Petit théorème de Fermat

Petit théorème de Fermat.

Soit p un nombre premier. Tout $a \in \mathbb{N}$ vérifie l'égalité : $a^p \equiv a(p)$ (p divise $(a^p - a)$).

Ce théorème peut aussi s'énoncer sous la forme.

Théorème bis, appelé aussi petit théorème de Fermat.

Soit p un nombre premier. Tout $a \in \mathbb{N}$ et non multiple de p vérifie l'égalité : $a^{p-1} \equiv 1(p)$ (p divise $(a^{p-1} - 1)$).

Démonstration de l'équivalence de ces deux théorèmes.

Le théorème bis implique le petit théorème de Fermat.

Si a est un multiple de p alors $a \equiv 0(p)$ et $a^p \equiv 0(p) \equiv a(p)$.
Si a n'est pas un multiple de p alors $a^{p-1} \equiv 1(p)$ et $a^p \equiv a(p)$.

Le petit théorème de Fermat implique le théorème bis.

$a^p \equiv a(p)$ ou p divise $(a^p - a) = a(a^{p-1} - 1)$. a n'est pas un multiple de p, p est premier donc a est premier avec p. D'après le théorème de Gauss p divise $(a^{p-1} - 1)$

Démonstration du théorème bis.

Soit E l'ensemble $\{a(p), 2a(p), 3a(p), \ldots, (p-1)a(p)\} = \{na(p),\ 1 \leqslant n \leqslant p-1\}$

$na \neq 0(p)$

On raisonne par l'absurde. On suppose que $na \equiv 0(p)$ ou p divise na.
a n'est pas un multiple de p, p est premier donc a est premier avec p. Si p divise na, d'après le théorème de Gauss p divise n. $1 \leqslant n \leqslant p-1$ donc c'est impossible.

Les p-1 éléments de E ne sont pas congrus modulo p.

On suppose que $na \equiv ma(p)$.
On peut toujours choisir $n \geqslant m$ donc $(n-m)a \equiv 0(p)$ avec $0 \leqslant n-m$.
$1 \leqslant n \leqslant p-1$ et $1 \leqslant m \leqslant p-1$ donc $n-m \leqslant p-1$
Comme dans la démonstration précédente on en déduit que p divise n-m.
$0 \leqslant n-m \leqslant p-1$ donc $n-m=0$.
$na \equiv ma(p) \Rightarrow n=m$ donc $n \neq m \Rightarrow na \neq ma(p)$.

$E = \{1(p), 2(p), \ldots, (p-1)(p)\}$.

On rappelle que $b \equiv r(p)$ avec $0 \leqslant r < p$ signifie que r est le reste dans la division euclidienne b par p.
Soit r_n le reste de la division euclidienne de na par p alors :

$$E = \{r_1(p), r_2(p), \ldots, r_{p-1}(p),\ 1 \leqslant r_i \leqslant p-1\}$$

Les p-1 restes sont distincts, non nuls et inférieurs à p-1 donc il prennent toutes les valeurs de 1 à p-1.

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

$E=\{a(p), 2a(p), 3a(p), ..., (p-1)a(p)\}=\{1(p), 2(p), ..., (p-1)(p)\}$

Effectuons le produit de tous les éléments de *E*.

$$\underbrace{a\times 2a\times 3a\times ...\times (p-1)a}_{p-1 \text{ facteurs}} \equiv \underbrace{1\times 2\times 3\times ...\times (p-1)}_{p-1 \text{ facteurs modulo } p}(p)$$

$$a^{p-1}\times (p-1)!=(p-1)!\ \underbrace{(p)}_{\text{modulo } p}$$

p divise $(a^{p-1}-1)(p-1)!$ et p est premier avec 1, 2, ... , (p-1) d'après le théorème de Gauss, p divise $(a^{p-1}-1)$, $a^{p-1}=1(p)$.

Démonstration directe du petit théorème de Fermat.

Si p premier alors pour tout k, $1\leqslant k\leqslant p-1$, $\binom{p}{k}$ ***est divisible par p.***

$\binom{p}{k}=\frac{p(p-1)(p-2)...(p-k+1)}{k(k-1)...2}=\frac{pq}{k(k-1)...2}=n\in\mathbb{N}$. donc

$pq=(k(k-1)...2)n=k!n$

p est premier donc il est premier avec tout nombre non nul et strictement inférieur à lui-même.

k divise pq et k est premier avec p donc k divise q, $q=kq_k$ et $pq_k k=k(k-1)...2$ donc $pq_k=(k-1)...2$

De même $(k-1)$ divise q_k donc $pq_{k-1}=(k-2)...2$ et $k(k-1)$*divise* q.

On répète ce raisonnement jusqu'à 2 et donc $k!$ divise q.

En simplifiant par $k!$ on obtient $pq'=n$

Si p est premier $(b+c)^p\equiv(b^p+c^p)(p)$

Pour $1\leqslant k\leqslant p-1$, $\binom{p}{k}$ est divisible par p donc $\binom{p}{k}=0(p)$

$$(a+b)^p\equiv\left(\binom{p}{p}b^p+\binom{p}{p-1}b^{p-1}c+\binom{p}{p-2}b^{p-2}c^2+...+\binom{p}{1}bc^{p-1}+\binom{p}{0}c^p\right)(p)$$

Pour $1\leqslant k\leqslant p-1$, $\binom{p}{k}$ est divisible par p donc $\binom{p}{k}=0(p)$ donc tous les termes sauf le premier et le dernier sont nuls.

$$(a+b)^p=\left(\binom{p}{p}b^p+\binom{p}{0}c^p\right)(p)=(a^p+b^p)(p).$$

Démonstration par récurrence du petit théorème de Fermat.

Soit p un nombre premier et $P(a)$ la propriété : $a^p=a(p)$

Initialisation.

$0^p=0\equiv 0(p)$, $P(0)$ est vraie

Hérédité.

On suppose $P(a)$ vraie.

$(a+1)^p \equiv (a^p+1)(p)$, en appliquant $P(a)$ on obtient $(a+1)^p \equiv (a+1)(p)$.

$P(a+1)$ est vraie.

Conclusion.

Pour tout $a \in \mathbb{N}$, $P(a)$ est vraie.