0 < k'-k < p$.
En conséquence, les $p-1$ restes r_k sont tous différents entre eux, et étant non nuls, on retrouve tous les entiers de 1 à $p-1$, soit : $r_1.r_2.r_3 \dots r_k \dots r_{p-1} = 1.2.3 \dots .k \dots (p-1) = (p-1)!$.

$a.2a.3a \dots ka \dots (p-1)a \equiv r_1.r_2.r_3 \dots r_k \dots r_{p-1}\ [p] \Rightarrow a^{p-1}(p-1)! \equiv (p-1)!\ [p]$, soit $(p-1)!(a^{p-1} - 1) \equiv 0\ [p]$.

p divise exactement le produit $(p-1)!(a^{p-1} - 1)$, mais étant premier avec chacun des facteurs de $(p-1)!$, il est premier avec ce produit, ce qui prouve que p divise exactement $a^{p-1} - 1$.

2/ Soit p un nombre premier.
Pour tout entier naturel a : $a^p - a$ est divisible par p .

Preuve :

- Si p divise a , il divise a^p , donc également $a^p - a$.
- Si p ne divise pas a , le théorème précédent affirme : $a^{p-1} - 1 \equiv 0\ [p]$, donc en multipliant les deux membres par a : $a^p - a \equiv 0\ [p]$.