

LES NOMBRES PREMIERS

1) DÉFINITION ET PROPRIÉTÉ

Définition :

Un entier naturel est **premier** s'il n'admet que deux diviseurs positifs : 1 et lui-même.

1 n'est pas un nombre premier.

Exemple :

2, 3, 5, 7 sont des nombres premiers. 4, 6, 8, 9, 10 ne sont pas des nombres premiers.

Propriétés :

Soit a un entier naturel strictement supérieur à 1.

- a possède au moins un diviseur premier.
- si a n'est pas premier, alors au moins un des diviseurs premiers de a est inférieur ou égal à \sqrt{a} .

Preuve :

Soit a un entier naturel strictement supérieur à 1.

- Considérons D_a l'ensemble des diviseurs de a strictement supérieurs à 1.

D_a n'est pas vide car il contient a . D_a a donc un plus petit élément n .

Par définition, ce plus petit élément n est un diviseur de a strictement supérieur à 1.

Supposons que n ne soit pas premier. n possède donc un diviseur p différent de 1 et de n .

Comme on sait que 0 ne divise pas n , on a $p > 1$.

D'autre part p étant un diviseur de n , on sait que $|p| \leq |n|$. On a donc $1 < p < n$.

Alors on sait que p divise n et n divise a , donc p divise a . On en déduit donc que $p \in D_a$.

Ceci est en contradiction avec le fait que n est le plus petit élément de D_a .

On ne peut donc pas supposer que n n'est pas premier.

On en déduit donc que n est un diviseur premier de a et que a possède donc au moins un diviseur premier.

- Soit n un diviseur premier de a . On peut écrire $a = n \times k$ avec $k \in \mathbb{N}^*$.

a n'est pas premier et ne peut donc pas être égal à n qui est premier. On a alors $k > 1$.

- Si $n \leq \sqrt{a}$, alors n est bien un diviseur premier de a inférieur ou égal à \sqrt{a} .

- Si $n > \sqrt{a}$, alors :

$$n \times k > k \sqrt{a} \Rightarrow a > k \sqrt{a} \Rightarrow k < \sqrt{a}.$$

k est donc un diviseur de a inférieur à \sqrt{a} .

k étant strictement supérieur à 1, il a un diviseur premier p et on sait que $p \leq k$ donc $p \leq \sqrt{a}$.

p étant un diviseur de k et k un diviseur de a , on en déduit que p est un diviseur de a .

p est donc un diviseur premier de a inférieur ou égal à \sqrt{a} .

Dans tous les cas on a donc trouvé un diviseur premier de a inférieur ou égal à \sqrt{a} .

Remarques :

- Un entier naturel strictement supérieur à 1 et qui n'est pas premier est appelé **nombre composé**.
- Pour déterminer si un nombre donné N est premier, on peut chercher s'il est divisible par un nombre premier inférieur ou égal à \sqrt{N} .
 - Si l'un des nombres premiers inférieurs ou égaux à \sqrt{N} divise N , alors N n'est pas premier.
 - Si aucun des nombres premiers inférieurs ou égaux à \sqrt{N} ne divise N , alors N est premier.

Cette méthode nécessite de connaître la liste des nombres premiers inférieurs ou égaux à \sqrt{N} .

2) CRIBLE D'ERATOSTHENE

Le crible d'Eratosthène est une méthode permettant d'obtenir tous les nombres premiers inférieurs à un nombre donné.

Pour trouver par exemple tous les nombres premiers inférieurs à 100, on écrit dans un tableau tous les nombres de 1 à 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- On raye le nombre 1 qui n'est pas premier.
- Le premier nombre non rayé est 2, il est premier.
- On raye tous les multiples de 2 supérieurs à 2.
- Le premier nombre non rayé est 3, il est premier.
- On raye tous les multiples de 3 supérieurs à 3.
- Le premier nombre non rayé est 5, il est premier.
- On raye tous les multiples de 5 supérieurs à 5.
- Le premier nombre non rayé est 7, il est premier.
- On raye tous les multiples de 7 supérieurs à 7.
- Le premier nombre non rayé est 11, il est premier.

On peut s'arrêter car $11 > \sqrt{100}$.

On a obtenu alors dans les cases non rayées, les nombres premiers inférieurs à 100.

3) INFINITÉ DES NOMBRES PREMIERS

Propriété :

Il existe dans \mathbb{N} une infinité de nombres premiers.

Preuve : exigible

Supposons que l'ensemble des nombres premiers soit un ensemble fini $\{p_1, p_2, \dots, p_k\}$.

Soit $n = p_1 \times p_2 \times \dots \times p_k + 1$.

n est strictement supérieur à 1, il admet donc un diviseur premier, c'est-à-dire l'un des nombres p_i .

p_i divise n et p_i divise $p_1 \times p_2 \times \dots \times p_k$, donc p_i divise leur différence, c'est-à-dire 1, ce qui est absurde.

L'ensemble des nombres premiers n'est donc pas un ensemble fini.

4) DÉCOMPOSITION EN PRODUIT DE FACTEURS PREMIERS

Propriété :

Soit n un entier supérieur ou égal à 2.

n peut se décomposer sous la forme : $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

où p_1, p_2, \dots, p_k sont des nombres premiers tels que $p_1 < p_2 < \dots < p_k$ et $\alpha_1, \alpha_2, \dots, \alpha_k$ des entiers naturels non nuls.

Cette décomposition est appelée **décomposition de n en produit de facteurs premiers**.

On admet que cette décomposition est unique.

Preuve :

Soit la propriété $P(n)$: "tout entier q tel que $2 \leq q \leq n$ peut se décomposer en produit de facteurs premiers.", pour $n \geq 2$ (HR)

Démontrons par récurrence que cette propriété est vraie pour tout entier $n \geq 2$.

Initialisation :

2 peut se décomposer sous la forme $2 = 2^1$. La propriété $P(2)$ est donc vraie.

Hérédité :

Supposons $P(n)$ vraie pour un entier $n \geq 2$ fixé, c'est à dire pour tout entier q tel que $2 \leq q \leq n$, q peut se décomposer en produit de facteurs premiers.

Montrons que la propriété $P(n+1)$ est vraie, c'est à dire pour tout entier q tel que $2 \leq q \leq n+1$, q peut se décomposer en produit de facteurs premiers.

Soit q un entier tel que $2 \leq q \leq n+1$

- Si $2 \leq q \leq n$, q peut se décomposer en produit de facteurs premiers, d'après (HR)

- Si $q = n+1$, alors on peut envisager deux cas :

- Si $n+1$ est premier, alors on peut écrire $n+1 = (n+1)^1$ et la décomposition est immédiate.

- Si $n+1$ n'est pas premier, alors $n+1$ a un diviseur premier p tel que $1 < p < n+1$, donc $2 \leq p \leq n$.

On peut alors écrire $(n+1) = p q$ avec q entier tel que $2 \leq q \leq n$.

D'après (HR), on peut décomposer q en facteurs premiers.

On obtient alors une décomposition de $p \times q$ en facteurs premiers, c'est-à-dire une décomposition de $n+1$ en facteurs premiers.

On a donc démontré que $P(n+1)$ est vraie.

Conclusion :

$P(n)$ est vraie pour tout entier $n \geq 2$ et en particulier tout entier $n \geq 2$ peut se décomposer en produit de facteurs premiers.

Exemples :

450	2
225	3
75	3
25	5
5	5
1	

On obtient :

$$450 = 2 \times 3^2 \times 5^2$$

17787	3
5929	7
847	7
121	11
11	11
1	

On obtient :

$$17787 = 3 \times 7^2 \times 11^2$$

On cherche les diviseurs premiers dans l'ordre croissant.

Remarques :

- Du fait de l'unicité de la décomposition, si n a pour décomposition en produit de facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ alors tout diviseur premier de n est l'un des nombres p_1, p_2, \dots, p_k
- La plupart des calculatrices de lycée permettent d'obtenir la décomposition d'un nombre en produit de facteurs premiers :

Avec une TI inspire:



factor(450)	$2 \cdot 3^2 \cdot 5^2$
factor(17787)	$3 \cdot 7^2 \cdot 11^2$

5) ENSEMBLE DES DIVISEURS

Exemple :

Dans \mathbb{N} l'ensemble des diviseurs de 200 est $\{1 ; 2 ; 4 ; 5 ; 8 ; 10 ; 20 ; 25 ; 40 ; 50 ; 100 ; 200\}$
On peut retrouver ce résultat à partir de la décomposition de 200 en produit de facteurs premiers.

En effet cette décomposition est $200 = 2^3 \times 5^2$

On peut alors vérifier que les diviseurs de 200 sont les nombres s'écrivant sous la forme $2^{\beta_1} 5^{\beta_2}$ avec $0 \leq \beta_1 \leq 3$ et $0 \leq \beta_2 \leq 2$.

Propriété :

Soit n un entier supérieur ou égal à 2, dont la décomposition en produit de facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$
L'ensemble des diviseurs naturels de n est l'ensemble des entiers d s'écrivant sous la forme $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$
où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_k \leq \alpha_k$.

Preuve :

n est un entier supérieur ou égal à 2, dont la décomposition en produit de facteurs premiers est : $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

• Considérons un entier d s'écrivant sous la forme $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$

où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_k \leq \alpha_k$.

On peut alors écrire $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = (p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}) \times (p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k})$

Donc $n = d \times q$ avec $q = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_k^{\alpha_k - \beta_k}$

On sait que $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_k \leq \alpha_k$.

Donc $\alpha_1 - \beta_1 ; \alpha_2 - \beta_2 ; \dots ; \alpha_k - \beta_k$ sont des entiers naturels.

Par conséquent q est un entier naturel et d est donc un diviseur de n .

• Considérons un entier d diviseur de n .

- Si $d = 1$, d peut s'écrire sous la forme $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $\beta_1 = \beta_2 = \dots = \beta_k = 0$

- Si $d > 1$, soit $d = q_1^{\gamma_1} q_2^{\gamma_2} \dots q_r^{\gamma_r}$ la décomposition de d en produit de facteurs premiers.

Alors q_1, q_2, \dots, q_r sont des diviseurs premiers de d , donc ce sont des diviseurs premiers de n , donc ce sont certains des nombres p_1, p_2, \dots, p_k .

On peut donc écrire $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels.

(Si le nombre p_i n'apparaît pas dans la décomposition de d , on aura $\beta_i = 0$)

Démontrons que l'on a alors que $\beta_1 \leq \alpha_1$

On sait que d divise n , et $p_1^{\beta_1}$ divise d , donc $p_1^{\beta_1}$ divise n , donc $p_1^{\beta_1}$ divise $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Si β_1 était strictement supérieur à α_1 , alors $p_1^{\beta_1 - \alpha_1}$ diviserait $p_2^{\alpha_2} \dots p_k^{\alpha_k}$ donc p_1 diviserait $p_2^{\alpha_2} \dots p_k^{\alpha_k}$, ce qui n'est pas possible puisque p_1 n'est pas l'un des nombres p_2, \dots, p_k .

On a donc $\beta_1 \leq \alpha_1$. De même on peut justifier que $\beta_2 \leq \alpha_2, \dots, \beta_k \leq \alpha_k$.

Donc d s'écrit sous la forme $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ où $\beta_1, \beta_2, \dots, \beta_k$ sont des entiers naturels tels que $0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_k \leq \alpha_k$

Remarque :

Si n a pour décomposition en produit de facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$,

le nombre de diviseurs naturels de n est alors $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1)$.

En effet tout diviseur naturel peut s'écrire $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ et chaque nombre β_i peut prendre les $(\alpha_i + 1)$ valeurs de 0 à α_i .

La décomposition de 200 en produit de facteurs premiers est : $200 = 2^3 \times 5^2$.

Ceci permet de dire que le nombre de diviseurs naturels de 200 est : $(3 + 1) \times (2 + 1) = 4 \times 3 = 12$.

6) APPLICATION : PETIT THÉORÈME DE FERMAT

Petit théorème de Fermat :

Si p un nombre premier et a un entier naturel non divisible par p , alors $a^{p-1} - 1$ est divisible par p .

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

Preuve :

Soit p un nombre premier et a un entier naturel non multiple de p .

Les entiers p et a sont donc premiers entre eux.

- Considérons l'ensemble des multiples de a : $A = \{ a, 2a, \dots, (p-1)a \}$
Ce sont $p-1$ multiples non nuls de a . L'entier p ne divise aucun d'entre eux.

En effet, si p divisait ka (avec k entier, $1 \leq k \leq p-1$), puisque p est premier avec a , il diviserait k d'après le théorème de Gauss, ce qui est impossible puisque $k < p$.

Donc leurs restes dans la division euclidienne par p sont non nuls et sont donc des éléments de $\{1, 2, \dots, p-1\}$

- Ces restes sont tous distincts : en effet si deux entiers k et k' appartenant à $\{1, 2, \dots, p-1\}$, avec $k > k'$, étaient tels que $ka \equiv ka' (p)$ alors p diviserait $(k-k')a$.

Or $1 \leq k-k' \leq p-2$, donc $(k-k')a$ est élément de A et aucun élément de A n'est divisible par p .

On a donc $p-1$ multiples de a dont les restes dans la division euclidienne par p sont exactement, à l'ordre près, les entiers $1, 2, \dots, p-1$.

- Considérons maintenant P le produit de ces multiples de a .

On a donc $P \equiv 1 \times 2 \times \dots \times (p-1) (p)$, c'est-à-dire $P \equiv (p-1)! (p)$. Ainsi p divise $(P - (p-1)!)$.

Or en réordonnant les facteurs de P , on obtient $P = (p-1)! \times a^{p-1}$.

Donc $P - (p-1)! = (p-1)! \times a^{p-1} - (p-1)! = (p-1)! \times (a^{p-1} - 1)$.

p divise donc $(p-1)! \times (a^{p-1} - 1)$.

Or p est premier et ne divise aucun des facteurs de $(p-1)!$. Il est donc premier avec $(p-1)!$

Donc d'après le théorème de Gauss, p divise $a^{p-1} - 1$.

Test de primalité :

Le petit théorème de Fermat donne une condition nécessaire pour que p soit premier. On dit qu'il constitue un test de primalité, ou plutôt ici de non primalité.

S'il existe un entier n compris entre 2 et $p-1$ tel que, n^{p-1} n'est pas congru à 1 modulo p , alors p n'est pas premier.

Ce test n'est pas efficace pour les grandes valeurs de p .

Propriété : Corollaire du petit théorème de Fermat

Si p un nombre premier et a un entier naturel, alors $a^p - a$ est divisible par p .

ou encore $a^p \equiv a [p]$

Preuve :

Dans la fiche d'exercices