Petit théorème de Fermat :

Soit p un nombre premier ; pour tout $a \in \mathbb{Z}$, on a : $a^p \equiv a \,[p]$.

Lemme : Soit p un nombre premier ; pour tout entier $0 < k < p$; on a : $\binom{p}{k} \equiv 0 \,[p]$.

Preuve : $\binom{p}{k} = \dfrac{p!}{(p-k)!\,k!}$ est un entier ;

$$p! = \binom{p}{k} (p-k)!\, k!$$

$k! = 1 \times 2 \times \dots \times k$; $p > k$, p ne peut diviser ni diviser ni 1, ni 2, ... ni k ;

p ne divise donc pas $k!$.

Idem pour $(p-k)!$; on conclut que :

$p \mid p!$, donc $p \mid \binom{p}{k} (p-k)!\, k!$

D'après le corollaire du lemme de Gauss ;

$p \mid \binom{p}{k}$.

preuve du th :

Supposons que a ∈ ℕ ; on fait une récurrence sur a.

On suppose donc : $a^p \equiv a \ [p]$.

si $a = 0$; la propriété est vérifiée.

Supposons qu'elle est vraie au rang a ;

On : $(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \dots + \binom{p}{p-1} a + 1$

D'après le lemme :

$$(a+1)^p \equiv a^p + 1 \ [p]$$
$$\equiv a + 1 \ [p]$$

↓ hypothèse de récurrence

Il nous reste donc à étudier le cas $a < 0$

On a : $(-1)^p a^p = (-a)^p \equiv -a \ [p]$

si $p \neq 2$; $(-1)^p = -1$, d'où $-a^p \equiv -a \ [p]$

ou encore : $a^p \equiv a \ [p]$

si $p = 2$; on obtient $a^p \equiv -a \ [p]$

or : $-1 \equiv 1 \ [p]$; ce qui donne le résultat.

Application :

Corollaire : Soit p un nombre premier : pour tout entier a ~~non nul~~ non multiple de p, on a :

$$a^{p-1} \equiv 1 \ [p].$$

Preuve : On a : $a^p \equiv a \ [p]$ (th).

On écrit : $a^p - a = a(a^{p-1} - 1)$:

p divise $a^{p-1} - a = a(a^{p-1} - 1)$:

(p, a) sont premiers entre eux, donc

$p \mid a^{p-1} - 1$.

Applications : ① reste de la division euclidienne de 666^{999} par 13 :

$666 = 13 \times 51 + 3 \equiv 3 \ [13]$.

$(666)^{999} \equiv 3^{999} \ [13]$.

or $3^{12} \equiv 1 \ [13]$

$999 = 12 \times 83 + 3$.

$3^{999} = 3^{12 \times 83 + 3} = (3^{12})^{83} \times 3^3 \equiv 3^3 \ [13]$

$\equiv 27 \equiv 1 \ [13]$

$(3 \mid$

(2) $26 \mid a^{13} - a$ pour tout entier a.

$a^{13} - a \equiv 0 \ [13]$.

$a^2 \equiv a \ [2] \Rightarrow a^{13} \equiv a \ [2]$.

$2 \mid a^{13} - a$ et $13 \mid a^{13} - a$.

$(2, 13) = 1 \Rightarrow 2 \times 13 = 26 \mid a^{13} - a$.

(3) $7 \mid 3^{6n} - 1$, pour tout entier $n \geq 0$

$3^{6n} - 1 = (3^6)^n - 1$ or $3^6 \equiv 1 \ [7]$.

$3^{6n} - 1 \equiv 1^n - 1 \equiv 0 \ [7]$.

(4) $30 \mid n^5 - n$;

(5) Le nombre 561, $561 = 3 \times 11 \times 17$

Soit a un entier ~~non divisible par~~ premier avec 561 donc a n'est pas un multiple ni de 3, ni de 11, ni de 17.

$a^{560} \equiv 1 \ [3]$. ($a^2 \equiv 1 \ [3]$

$a^{560} \equiv 1 \ [11]$ (car $a^{10} \equiv 1 \ [11]$)

$a^{560} \equiv 1 \ [17]$ car $a^{16} \equiv 1 \ [17]$ et $560 = 16 \times 35$)

· on conclut que : $3 \mid a^{560} - 1$,

$11 \mid a^{560} - 1$

$17 \mid a^{560} - 1$

ce qui donne : $561 = 3 \times 11 \times 17 \mid a^{560} - 1$.

ou encore : $a^{560} - 1 \equiv 0 [561)$ ou.

$a^{561} - a \equiv 0 [561]$.

561 est vérifié ~~a vérifié~~ ça n'est pas premier, et vérifie $a^{561} - a \equiv 0 [56$

pas de réciproque du théorème de Fermat.