# Maths Expertes
## Terminale

# Nombres Premiers

## CORRIGÉ DE L'EXERCICE

# Petit théorème de Fermat

02

## Correction

NB. Enoncé du petit théorème de Fermat : Si *P* est un nombre premier et si *a* est un entier non divisible par *P*, alors $a^{P-1} \equiv 1 \ [P]$.

Rappelons aussi que sont équivalentes les formulations :

- *a* est multiple de *b*.
- *a* est divisible par *b*.
- $a \equiv 0 \ [b]$.

**1. Montrons que $4^{28} - 1$ est divisible par 29 :**

- 29 est un nombre premier.
- Le nombre entier naturel 4 n'est pas divisible par 29.

Nous pouvons appliquer le petit théorème de Fermat avec $P = 29$ ; $a = 4$ ; $P - 1 = 28$.

D'après le petit théorème de Fermat : $4^{28} \equiv 1 \ [29]$.

Il en résulte la congruence $4^{28} - 1 \equiv 0 \ [29]$, donc le nombre $4^{28} - 1$ est divisible par 29.

**2. Montrons que pour tout entier naturel *n*, $4^n - 1$ est divisible par 3 :**

De la division euclidienne $4 = 1 \times 3 + 1$, nous déduisons la congruence $4 \equiv 1 \ [3]$.

Pour tout entier naturel *n*, nous obtenons une nouvelle congruence modulo 3 en élevant chaque membre de cette congruence à la puissance *n* : $4^n \equiv 1^n \ [3]$.

Or, 1 est invariant par élévation à une puissance. Nous obtenons : $4^n \equiv 1 \ [3]$ soit, aussi bien :

$4^n - 1 \equiv 0 \ [3]$. Pour tout entier naturel *n*, $4^n - 1$ est divisible par 3.

**3. Montrons que pour tout entier naturel *k*, $4^{4k}-1$ est divisible par 5 et par 17 :**

Soit *k* un entier naturel.

**Montrons la divisibilité de $4^{4k}-1$ par 5 :**

Compte tenu des règles d'opérations sur les puissances : $4^{4k}=\left(4^k\right)^4$.

- 5 est un nombre premier.
- Le nombre entier naturel $4^k$ n'est pas divisible par le nombre premier 5 puisque 4 ne l'est pas.

Nous pouvons appliquer le petit théorème de Fermat avec $P=5$ ; $a=4^k$ ; $P-1=4$.

D'après le petit théorème de Fermat : $\left(4^k\right)^4 \equiv 1\ [5]$.

Il en résulte la congruence $4^{4k}-1 \equiv 0\ [5]$, le nombre $4^{4k}-1$ est divisible par 5.

**Montrons la divisibilité de $4^{4k}-1$ par 17 :**

17 est un nombre premier et son prédécesseur est 16, nous pouvons penser à une nouvelle application du petit théorème de Fermat, mais le nombre $4^{4k}$ n'apparaît pas comme étant la puissance seizième d'un entier. Les conditions d'application du théorème ne semblent pas être facilement réunies. Procédons autrement …

Effectuons la division euclidienne de $4^4=256$ par 17 : $256=15\times 17+1$. Le reste de cette division euclidienne est égal à 1, nous en déduisons la congruence : $4^4 \equiv 1\ [17]$ .

Elevons à la puissance *k* chaque membre de cette congruence : $(4^4)^k \equiv 1^k\ [17]$.

Or, 1 est invariant par élévation à une puissance. Nous obtenons : $(4^4)^k \equiv 1\ [17]$ soit, aussi bien :

$4^{4k}-1 \equiv 0\ [17]$, donc pour tout entier naturel *k*, $4^{4k}-1$ est divisible par 17.

**4. Déduisons-en quatre diviseurs de $4^{28}-1$ :**

Les questions 1 et 2 montrent explicitement que $4^{28}-1$ est divisible par 29 et par 3. D'autre part : $28=4\times 7$. Nous pouvons appliquer les résultats de la question 3 avec $k=7$. Le nombre $4^{28}-1$ est divisible par 5 et par 17.

3, 5, 17 et 29 sont quatre diviseurs de $4^{28}-1$.

NB. Ce que nous constatons en lisant la factorisation aimablement fournie par notre calculatrice.

$$\text{factor}\left(4^{28}-1\right)$$
$$3\cdot 5\cdot 17\cdot 29\cdot 43\cdot 113\cdot 127\cdot 15790321$$