Terminale Maths expertes

Les nombres premiers

Cours

Dans tout le chapitre, les lettres désignent des **entiers**, relatifs ou naturels selon le contexte, et la lettre p désigne un nombre premier.

Remarques : rappels utilisés dans ce chapitre

- **Bon ordre :** toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- **Transitivité :** si a divise b et b divise c, alors a divise c.
- **Théorème de Gauss :** si a divise bc et $\text{PGCD}(a\,;b) = 1$, alors a divise c. **Corollaire :** si a et b divisent c et $\text{PGCD}(a\,;b) = 1$, alors ab divise c.
- **Congruences :** on peut multiplier membre à membre des congruences de même module et les élever à une puissance entière.

I. Nombres premiers

1. Définition

Définition 1 : nombre premier

Un entier naturel n est **premier** s'il admet **exactement deux** diviseurs positifs distincts : 1 et lui-même.
Un entier naturel $n \geqslant 2$ qui n'est pas premier est dit **composé** : il s'écrit $n = ab$ avec $2 \leqslant a \leqslant n-1$ et $2 \leqslant b \leqslant n-1$.

Exemples :

- 0 n'est pas premier : tout entier naturel divise 0, il a donc une infinité de diviseurs.
- 1 n'est pas premier : il n'a qu'un seul diviseur positif, lui-même.
- 2 est premier, et c'est le **seul nombre premier pair** : un nombre pair $n > 2$ admet le diviseur 2, différent de 1 et de n.
- 17 est premier ; $27 = 3 \times 9$ n'est pas premier.
- Les nombres premiers inférieurs à 50 sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

2. Le plus petit diviseur d'un entier

Propriété 1 : plus petit diviseur

Soit n un entier naturel tel que $n \geqslant 2$.

a. Le plus petit diviseur $p \geqslant 2$ de n est un nombre premier. En particulier, **tout entier $n \geqslant 2$ admet au moins un diviseur premier**.

b. Si n n'est pas premier, ce plus petit diviseur premier vérifie

$$p^2 \leqslant n, \qquad \text{c'est-à-dire} \qquad p \leqslant \sqrt{n}.$$

Démonstration

a. Soit E l'ensemble des diviseurs d de n tels que $d \geqslant 2$. Il n'est pas vide, puisqu'il contient n. D'après le bon ordre, il admet un plus petit élément, noté p.
Supposons que p ne soit pas premier. Comme $p \geqslant 2$, il admet alors un diviseur q avec $2 \leqslant q \leqslant p-1$. q divise p et p divise n : par transitivité, q divise n. Donc $q \in E$, alors que $q < p$: c'est impossible, puisque p est le plus petit élément de E.
Donc p est premier.

b. n n'est pas premier, donc $p \neq n$. On écrit $n = p\,q$ avec $q = \dfrac{n}{p}$ entier et $q \geqslant 2$.
q est un diviseur de n supérieur ou égal à 2 : $q \in E$, donc $q \geqslant p$ puisque p est le plus petit élément de E. Par conséquent :

$$n = p \times q \geqslant p \times p = p^2, \qquad \text{d'où} \qquad p \leqslant \sqrt{n}.$$

Propriété 2 : test de primalité

Soit $n \geqslant 2$. Si n n'est divisible par aucun nombre premier p tel que $p^2 \leqslant n$, alors n est premier.

Démonstration

C'est la contraposée de la propriété 1 b. : si n n'était pas premier, son plus petit diviseur premier p vérifierait $p^2 \leqslant n$, et n serait divisible par ce nombre premier.

Méthode 1 : montrer qu'un entier est premier, ou ne l'est pas

Énoncé. Les entiers 287 et 467 sont-ils premiers ?

Solution. Pour 287 **:** on teste les nombres premiers dans l'ordre : 287 n'est divisible ni par 2, ni par 3, ni par 5, mais $287 = 7 \times 41$. Il n'est pas premier.

Pour 467 **:** $21^2 = 441 \leqslant 467 < 484 = 22^2$, donc il suffit de tester les nombres premiers inférieurs ou égaux à 21.

p	2	3	5	7	11	13	17	19
reste de 467 par p	1	2	2	5	5	12	8	11

Aucun reste n'est nul : d'après la propriété 2, **467 est premier**.

Exercice d'application 1 : premier ou composé ?

a. Jusqu'à quel nombre premier faut-il tester les divisions pour savoir si 401 est premier ? Justifier.

.....

.....

b. Les entiers 391, 401 et 2 027 sont-ils premiers ?

.....

.....

.....

.....

c. Soit $n \geqslant 2$ un entier. Factoriser $n^2 + 2n - 3$, puis déterminer les entiers n pour lesquels $n^2 + 2n - 3$ est un nombre premier.

.....

.....

.....

.....

3. Une infinité de nombres premiers

Théorème 1 : infinité des nombres premiers

L'ensemble des nombres premiers est infini : il n'existe pas de plus grand nombre premier.

Démonstration

On raisonne **par l'absurde** : on suppose qu'il n'y a qu'un nombre fini de nombres premiers, et on les note $p_1, p_2, \ldots, p_k$.

On construit un entier. On pose

$$N = p_1 \times p_2 \times \cdots \times p_k + 1.$$

Comme $N \geqslant 2 + 1 = 3$, d'après la propriété 1, N admet un diviseur premier, que l'on note d.

d **divise le produit.** Par hypothèse, $p_1, \ldots, p_k$ sont **tous** les nombres premiers : d est donc l'un d'eux, et il divise le produit $P = p_1 \times p_2 \times \cdots \times p_k$.

Contradiction. d divise N et P, donc il divise leur différence $N - P = 1$. Ainsi $d = 1$, ce qui est impossible puisque d est premier.

L'hypothèse de départ est fausse : il existe une infinité de nombres premiers.

Attention : N n'est pas forcément premier

La démonstration utilise seulement que N a un diviseur premier qui n'est pas dans la liste. Par exemple,

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031 = 59 \times 509$$

n'est pas premier, mais ses diviseurs premiers 59 et 509 ne figurent pas parmi 2, 3, 5, 7, 11, 13.

4. Nombres premiers et divisibilité

Propriété 3 : premier avec un entier

Soit p un nombre premier et a un entier. Alors **ou bien p divise a, ou bien p et a sont premiers entre eux**.

Démonstration

PGCD$(p\,;a)$ est un diviseur positif de p : il vaut donc 1 ou p.
• S'il vaut p, alors p divise a. • S'il vaut 1, alors p et a sont premiers entre eux.

Propriété 4 : lemme d'Euclide

Soit p un nombre premier et a, b deux entiers.

Si p divise ab, alors p divise a ou p divise b.

Plus généralement, si p divise un produit $a_1a_2\cdots a_k$, alors p divise l'un des facteurs a_i. En particulier, si p divise un produit de nombres premiers $q_1q_2\cdots q_k$, alors p est égal à l'un des q_i.

Démonstration

Deux facteurs. Supposons que p divise ab et que p ne divise pas a. D'après la propriété 3, PGCD$(p\,;a) = 1$. Comme p divise ab, le théorème de Gauss donne : p divise b.

Plusieurs facteurs. On écrit $a_1a_2\cdots a_k = a_1 \times (a_2\cdots a_k)$: p divise a_1 ou p divise $a_2\cdots a_k$; dans le second cas, on recommence avec $a_2 \times (a_3\cdots a_k)$, et ainsi de suite (récurrence sur k).

Produit de nombres premiers. Si p divise $q_1\cdots q_k$, il divise l'un des q_i. Les seuls diviseurs positifs de q_i sont 1 et q_i, et $p \neq 1$: donc $p = q_i$.

Attention

L'hypothèse « p premier » est indispensable : 6 divise $4 \times 9 = 36$, mais 6 ne divise ni 4 ni 9.

II. Décomposition en produit de facteurs premiers

1. Le théorème fondamental

Théorème 2 : décomposition en facteurs premiers

Tout entier naturel $n \geqslant 2$ s'écrit comme un produit de nombres premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r},$$

où $p_1 < p_2 < \cdots < p_r$ sont des nombres premiers et $\alpha_1, \ldots, \alpha_r$ des entiers naturels non nuls.
Cette décomposition est **unique** (à l'ordre des facteurs près).

Exemple

On peut décomposer 300 de plusieurs façons : $300 = 2 \times 150 = 2 \times 2 \times 75 = 2 \times 2 \times 3 \times 5 \times 5$, ou $300 = 10 \times 30 = 2 \times 5 \times 2 \times 3 \times 5$.
On aboutit toujours à la même décomposition : $300 = 2^2 \times 3 \times 5^2$.

Démonstration : existence

Si n est premier, il est sa propre décomposition : $n = n^1$.
Sinon, on divise n par son plus petit diviseur premier q_1 (propriété 1) : $n = q_1 n_1$, avec $2 \leqslant n_1 < n$.
Si n_1 est premier, on s'arrête ; sinon, on divise n_1 par son plus petit diviseur premier q_2 : $n_1 = q_2 n_2$, avec $2 \leqslant n_2 < n_1$, et ainsi de suite.

Les quotients $n > n_1 > n_2 > \cdots \geqslant 2$ forment une suite d'entiers strictement décroissante : elle ne peut pas être infinie. Le dernier quotient n_k est donc premier, et

$$n = q_1 \times q_2 \times \cdots \times q_k \times n_k$$

est un produit de nombres premiers. En regroupant les facteurs égaux, on obtient l'écriture $p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$.

Démonstration : unicité

Supposons que n s'écrive de deux façons comme produit de nombres premiers (écrits avec répétitions) :

$$n = q_1 \times q_2 \times \cdots \times q_k = s_1 \times s_2 \times \cdots \times s_l.$$

q_1 divise $n = s_1 \times \cdots \times s_l$: d'après le lemme d'Euclide, q_1 est égal à l'un des s_j. On simplifie les deux membres par ce facteur commun : on obtient deux écritures d'un même entier plus petit, chacune avec un facteur de moins.
En répétant ce raisonnement, on élimine les facteurs un à un : ceux de la première écriture se retrouvent tous dans la seconde, et réciproquement. Les deux écritures comportent donc les mêmes nombres premiers, chacun répété le même nombre de fois : les exposants sont les mêmes.

Méthode 2 : décomposer un entier

Énoncé. Décomposer 2 940 en produit de facteurs premiers.

Solution. On divise successivement par les nombres premiers 2, 3, 5, 7… tant que c'est possible :

2 940	2
1 470	2
735	3
245	5
49	7
7	7
1	

On lit les diviseurs dans la colonne de droite :

$$2\,940 = 2^2 \times 3 \times 5 \times 7^2.$$

On vérifie : $4 \times 3 \times 5 \times 49 = 2\,940$.

Astuce : on s'arrête dès que le quotient restant est premier ; pour le savoir, on utilise la propriété 2.

Exercice d'application 2 : décomposer

a. Décomposer en produit de facteurs premiers : 240, 1 386 et 2 025.

……

……

……

……

b. Décomposer 7 056. En déduire que 7 056 est le carré d'un entier que l'on précisera.

……

……

……

2. Les diviseurs d'un entier

Propriété 5 : diviseurs et nombre de diviseurs

Soit $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$ la décomposition en facteurs premiers d'un entier $n \geqslant 2$.
Les diviseurs positifs de n sont les entiers

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_r^{\beta_r} \qquad \text{avec} \qquad 0 \leqslant \beta_i \leqslant \alpha_i \text{ pour tout } i.$$

L'entier n a donc exactement $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$ diviseurs positifs.

Démonstration

Ces entiers sont des diviseurs. Si $0 \leqslant \beta_i \leqslant \alpha_i$, alors $n = d \times p_1^{\alpha_1-\beta_1} \times \cdots \times p_r^{\alpha_r-\beta_r}$, avec des exposants positifs ou nuls : d divise n.

Tout diviseur est de cette forme. Soit d un diviseur positif de n : $n = dk$. Tout nombre premier qui divise d divise n, donc, d'après le lemme d'Euclide, c'est l'un des p_i ; il en est de même pour k. On peut donc écrire $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$ et $k = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ avec des exposants positifs ou nuls. Alors

$$n = dk = p_1^{\beta_1+\gamma_1} \times \cdots \times p_r^{\beta_r+\gamma_r},$$

et par unicité de la décomposition, $\beta_i + \gamma_i = \alpha_i$: donc $\beta_i \leqslant \alpha_i$.

Dénombrement. Pour chaque i, l'exposant β_i peut prendre les $\alpha_i + 1$ valeurs $0, 1, \ldots, \alpha_i$, indépendamment des autres. Deux choix différents donnent deux diviseurs différents (unicité de la décomposition). Il y a donc $(\alpha_1+1) \times \cdots \times (\alpha_r+1)$ diviseurs.

Exemple : les diviseurs de $12 = 2^2 \times 3$

Un diviseur s'écrit $2^{\beta_1} \times 3^{\beta_2}$ avec $0 \leqslant \beta_1 \leqslant 2$ et $0 \leqslant \beta_2 \leqslant 1$. On les range dans un tableau : il y en a $(2+1) \times (1+1) = 6$.

$\times$	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$
$3^0 = 1$	1	2	4
$3^1 = 3$	3	6	12

Méthode 3 : compter des diviseurs

Énoncé. a. Combien 240 a-t-il de diviseurs positifs ? **b.** Quels sont les entiers qui ont exactement 5 diviseurs positifs ?

Solution. a. $240 = 2^4 \times 3 \times 5$: il a $(4+1)(1+1)(1+1) = 20$ diviseurs positifs.
b. Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, il faut $(\alpha_1+1)\cdots(\alpha_r+1) = 5$, avec des facteurs $\alpha_i + 1 \geqslant 2$. Comme 5 est premier, il n'y a qu'un seul facteur : $r = 1$ et $\alpha_1 + 1 = 5$.
Les entiers cherchés sont les p^4, avec p premier : 16, 81, 625, ...

Exercice d'application 3 : diviseurs d'un entier

a. Décomposer 72, puis compléter le tableau de ses diviseurs positifs. Combien en a-t-il ?

×	1	2	4	8
1				
3				
9				

.....

b. Combien 2 025 et 1 000 ont-ils de diviseurs positifs ?

.....

.....

c. Quel est le plus petit entier naturel qui a exactement 6 diviseurs positifs ?

.....

.....

.....

3. PGCD et PPCM

Définition 2 : PPCM

Soit a et b deux entiers naturels non nuls. Le **plus petit commun multiple** de a et b est le plus petit entier strictement positif qui est à la fois multiple de a et de b ; on le note $\text{PPCM}(a\,;b)$.
Il existe, car ab est un multiple commun strictement positif (bon ordre).

Propriété 6 : PGCD et PPCM par la décomposition

Soit a et b deux entiers naturels non nuls, décomposés avec les mêmes nombres premiers $p_1, \dots, p_r$ (certains exposants pouvant être nuls) :

$$a = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r} \qquad \text{et} \qquad b = p_1^{\beta_1} \times \cdots \times p_r^{\beta_r}.$$

a. $\text{PGCD}(a\,;b) = p_1^{\min(\alpha_1,\beta_1)} \times \cdots \times p_r^{\min(\alpha_r,\beta_r)}$: les facteurs premiers **communs**, avec le **plus petit** exposant.

b. $\text{PPCM}(a\,;b) = p_1^{\max(\alpha_1,\beta_1)} \times \cdots \times p_r^{\max(\alpha_r,\beta_r)}$: **tous** les facteurs premiers, avec le **plus grand** exposant.

c. $\text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) = a \times b$.

Démonstration

a. D'après la propriété 5, un diviseur positif commun s'écrit $p_1^{\delta_1} \cdots p_r^{\delta_r}$ avec $\delta_i \leqslant \alpha_i$ et $\delta_i \leqslant \beta_i$, c'est-à-dire $\delta_i \leqslant \min(\alpha_i, \beta_i)$. Le plus grand s'obtient en prenant chaque exposant maximal : $\delta_i = \min(\alpha_i, \beta_i)$.

b. Un multiple commun $m > 0$ est divisible par a et par b : d'après la propriété 5, dans sa décomposition, l'exposant de chaque p_i est au moins α_i et au moins β_i, donc au moins $\max(\alpha_i, \beta_i)$. Le plus petit s'obtient avec ces exposants exactement, et sans autre facteur premier.

c. Pour tous réels x et y : $\min(x, y) + \max(x, y) = x + y$. En multipliant les deux décompositions, l'exposant de p_i dans PGCD × PPCM est $\alpha_i + \beta_i$, comme dans $a \times b$.

Exemple : $a = 27\,216$ et $b = 60$

$27\,216 = 2^4 \times 3^5 \times 7$ et $60 = 2^2 \times 3 \times 5$. On complète avec des exposants nuls : $a = 2^4 \times 3^5 \times 5^0 \times 7^1$ et $b = 2^2 \times 3^1 \times 5^1 \times 7^0$.

$$\text{PGCD}(a\,;b) = 2^2 \times 3 = 12 \qquad \text{et} \qquad \text{PPCM}(a\,;b) = 2^4 \times 3^5 \times 5 \times 7 = 136\,080.$$

Vérification : $12 \times 136\,080 = 1\,632\,960 = 27\,216 \times 60$.

Exercice d'application 4 : PGCD et PPCM

a. Décomposer 360 et 756 en produit de facteurs premiers.

.....

.....

b. En déduire $\text{PGCD}(360\,;756)$ et $\text{PPCM}(360\,;756)$.

.....

.....

c. Vérifier la relation $\text{PGCD} \times \text{PPCM} = a \times b$.

.....

.....

III. Le petit théorème de Fermat

1. Le théorème

Théorème 3 : petit théorème de Fermat

Soit p un nombre premier et a un entier **non divisible par p**. Alors

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

Exemple

5 est premier et ne divise pas 12 : donc $12^4 \equiv 1\ [5]$. En effet, $12^4 = 20\,736 = 5 \times 4\,147 + 1$.

Démonstration

Étape 1 : les restes de a, $2a$, …, $(p-1)a$ ne sont pas nuls. Pour $1 \leqslant k \leqslant p-1$, on note r_k le reste de la division euclidienne de ka par p.
p ne divise pas k (car $1 \leqslant k < p$) et ne divise pas a : d'après le lemme d'Euclide, p ne divise pas ka. Donc $r_k \neq 0$, et $1 \leqslant r_k \leqslant p-1$.

Étape 2 : ces restes sont deux à deux distincts. Soit $1 \leqslant k < k' \leqslant p-1$. Si on avait $r_k = r_{k'}$, alors $k'a \equiv ka\ [p]$, et p diviserait $(k'-k)\,a$. Or $1 \leqslant k'-k \leqslant p-1$: p ne divise ni $k'-k$, ni a, donc (lemme d'Euclide) il ne divise pas leur produit. Contradiction : $r_k \neq r_{k'}$.

Étape 3 : les restes sont les entiers de 1 à $p-1$. $r_1, \ldots, r_{p-1}$ sont $p-1$ entiers distincts compris entre 1 et $p-1$: ce sont exactement $1, 2, \ldots, p-1$, dans un certain ordre. Donc

$$r_1 \times r_2 \times \cdots \times r_{p-1} = 1 \times 2 \times \cdots \times (p-1) = (p-1)!\,.$$

Étape 4 : on multiplie les congruences. Pour tout k, $ka \equiv r_k\ [p]$. En multipliant ces $p-1$ congruences :

$$a \times 2a \times \cdots \times (p-1)a \equiv r_1 \times \cdots \times r_{p-1}\ [p], \qquad \text{soit} \qquad (p-1)! \times a^{p-1} \equiv (p-1)!\ [p].$$

Donc p divise $(p-1)! \times \left(a^{p-1} - 1\right)$.

Étape 5 : conclusion avec Gauss. p ne divise aucun des facteurs $1, 2, \ldots, p-1$, donc (lemme d'Euclide) il ne divise pas $(p-1)!$: p et $(p-1)!$ sont premiers entre eux (propriété 3). D'après le théorème de Gauss, p divise $a^{p-1}-1$, c'est-à-dire $a^{p-1} \equiv 1\ [p]$.

Remarque : la réciproque est fausse

On peut avoir $a^{n-1} \equiv 1\ [n]$ sans que n soit premier. Par exemple $341 = 11 \times 31$ n'est pas premier, et pourtant $2^{10} = 1\,024 = 3 \times 341 + 1$, donc $2^{340} = \left(2^{10}\right)^{34} \equiv 1\ [341]$.

Méthode 4 : calculer un reste avec le petit théorème de Fermat

Énoncé. Déterminer le reste de la division euclidienne de $3^{2\,026}$ par 7.

Solution. 7 est premier et ne divise pas 3 : d'après le petit théorème de Fermat, $3^6 \equiv 1\ [7]$.
On divise l'exposant par 6 : $2\,026 = 6 \times 337 + 4$. Donc

$$3^{2\,026} = \left(3^6\right)^{337} \times 3^4 \equiv 1^{337} \times 81 \equiv 81\ [7].$$

Or $81 = 7 \times 11 + 4$: le reste cherché est 4.

2. Une conséquence

Propriété 7 : forme générale

Soit p un nombre premier. Pour tout entier a :

$$a^p \equiv a\ [p].$$

Démonstration

$a^p \equiv a\ [p] \iff p$ divise $a^p - a = a\left(a^{p-1}-1\right)$. On distingue deux cas.
• Si p divise a : p divise le produit $a\left(a^{p-1}-1\right)$.
• Si p ne divise pas a : d'après le petit théorème de Fermat, p divise $a^{p-1}-1$, donc aussi le produit.
Dans les deux cas, $a^p \equiv a\ [p]$.

Exemple

Pour tout entier n, $n^7 - n$ est divisible par 7, puisque $n^7 \equiv n\ [7]$.

Exercice d'application 5 : utiliser le petit théorème de Fermat

a. Déterminer le reste de la division euclidienne de 2^{100} par 11.

.....

.....

.....

b. Déterminer le reste de la division euclidienne de $2^{2\,027}$ par 13.

.....

.....

.....

c. Démontrer que, pour tout entier n, l'entier $n^5 - n$ est divisible par 5.

.....

.....

IV. Algorithmique

La fonction `est_premier` applique le test de la propriété 2 : on cherche un diviseur d tant que $d^2 \leqslant n$. La fonction `decomposition` reprend la méthode 2 : on divise par d tant que c'est possible, puis on passe à $d+1$.

Python

```
def est_premier(n):
    if n < 2:
        return False
    d = 2
    while d * d <= n:
        if n % d == 0:
            return False
        d = d + 1
    return True

print(est_premier(467))   # True
```

Python

```
def decomposition(n):
    facteurs = []
    d = 2
    while n > 1:
        while n % d == 0:
            facteurs.append(d)
            n = n // d
        d = d + 1
    return facteurs

print(decomposition(2940))
# [2, 2, 3, 5, 7, 7]
```

Remarque

Dans `decomposition`, les diviseurs trouvés sont toujours premiers : quand on arrive à un entier d composé, ses facteurs premiers, plus petits que lui, ont déjà été retirés de n.

L'essentiel du chapitre

Nombre premier	Exactement deux diviseurs positifs : 1 et lui-même. 0 et 1 ne sont pas premiers ; 2 est le seul premier pair.
Test	Si $n \geqslant 2$ n'a aucun diviseur premier p tel que $p^2 \leqslant n$, alors n est premier.
Infinité	Il existe une infinité de nombres premiers.
Lemme d'Euclide	Si p premier divise ab, alors p divise a ou b.
Décomposition	$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, unique ; $(\alpha_1+1)\cdots(\alpha_r+1)$ diviseurs positifs.
PGCD, PPCM	Exposants minimum (facteurs communs), maximum (tous les facteurs) ; PGCD $\times$ PPCM $= ab$.
Fermat	Si p est premier et ne divise pas a : $a^{p-1} \equiv 1\ [p]$. Pour tout a : $a^p \equiv a\ [p]$.