Nombres premiers

Compétences attendues en fin de chapitre :

- Établir et utiliser des tests de divisibilités, étudier la primalité de certains nombres, étudier des problèmes de chiffrement.
- Existence et unicité de la décomposition en produit de facteurs premiers.
- Le petit théorème de Fermat.

Le mathématicien du chapitre :

Pierre de Fermat, mort en 1665, est un mathématicien Français d'Occitanie. Il fut surnommé le prince des amateurs. On lui doit notamment le principe de Fermat en optique. Il est surtout célèbre pour avoir énoncé le dernier théorème de Fermat qui ne sera démontré que 300 plus tard, en 1994.
En arithmétique, le petit théorème de Fermat va être travailler ici.

1) Nombres premiers

Définition :

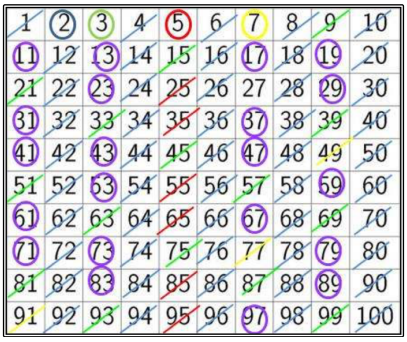
Un entier naturel est un nombre premier s'il admet exactement deux diviseurs positifs qui sont 1 et lui-même.

Remarque :

1 n'est donc pas un nombre premier car il ne possède qu'un seul diviseur.

- ***Le crible d'Ératosthène***

C'est un procédé qui permet de donner tous les nombres premiers. Il procède par élimination de tous les multiples d'un entier donné. A la fin, il ne reste que les nombres entiers qui ne sont multiples de personne : les nombres premiers.
Ci-contre, une représentation colorée du crible. Les nombres premiers sont matérialisés par un cercle violet.



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

- ***Les critères de divisibilité***

Ce sont l'ensemble des règles qui permettent (en un rapide coup d'œil) de savoir si on peut diviser un nombre. Un élève doit connaître le critère de divisibilité par : 2, 3,5, 9,10, et 11. Il en existe évidemment d'autres.

Définition :

Un nombre entier relatif est divisible par :
2 lorsque son chiffre des unités est 0, 2, 4, 6, 8.
3 lorsque la somme des chiffres qui le composent est divisible par 3.
5 lorsque son chiffre des unités est 0 ou 5.
9 lorsque la somme des chiffres qui le composent est divisible par 9.

Remarques :

Il existe d'autres critères de divisibilité qui sont bien moins utilisés.

Exemples :

- 128 est divisible par 2
- 321 est divisible par 3
- 1245 est divisible par 5 mais aussi par 3 donc est divisible par 15.
- 1342 est divisible par 11.

Théorème :

Il existe une infinité de nombres premiers et donc il n'existe pas de plus grand nombre premier.

Remarques :

- En décembre 2018, le plus grand nombre premier découvert a été le nombre qui possède presque 25 millions de chiffres $N = 2^{82\,559\,933} - 1$
- Il n'existe pas de formule donnant tous les nombres premiers. Certaines formules en donnent quelques-uns comme le polynôme $n^2 + n + 41$

Démonstration :

On va procéder à un raisonnement par l'absurde. On suppose qu'il existe un nombre fini de nombres premiers notés $p_1, p_2, p_3, \ldots\ldots, p_n$.
On considère le nombre $a = p_1 p_2 p_3 \ldots\ldots p_n + 1$. Ce nombre est un entier naturel supérieur ou égal à 2, il admet donc au moins un diviseur premier parmi les nombres $p_1, p_2, p_3, \ldots\ldots, p_n$
Cet entier p_i divise a et divise aussi $p_1 p_2 p_3 \ldots\ldots p_n$ donc divise leur différence, c'est-à-dire 1.
Ce qui est impossible car 1 ne possède pas d'autre diviseur que lui-même.

2) *Étudier un test de primalité*

Propriété :

Tout entier naturel supérieur ou égal à 2 est divisible par un nombre premier.

Démonstration :

On va procéder à un raisonnement par récurrence sur n, avec n supérieur ou égal à 2.
On note : P_n: Tout entier naturel compris entre 2 et n admet un diviseur premier.

Initialisation :

2 est divisible par 2 qui est un nombre premier donc P_2 est vraie, ***la propriété est initialisée.***

Hérédité :

Je suppose qu'il existe ***un entier n*** tel que P_n soit vraie et je veux montrer :
P_{n+1} : Tout entier naturel compris entre 2 et $n + 1$ admet un diviseur premier
Puisque P_n est vraie, tous les entiers naturels compris entre 2 et n admettent un diviseur premier. Il suffit donc de montrer que $n + 1$ admet un diviseur premier.

- Si $n + 1$ est premier, alors il admet un diviseur premier qui est lui-même.
- Si $n + 1$ n'est pas premier, il existe deux entiers a et b compris entre 2 et n tels que $n + 1 = a \times b$

a étant un entier naturel inférieur ou égal à n, l'hypothèse de récurrence donne l'existence d'un diviseur premier de a noté p.
D'où p/a et $a/(n + 1)$. Par transitivité, $p/(n + 1)$.
donc P_{n+1} est vraie, ***la propriété est héréditaire.***

Conclusion :

Tout entier naturel compris entre 2 et n admet un diviseur premier.

Propriété :

Soit n un entier naturel supérieur ou égal à 4.
Si n n'est pas premier, alors n admet au moins un diviseur premier noté p : son plus petit diviseur dans $\mathbb{N}$ autre que 1 est compris entre $2 \leq p \leq \sqrt{n}$

Démonstration :

On a $n \geq 4$ un nombre entier naturel non premier. L'ensemble de ses diviseurs supérieurs ou égaux à 2 contient au moins un élément différent de n. On note p le plus petit de ces diviseurs
On va procéder à un raisonnement par l'absurde.
On suppose donc que p n'est pas premier. Alors p admet un diviseur d tel que $2 \leq d < p$.
De plus, d divise p et p divise n, on en déduit que d divise n ce qui établit une contradiction car p est le plus petit diviseur de n strictement supérieur à 1.
Ainsi, p est premier.
On sait que $n = pq$ avec $2 \leq p \leq q$. Donc $p^2 \leq pq$ soit $p^2 \leq n$ et donc $p \leq \sqrt{n}$

Propriété :

Soit n un entier naturel supérieur ou égal à 4.
Si n n'est divisible par aucun nombre p compris entre $2 \leq p \leq \sqrt{n}$, alors n est premier.

Remarques :

- Il s'agit de la contraposée de la propriété précédente.
- Ce test devient rapidement inefficace si n est trop grand.

Exemple :

On considère 83. On a $\sqrt{83} \approx 9{,}1$.
83 n'est pas pair donc n'est pas divisible ni par 2, 4, 6 ou 8
La somme des chiffres de 83 est 11. Il n'est donc pas divisible par 3.
83 ne termine pas par 0 ou 5. Il n'est donc pas divisible par 5.
Enfin, 83 n'est pas dans la table de 7.
83 est donc un nombre premier (voir crible d'Ératosthène)

3) Décomposition d'un entier en produit de facteurs premiers

a) Existence et unicité d'une décomposition

Propriété :

Tout entier naturel $n \geq 2$ est premier ou produit de nombres premiers.

Démonstration :

Si n est premier, la propriété est établie.
Si n n'est pas premier, alors son plus petit diviseur $p_1 \geq 2$ est premier et il existe un entier naturel n_1 tel que $n = p_1 \times n_1$ avec $n_1 < n$
Si n_1 est premier, alors la propriété est établie.
Si n_1 n'est pas premier, on réitère le processus.
De proche en proche, on obtient ainsi une suite d'entiers naturels strictement décroissante notée (n_i) avec $2 \leq \ldots < n_i < \ldots < n_2 < n_1$.
Cette suite est finie est le dernier élément, noté n_k est un nombre premier.
On a donc $n = p_1 p_2 p_3 \ldots . p_k n_k$ avec les nombres $p_1, p_2, p_3 \ldots . p_k, n_k$ premiers.

Remarque :

Les nombres premiers ci-dessus ne sont pas nécessairement distincts. En les regroupant, on obtient $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} {p_3}^{\alpha_3} \ldots . {p_r}^{\alpha_r}$ avec $p_1, p_2, \ldots . p_r$ des nombres premiers et $\alpha_1, \alpha_2, \ldots . \alpha_r$ des entiers naturels non nuls. On dit que n est décomposé en produit de facteurs premiers.

Méthode :

On teste tous les nombres premiers dans l'ordre croissant en simplifiant autant de fois que nécessaire à chaque fois le nombre initial. Même si cela semble plus simple de diviser par un grand nombre, il est plus sur de prendre les diviseurs dans l'ordre.

Exemple :

84 est divisible par 2 : On a :$84 = 2 \times 42$
42 est divisible par 2 : On a :$42 = 2 \times 21$
21est divisible par 3 : On a :$21 = 3 \times 7$
7 est divisible par 7 : On a :$7 = 7 \times 1$
On a donc finalement : $84 = 2^2 \times 3 \times 7$

84	2
42	2
21	3
7	7
1	

Exercice :

Donner la décomposition en produit de facteurs premiers de 2520. $2520 = 2^3 \times 3^2 \times 5 \times 7$
Donner la décomposition en produit de facteurs premiers de 2450. $2450 = 2 \times 5^2 \times 7^2$
Donner la décomposition en produit de facteurs premiers de 429. $429 = 3 \times 11 \times 13$

Propriété :

La décomposition en produit de facteurs premiers de tout nombre entier naturel supérieur ou égal à 2 est unique.

b) *Diviseurs d'un nombre entier naturel non premier*

Propriété :

Soit n un entier naturel supérieur ou égal à 2.
La décomposition en produit de facteurs premiers s'écrit $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3} \ldots . {p_r}^{\alpha_r}$ avec $p_1, p_2, \ldots . p_r$ des nombres premiers et $\alpha_1, \alpha_2, \ldots . \alpha_r$ des entiers naturels non nuls.
Les diviseurs positifs de n sont de la forme ${p_1}^{\alpha'_1}{p_2}^{\alpha'_2} \ldots . {p_r}^{\alpha'_r}$ avec pour chaque exposant $0 \leq {\alpha'}_1 \leq \alpha_1, \ldots \ldots \ldots \ldots, 0 \leq {\alpha'}_5 \leq \alpha_5$

Remarque :

Le nombre de diviseurs de n est :$(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \times \ldots \times (\alpha_r + 1)$

Exemple :

Déterminer tous les diviseurs de 140 puis de 256.

- La décomposition en produit de facteurs premiers est : $140 = 2^2 \times 5 \times 7$
  On détermine alors la liste des diviseurs en prenant chaque nombre premier avec chacune de ses puissances. On peut s'aider d'un arbre si on le souhaite.
  Ainsi, $div(140) = \{1,2,4,5,7,10,14,20,28,35,70,140\}$ et $Card\big(div(140)\big) = 12$
- Pour 256, il s'agit finalement de 2^8 et on a : $256 = 2^8$
  La liste des diviseurs de 256 est constituée de toutes les puissances de 2.
  $div(256) = \{1,2,4,8,16,32,64,128,256\}$ et $Card\big(div(256)\big) = 9$

c) *Déterminer le PGCD et le PPCM*

Rappelons pour commencer les définitions.
PGCD : Plus Grand Commun Diviseur.
PPCM : Plus Petit Commun Multiple.
Soient m et n deux entiers naturels supérieurs ou égaux à 2. On suppose, quitte à utiliser des exposants nuls que, m et n peuvent s'écrire sous la forme d'un produit de facteurs premiers de la façon suivante :
$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3} \ldots . {p_r}^{\alpha_r}$ et $m = {p_1}^{\beta_1}{p_2}^{\beta_2}{p_3}^{\beta_3} \ldots . {p_r}^{\beta_r}$
On a alors :
$PGCD(m;n) = {p_1}^{min(\beta_1,\alpha_1)}{p_2}^{min(\beta_2,\alpha_2)}{p_3}^{min(\beta_3,\alpha_3)} \ldots . {p_r}^{min(\beta_r,\alpha_r)}$
$PPPCM(m;n) = {p_1}^{max(\beta_1,\alpha_1)}{p_2}^{max(\beta_2,\alpha_2)}{p_3}^{max(\beta_3,\alpha_3)} \ldots . {p_r}^{max(\beta_r,\alpha_r)}$

Utilité du PGCD et du PPCM :

Lorsqu'on doit simplifier une fraction, on divise numérateur et dénominateur par le PGCD.
Lorsqu'on doit ajouter deux fractions, le dénominateur commun est le PPCM

Exemple :

On donne les deux entiers naturels $m = 24$ et $n = 84$.
On obtient la décomposition en élément simple des deux entiers.
$24 = 2^3 \times 3^1 \times 7^0$ et $84 = 2^2 \times 3^1 \times 7^1$
$PGCD(24; 84) = 2^2 \times 3^1 \times 7^0 = 12$
$PPCM(24; 84) = 2^3 \times 3^1 \times 7^1 = 168$

4) Le petit théorème de Fermat

a) Un peu d'histoire

La célébrité de Pierre de Fermat provient de ses annotations dans la marge d'un exemplaire d'un ouvrage de Diophante : « diviser un cube en deux cubes, une puissance quelconque en deux puissances de même dénomination est impossible »
En d'autres termes, pour tout entier naturel n strictement supérieur à 2, il est impossible de trouver un triplet $(x; y; z)$ d'entiers non nuls tels que $x^n + y^n = z^n$
Cette propriété démontrée par Fermat uniquement pour $n = 4$ porte le nom de Grand théorème de Fermat. Ce n'est qu'en 1994 qu'Andrew Wiles est parvenu à le démontrer.
Le petit théorème de Fermat est énoncé en 1640 et les premières preuves sont dues à Leibniz et Euler.

b) Le théorème

Théorème :

p désigne un nombre premier et a un nombre entier naturel non divisible par p
Alors $a^{p-1} \equiv 1[p]$

c) Conséquence du théorème

Conséquence :

p désigne un nombre premier et a un nombre entier naturel
Alors $a^p - a$ est divisible par p, c'est à dire $a^p \equiv a[p]$

Exercice :

Montrer que, quel que soit l'entier naturel n, $n^{13} - n$ est divisible par 26.

Solution :

13 étant un nombre premier, d'après la conséquence du petit théorème de Fermat, on a :
$n^{13} - n \equiv 0[13]$. De la même manière, on a : $n^2 - n \equiv 0[2]$
On a $n^{13} = (n^2)^6 \times n$. Puisque $n^2 \equiv n[2]$ soit $(n^2)^3 \equiv n^3[2]$ donc $(n^2)^6 \times n \equiv n^4[2]$
On en déduit donc que $n^{13} \equiv n^4[2]$. $n^2 \equiv n[2]$ soit $n^4 \equiv n^2[2]$ et donc $n^4 \equiv n[2]$ et donc au final, $n^{13} \equiv n[2]$,
Puisque $n^{13} \equiv n[13]$, il existe donc un entier k tel que $n^{13} = n + 13k$
De même, $n^{13} \equiv n[2]$, il existe donc un entier k' tel que $n^{13} = n + 2k'$
Par soustraction, $n + 13k = n + 2k'$ soit donc $13k = 2k'$. Puisque 13 et 2 sont premiers entre eux, d'après le théorème de Gauss, il existe k'' tel que $k' = 13k''$.
On en déduit alors $n^{13} = n + 2k'$ soit donc $n^{13} = n + 2 \times 13k''$
On a donc $n^{13} = n + 26k''$ soit donc $n^{13} \equiv n[26]$ et $n^{13} - n$ est divisible par 26.