Terminale Maths Expertes – Chapitre 06

NOMBRES PREMIERS

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; ....

61357004981 ?

Table des matières

I Définition et propriétés des nombres premiers

1) Définition

DÉFINITION

Soit $n \in \mathbb{N}$.
On dit que n est **premier** s'il possède **exactement** deux diviseurs distincts positifs, 1 et lui-même.

EXEMPLES

- 0 n'est pas premier (car il possède une infinité de diviseurs dans $\mathbb{N}$).
- 1 n'est pas premier (car il ne possède qu'un seul diviseur dans $\mathbb{N}$: lui-même).
- 17 est un nombre premier.
- 27 n'est pas un nombre premier car 27 est divisible par 3.

2) Propriétés

a Première propriété

PROPRIÉTÉ

Tout entier naturel **non premier** $n \geqslant 2$ possède au moins un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.

DÉMONSTRATION

Puisque n n'est pas premier, il admet des diviseurs autres que 1 et lui-même.
Soit E l'ensemble des diviseurs de n privé de 1 et de lui-même. E n'est pas vide car n n'est pas premier.
Il existe donc un plus petit élément de E noté p.
Si p n'était pas premier, p possèderait un diviseur p' distinct de 1 et de lui-même.
Ainsi, on aurait $p' < p$ et p' divise n (car il divise p), d'où $p' \in E$.
Ceci contredit le fait que p est le plus petit élément de E, donc p est premier.

On suppose que $n = pq$ avec $p < q$ car p est le plus petit diviseur premier de n.
Comme $p < q$, on a $p \times p < p \times q$. On en déduit $p^2 < n$, puis $p < \sqrt{n}$.

b Conséquence directe

PROPRIÉTÉ

Soit n un entier naturel tel que $n \geqslant 2$.
Si n n'est divisible par aucun nombre premier p tel que $2 \leqslant p \leqslant \sqrt{n}$, alors n est premier.

EXEMPLES

- Montrer que $n = 287$ n'est pas premier.
- Montrer que $p = 467$ est premier.

3) Infinitude des nombres premiers

THÉORÈME

L'ensemble des nombres premiers est infini.

REMARQUE

Autrement dit, ce théorème signifie qu'il n'existe pas de « plus grand nombre premier » : pour tout nombre premier p, il existe un nombre premier q tel que $q > p$.

DÉMONSTRATION

Démontrons ce théorème par l'absurde. Supposons donc qu'il n'existe qu'un nombre fini de nombres premiers : $2 < 3 < 5 < ... < p$ où p serait le plus grand nombre premier.
Posons $N = 2 \times 3 \times ... \times p + 1$. Le nombre N est strictement supérieur à 1. Il admet donc un diviseur premier d (propriété précédente).
Comme les nombres 2, 3, 4, ..., p sont les seuls nombres premiers, d est **nécessairement** l'un de ces nombres. Le nombre d divise donc le produit $2 \times 3 \times ... \times p$.
Mais d divise également le nombre N : il divise donc leur différence, c'est-à-dire 1, ce qui signifie que que $d = 1$. Or d est premier, donc d ne peut être égal à 1 !
Il existe donc une infinité de nombres premiers.

II Décomposition d'un entier en un produit de facteurs premiers

1) Le théorème de décomposition

THÉORÈME

Tout entier naturel supérieur ou égal à 2 se décompose en produit de facteurs premiers.
On note alors $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ où p_1, p_2, ..., p_r sont des nombres premiers distincts et α_1, α_2, ..., α_r sont des entiers naturels non nuls.
Cette décomposition est unique à l'ordre près des facteurs.

EXEMPLE

On peut décomposer 300 par étapes de plusieurs manières :
$300 = 2 \times 150 = 2 \times 15 \times 10 = 2 \times 3 \times 5 \times 2 \times 5$
ou encore $300 = 3 \times 100 = 3 \times 10 \times 10 = 3 \times 2 \times 5 \times 2 \times 5$.
Dans tous les cas, la décomposition sera $300 = 2^2 \times 3 \times 5^2$.

DÉMONSTRATION

Existence :
Si n est premier, alors le théorème est établi.
Sinon, le plus petit diviseur de $n > 1$ est premier (d'après la propriété 1). Notons le p_1.
On peut donc définir $n_1 = \dfrac{n}{p_1}$ avec $n_1 < n$.
Si n_1 est premier, alors le théorème est établi.
Sinon, on réitère le processus : il existe p_2 premier et l'on peut donc définit $n_2 = \dfrac{n_1}{p_2}$ avec $n_2 < n_1$.
On peut ainsi créer une suite (n_k) d'entiers naturels, strictement décroissante. Cette suite est nécessairement finie (principe de descente infinie) et son dernier terme est premier.
En regroupant les facteurs premiers identiques, on obtient $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$.

Unicité :
On démontre l'unicité par récurrence à l'aide du théorème de Gauss.
L'unicité de la décomposition est immédiate pour $n = 2$.
On suppose que la décomposition est unique pour tout entier inférieur strictement à un n donné et on montre que la décomposition de n en produit de facteurs premiers est unique.
On suppose que n admette deux décompositions distinctes en produit de facteurs premiers :

$$n = p_1 \times p_2 \times ... \times p_r = q_1 \times q_2 \times ... \times q_s$$

Si p_1 était premier avec q_i pour tout $1 \leqslant i \leqslant s$, alors d'après un corollaire du théorème de Gauss, p_1 serait premier avec $q_1 \times q_2 \times ... \times q_s$; or p_1 divise $q_1 \times q_2 \times ... \times q_s$ d'où une contradiction.
Donc il existe i tel que p_1 et q_i ne sont pas premiers entre eux. Comme ce sont des nombres premiers, on a nécessairement $p_1 = q_i$.
Le nombre $n_1 = \dfrac{n}{p_1}$ admettrait donc deux décompositions distinctes :

$$n_1 = p_2 \times p_3 \times ... \times p_r = q_1 \times q_2 \times ... \times q_{i-1} \times q_{i+1} \times ... \times q_s$$

ce qui contredit l'hypothèse de récurrence car $n_1 < n$ (car $p_2 \geqslant 2$). On en déduit que n admet une décomposition unique.
On a ainsi démontré par récurrence l'unicité de la décomposition pour tout $n \geqslant 2$.

EXERCICE

Déterminer la décomposition de 240 en produit de facteurs premiers.

2) Recherche des diviseurs

PROPRIÉTÉ — **admise**

Soit un entier $n \geqslant 2$.
Si la décomposition en facteurs premiers de n est : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k}$, alors les diviseurs positifs de n sont les entiers :
$p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout entier i de 1 à k.
Il y a donc $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$ diviseurs positifs de n.

EXEMPLE

$12 = 2^3 \times 3$.
$2^0 \times 3^0 = 1$; $2^1 \times 3^0 = 1$; $2^2 \times 3^0 = 4$; $2^0 \times 3 = 3$; $2^1 \times 3 = 6$ et $2^2 \times 3 = 12$.
Soit 6 diviseurs. $(2+1)(1+1) = 3 \times 2 = 6$.
Faire l'arbre : puissances de 2, puis puissances de 3

EXERCICE

• Déterminer le nombre de diviseurs positifs de 240.
• Soit n un entier naturel possédant exactement 5 diviseurs positifs. Quelles sont les valeurs possibles de n ?
$5 = 5 \times 1 = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1)$ avec $\alpha_i \geqslant 1$.
Donc $\alpha_1 = 4$ et c'est le seul. Donc $n = p^4$ avec p premier.

3) PGCD et PPCM

DÉFINITION

• Le **PGCD** de deux entiers est égal au produit de leurs diviseurs premiers communs, chacun d'eux étant élevé à son plus petit exposant.
• Le **PPCM** de deux entiers est égal au produit de tous leurs diviseurs premiers des deux décompositions, chacun d'eux étant élevé à son plus grand exposant.

REMARQUE

PGCD$(a\,;b)$ × PPCM$(a\,;b)$=ab.

EXEMPLE

Soient $a = 27\,216$ et $b = 60$.
Déterminer les décompositions en produit de facteurs premiers de a et de b, et en déduire PGCD$(a\,;b)$ et PPCM$(a\,;b)$.

III Petit théorème de Fermat

1) Le théorème

THÉORÈME

Soit p un nombre premier.
Pour tout entier naturel a non divisible par p, on a :

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

EXEMPLE

5 est un nombre premier et 7 est un entier naturel non divisible par 5.
Alors $5^6 \equiv 1\,[7]$, c'est-à-dire que $5^6 - 1$ est un multiple de 7.

DÉMONSTRATION

• p est un nombre premier donc il est premier avec tout entier k tel que $1 \leqslant k \leqslant p-1$, donc p est premier avec $(p-1)!$.

• Soient k un entier compris entre 1 et $p-1$, et r_k le reste de la division euclidienne de ka par p.
p est premier avec k et avec a (car a n'est pas divisible par p), donc p est premier avec ka, donc p n'est pas divisible par ka, donc $r_k \neq 0$.

• Soient k' un entier compris entre 1 et $p-1$ avec $k' \neq k$ (par exemple $k' > k$), et $r_{k'}$ le reste de la division euclidienne de $k'a$ par p. Alors $r_{k'} \neq r_k$.
En effet, si $r_{k'} = r_k$, alors $k'a \equiv ka\,[p]$, donc p divise $k'a - ka$, c'est-à-dire $a(k'-k)$.
Or $1 \leqslant k'-k \leqslant p-1$, donc p est premier avec $k'-k'$ et p est premier avec a donc p ne divise pas $a(k'-k)$, donc $r_{k'} \neq r_k$.

• Pour tout entier k compris entre 1 et $p-1$, $ka \equiv r_k\,[p]$, donc, par produits,
$a \times 2a \times ... \times (p-1)a \equiv r_1 \times r_2 \times ... \times r_{p-1}\,[p]$.
Or les r_k sont $p-1$ entiers distincts compris entre 1 et $p-1$ donc $r_1 \times r_2 \times ... \times r_{p-1} = (p-1)!$ et on a $(p-1)!a^{p-1} \equiv (p-1)!\,[p]$.
Donc p divise $(p-1)!a^{p-1} - (p-1)!$, c'est-à-dire p divise $(p-1)!(a^{p-1}-1)$.
Mais p est premier avec $(p-1)!$, donc d'après le théorème de Gauss, p divise $a^{p-1}-1$, donc $a^{p-1} \equiv 1\,[p]$.

REMARQUE

Ce théorème est connu comme le « petit théorème » de Fermat. Il existe un « grand théorème » de Fermat, qui n'est pas au programme, mais qui s'énonce ainsi :

Pour tout entier naturel $n > 2$, il n'existe pas de triplet $(x\,;y\,;z)$ d'entiers strictement positifs tel que $x^n + y^n = z^n$.

Son énoncé date du XVIIe siècle, mais sa démonstration n'a été établie qu'en 1994 !

2) Sa conséquence

PROPRIÉTÉ

Soit p un nombre premier.
Pour tout entier naturel a, on a :

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

DÉMONSTRATION

$a^p \equiv a\,[p] \iff p$ divise $a^p - a \iff p$ divise $a(a^{p-1}-1)$.

Si a est divisible par p, alors p divise bien $a(a^{p-1}-1)$, donc $a^p \equiv a\,[p]$.
Si a n'est pas divisible par p, alors p divise $a^{p-1}-1$ (d'après le petit théorème de Fermat), donc p divise $a(a^{p-1}-1)$, donc $a^p \equiv a\,[p]$.