Petit théorème de Fermat
Si p est un entier naturel premier et a un autre entier naturel premier avec p alors :
$a^{p-1}-1$ est divisible par p autrement dit $a^{p-1}\equiv 1$ modulo p

Conséquence : si p est un entier premier et si $\text{PGCD}(a;p)=1$ alors $a^p \equiv a$ modulo p .
D'après ce qui précède, nous pouvons affirmer que :

$8^6 \equiv 1$ modulo 7 $\qquad$ $10^{11} \equiv 10$ modulo 11

La preuve de ce théorème

Cette démonstration comporte plusieurs phases.

❶ p divise-t-il les $p-1$ premiers multiples de a que sont $a;2.a;3.a;\ldots;(p-1).a$?

Procédons par l'absurde et supposons que p divise l'un de ces multiples k.a .
Comme p est premier avec le second facteur a alors en application du théorème de Gauss, p divise nécessairement k.
Or k est un entier naturel compris entre 1 et $p-1$. Il est donc inférieur strictement à p et ce dernier ne peut donc pas le diviser.
Notre supposition nous amène à une contradiction avec ce que nous savons vrai. Elle était donc erronée.
Conclusion : l'entier premier p ne divise aucun des multiples $a;2.a;3.a;\ldots;(p-1).a$.

❷ Les restes des divisions euclidiennes par p des multiples $a;2.a;3.a;\ldots;(p-1).a$.

L'entier premier p ne divisant pas les $p-1$ premiers multiples de a, les restes des divisions euclidiennes de chacun d'eux par p sont non nuls.
Pour fixer les idées, appelons r_k le reste de la division euclidienne du multiple k.a par p.
Chacun de ces restes r_k est tel que $\underbrace{0<r_k<p}_{\text{Non nul car p ne divise pas k.a et strictement inférieur au diviseur p}}$

❸ Deux de ces restes r_k et r_n peuvent-ils être égaux ?
Procédons par l'absurde. Supposons qu'il existe deux entiers distincts k et n compris entre 1 et $p-1$ tels que $r_k = r_n$.
Quand on travaille avec deux entiers distincts, l'un est nécessairement plus grand que l'autre. Pour fixer les idées, disons que $k<n$.
Si q_k et q_n désignent les quotients des divisions euclidiennes des multiples k.a et n.a par p alors nous avons : $\begin{cases} k.a = q_k.p + r_k \quad \text{d'où} \quad r_k = k.a - q_k.p \\ n.a = q_n.p + r_n \quad \text{d'où} \quad r_n = n.a - q_n.p \end{cases}$.

Les deux restes r_k et r_n étant égaux, il vient alors :

$$k.a - q_k.p = n.a - q_n.p \Leftrightarrow p.(q_k - q_n) = a.(n-k)$$

Donc p divise le produit $a.(n-k)$. Mais comment il est premier avec a alors en application du théorème de Gauss, il divise nécessairement le facteur $n-k$.
Or cette différence $n-k$ est comprise entre 1 et $p-1$ car nous avons $1 \le k < n \le p-1$.
Donc p ne peut diviser cette différence $n-k$.
Supposer que deux restes r_k et r_n peuvent être égaux nous a amené à une contradiction.
Conclusion : les $p-1$ restes r_k sont tous distincts deux à deux. Ils prennent tous des valeurs différentes. Comme les $p-1$ restes r_k sont tous compris entre $\underbrace{1 \text{ et } p-1}_{p-1 \text{ valeurs possibles}}$,
alors chacun des $p-1$ entiers $1;2;3;\ldots;p-1$ est le reste d'une seule division euclidienne d'un des $p-1$ premiers multiples de a par p. Et réciproquement !
Autrement dit : un entier = Un reste.

❹ La dernière carte.
Chacun des $p-1$ multiples k.a est congru modulo p à son reste r_k .
Justement intéressons-nous au produit de ces $p-1$ premiers multiples de a.

$$1.a \times 2.a \times \ldots \times (p-1).a = 1 \times 2 \times \ldots \times (p-1) \times a^{p-1}$$

Or chaque multiple k.a est congru à son reste r_k modulo p. Il vient alors :

$$1.a \times 2.a \times \ldots \times (p-1).a \equiv \underbrace{r_1 \times r_2 \times \ldots \times r_{p-1}}_{\substack{\text{Chacun est égal à l'un} \\ \text{des p–1 entiers 1;2;…;p–1}}} \text{ modulo } p = 1 \times 2 \times \ldots \times (p-1) \text{ modulo p}$$

Donc la différence $\underbrace{1 \times 2 \times \ldots \times (p-1)}_{\text{Facteurs...}} \times a^{p-1} - \underbrace{1 \times 2 \times \ldots \times (p-1)}_{\text{...communs}}$ est congrue à 0 modulo p.

Autrement dit, l'entier p divise le produit $1 \times 2 \times \ldots \times (p-1).\left[a^{p-1}-1\right]$.

Comme p est un nombre premier alors il est premier avec chacun des entiers $1;2;\ldots;p-1$.

En application du théorème de Gauss, il ne peut donc diviser que le facteur $a^{p-1}-1$.
D'où le théorème.

Précision : tout entier naturel premier p est premier avec tous ceux qui le précèdent.
Si un entier naturel p est premier alors ses seuls diviseurs dans $\mathbb{N}$ sont 1 et lui-même.
Soit n un entier naturel compris entre 1 et $p-1$ c'est-à-dire strictement inférieur à p.
On pose $\delta = \text{PGCD}(p;n)$. L'entier naturel δ est un diviseur commun de p et n dans $\mathbb{N}$.
Comme δ est un diviseur de p alors il est soit égal à 1, soit égal à p.
Comme δ est un diviseur de n alors $\delta \le n < p$.
Conclusion : le PGCD δ ne peut être égal qu'à 1. Tout entier premier est premier avec tous les entiers naturels non nuls $1;2;\ldots;p-1$ qui le précèdent.