Nombres premiers

Extrait de Pour la Science n°251 Septembre 1998

La factorisation des grands nombres (Johannes Buchmann)

Le nombre 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541 est le produit de deux nombres premiers ; lesquels ?
Martin Gardner posa cette question aux lecteurs de Pour la Science en octobre 1977. dans sa rubrique de «Jeux mathématiques», mais une réponse ne fut donnée que 16 ans plus tard : en avril 1994, Paul Leyland, de l'Université d'Oxford. Michael Graff, de l'Université de l'Iowa, et Derek Atkins, de l'Institut de technologie du Massachusetts, identifièrent les deux facteurs, après avoir distribué des parties de la tâche, grâce au réseau Internet, à quelque 600 volontaires, qui laissèrent fonctionner sur leurs ordinateurs, pendant de nombreuses nuits, le programme écrit par Arjen Lenstra, du Centre de recherches de la Société Bell Communications.
La multiplication de deux nombres, même très grands, n'est pas compliquée : avec du papier et un crayon, on calcule le produit de deux nombres de 65 chiffres en une heure environ ; par ordinateur, le calcul est immédiat. En revanche, l'opération inverse, c'est-à-dire l'identification des facteurs d'un produit, est très difficile, même avec les calculateurs les plus rapides. (...)
Les opérations mathématiques telles que la multiplication et la factorisation sont à la base des systèmes cryptographiques modernes : le cryptage est rapide, mais le décryptage est quasi impossible en pratique. (...)
On ignore si la factorisation est difficile par essence ou si les mathématiciens n'ont pas encore trouvé la méthode la plus habile. Aussi la seule garantie de la sécurité des procédés de cryptage est l'ignorance d'une méthode rapide de factorisation des nombres entiers. L'étude de la factorisation date de l'Antiquité : les mathématiciens d'alors savaient déjà que chaque nombre naturel est un produit de nombres premiers, et que la décomposition en facteurs premiers est unique, à l'ordre près. Par exemple, 12 se décompose seulement en 2 x 2 x 3. L'étude des propriétés des nombres entiers naturels impose souvent la décomposition en facteurs premiers. (...)

Définition

Soit p un entier naturel strictement supérieur à 1.
On dit que p est un nombre premier si l'ensemble de ses diviseurs dans $\mathbb{N}$ est $\{1 ; p\}$.

Exemple 1 : nombres premiers

2 ; 3 ; 5 ; 7 sont des nombres premiers. 4, 6, 8, 9, 10 ne sont pas des nombres premiers.
Par convention, et pour des raisons de facilité, 1 n'est pas un nombre premier.

Exercice 01 (voir réponses et correction)

Les nombres suivants sont-ils premiers ?
43 ; 91 ; 871 ; 12 815 ; 568 793 ; 4 295 229 443 ; $10^{37} + 1$

Propriété (voir démonstration 01)

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 $\sqrt{a}$.

Remarque

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 $\sqrt{N}$.

Crible d'Eratosthène

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.
On raye tous les multiples de 2 supérieurs à 2.
On raye tous les multiples de 3 supérieurs à 3.
On raye tous les multiples de 5 supérieurs à 5.
On raye tous les multiples de 7 supérieurs à 7.
On peut s'arrêter car $11 > \sqrt{100}$.

Le premier nombre non rayé est 2, il est premier.
Le premier nombre non rayé est 3, il est premier.
Le premier nombre non rayé est 5, il est premier.
Le premier nombre non rayé est 7, il est premier.
Le premier nombre non rayé est 11, il est premier.

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

Les nombres rayés ne sont pas premiers puisque ce sont des multiples de l'un des nombres qui précèdent.
Si un nombre N n'est pas rayé, c'est que N n'est multiple d'aucun des nombres non rayés strictement inférieurs à 11, donc N n'est multiple d'aucun nombre premier strictement inférieur à $\sqrt{N}$, donc N est premier.

Exercice 02 (voir réponses et correction)

3 527, 3 529, 3 531, 3 533, 3 535, 3 537, 3 539, 3 541 sont-ils des nombres premiers ?
8 801, 8 803, 8 805, 8 807, 8 809, 8 811, 8 813, 8 815, 8 817 sont-ils des nombres premiers ?
9 431, 9 433, 9 435, 9 437, 9 439, 9 441 sont-ils des nombres premiers ?

Exercice 03 (voir réponses et correction)

Soit $f(n) = n^2 + n + 41$.
Montrer que pour $1 \leqslant n \leqslant 20$, $f(n)$ est un nombre premier.
Est-il possible que $f(n)$ soit un nombre premier pour tout entier naturel n ?
Qu'en est-il pour les valeurs de n comprises entre 21 et 40 ?

Propriété (voir démonstration 02)

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

Exercice 04 (voir réponses et correction)

Les nombres de Fermat sont les nombres de la forme $F_n = 2^{2^n} + 1$ avec $n \in \mathbb{N}$.
Fermat avait conjecturé que les nombres F_n étaient tous des nombres premiers.
Calculer F_0, F_1, F_2, F_3, F_4, F_5. Que pensez-vous de la conjecture de Fermat ?

Exemple 2 : Décomposition d'un nombre en facteurs premiers

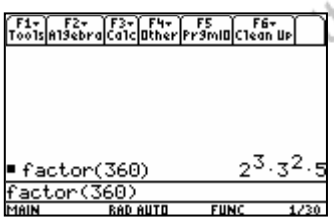
360	2
180	2
90	2
45	3
15	3
5	5
1	

On considère le nombre 360.
Il est divisible par 2 et on peut écrire $360 = 2 \times 180$
180 est encore divisible par 2 et on peut écrire $180 = 2 \times 90$
90 est encore divisble par 2 et on peut écrire $90 = 2 \times 45$
45 est divisible par 3 et on peut écrire $45 = 3 \times 15$
15 est divisible par 3 et on peut écrire $15 = 3 \times 5$

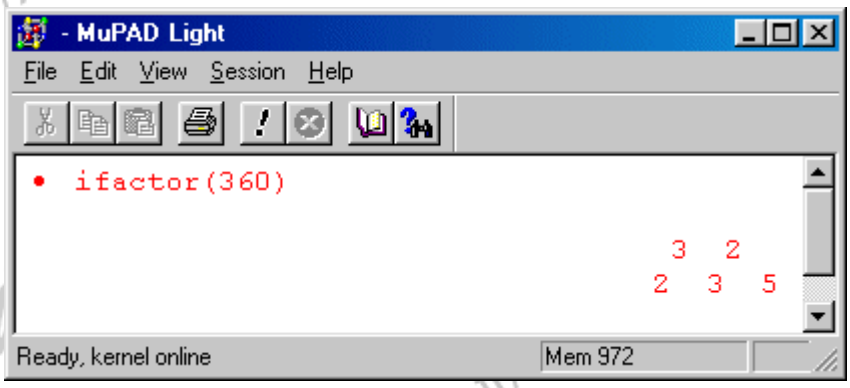
Finalement on obtient $360 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 = 2^3 \times 3^2 \times 5$
C'est la décomposition du nombre 360 en produit de facteurs premiers.

Certaines calculatrices et certains outils de calcul sur ordinateur permettent d'obtenir la décomposition d'un nombre en produit de facteurs premiers :

Calculatrice TI 89



Logiciel MuPad Light



Propriété (voir démonstration 03)

Soit n un entier supérieur ou égal à 2.
n peut se décomposer sous la forme : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$
où $p_1\ p_2 \cdots p_k$ sont des nombres premiers tels que $p_1 < p_2 < \cdots < p_k$
et $\alpha_1\ \alpha_2 \cdots \alpha_k$ des entiers naturels non nuls.
Cette décomposition est appelée décomposition de n en produit de facteurs premiers.
On admet que cette décomposition est unique.

Remarque

Du fait de l'unicité de le décomposition, si n a pour décomposition en produit de facteurs premiers
$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$
alors tout diviseur premier de n est l'un des nombres $p_1 ; p_2 ; \ldots ; p_k$

Exercice 05 (voir réponses et correction)

Décomposer en produit de facteurs premiers les nombres 1260 et 508 950 .

Exemple 3 : ensemble des diviseurs

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 $0 \leqslant \beta_1 \leqslant 3$ et $0 \leqslant \beta_2 \leqslant 2$,

c'est-à-dire
$2^0 \times 5^0 = 1$; $2^0 \times 5^1 = 5$; $2^0 \times 5^2 = 25$
$2^1 \times 5^0 = 2$; $2^1 \times 5^1 = 10$; $2^1 \times 5^2 = 50$
$2^2 \times 5^0 = 4$; $2^2 \times 5^1 = 20$; $2^2 \times 5^2 = 100$
$2^3 \times 5^0 = 8$; $2^3 \times 5^1 = 40$; $2^3 \times 5^2 = 200$

Propriété (voir démonstration 04)

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

Remarque

Si n a pour décomposition en produit de facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,
le nombre de diviseurs naturels de n est alors $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \ldots \times (\alpha_k + 1)$.
En effet tout diviseur naturel peut s'écrire $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ 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 quele nombre de diviseurs naturels de 200 est : $(3 + 1)(2 + 1) = 4 \times 3 = 12$.

Exercice 06 (voir réponses et correction)

Décomposer le nombre 504 en facteurs premiers, en déduire l'ensemble des diviseurs dans $\mathbb{N}$ de 504.

Exemple 4 : PGCD et PPCM

L'algorithme d'Euclide permet de justifier que PGCD(1500 ; 4725) = 75.
On sait que PGCD(1500 ; 4725) x PPCM(1500 ; 4725) = 1500 x 4725.
On peut en déduire que PPCM(1500 ; 4725) = 94500.
Ce résultat peut être obtenu à partir de la décomposition des nombres en facteurs premiers.
On a $1500 = 2^2 \times 3 \times 5^3$ et $4725 = 3^3 \times 5^2 \times 7$
Si on écrit la décomposition en utilisant les mêmes facteurs premiers pour les deux nombres et en autorisant l'utilisation d'exposants nuls, on peut écrire :
$1500 = 2^2 \times 3^1 \times 5^3 \times 7^0$ et
$4725 = 2^0 \times 3^3 \times 5^2 \times 7^1$
On peut alors remarquer que le nombre obtenu en prenant les exposants les plus petits est :
$2^0 \times 3^1 \times 5^2 \times 7^0 = 75 = \text{PGCD}(1500 ; 4725)$
et le nombre obtenu en prenant les exposants les plus grands est :
$2^2 \times 3^3 \times 5^3 \times 7^1 = 94500 = \text{PPCM}(1500 ; 4725)$

Propriété (voir démonstration 05)

Soient a et b deux entiers naturels supérieurs ou égaux à 2, se décomposant sous la forme :
$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$
où $p_1\ p_2 \cdots p_k$ sont des nombres premiers,
$\alpha_1\ \alpha_2 \cdots \alpha_k$ et $\beta_1\ \beta_2 \cdots \beta_k$ des entiers naturels éventuellement nuls.
Pour chaque valeur de i entre 1 et k, on pose $\delta_i = \text{minimum}(\alpha_i , \beta_i)$ et $\gamma_i = \text{maximum}(\alpha_i , \beta_i)$.
Alors $\text{PGCD}(a ; b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$ et $\text{PPCM}(a ; b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$.

Exercice 07 (voir réponses et correction)

En utilisant la décomposition en facteurs premiers, déterminer le PGCD et le PPCM de 414 et 888 .
Même question avec 1 272 et 2 650 .

Exercice 08 (voir réponses et correction)

En utilisant la décomposition en facteurs premiers, écrire la fraction $\frac{3\,675}{1\,470}$ sous forme irréductible.

Même question avec $\frac{306\,360}{428\,904}$.

Exercice 09 (voir réponses et correction)

En utilisant la décomposition en facteurs premiers, trouver un dénominateur commun le plus simple possible pour les trois fractions : $\frac{1}{756}$; $\frac{1}{504}$; $\frac{1}{468}$.

En déduire l'écriture de $\frac{1}{756} + \frac{1}{504} - \frac{1}{468}$ sous forme de fraction irréductible.

Exercice 10 (voir réponses et correction)

On considère le nombre $N = 2n^2 + 7n + 6$ avec $n \in \mathbb{N}$.
Pour quelles valeurs de n le nombre N est-il un nombre premier ?

Exercice 11 (voir réponses et correction)

On considère le nombre $N = 3n^2 + 8n + 5$ avec $n \in \mathbb{N}$.
Pour quelles valeurs de n le nombre N est-il un nombre premier ?

Exercice 12 (voir réponses et correction)

Soit p un nombre premier strictement supérieur à 3.
Démontrer que $p^2 + 11$ est divisible par 12.

Exercice 13 (voir réponses et correction)

Déterminer tous les couples d'entiers relatifs $(x ; y)$ tels que $x^2 - y^2 = 7$

Exercice 14 (voir réponses et correction)

Soit p un nombre premier.
Déterminer tous les couples d'entiers relatifs $(x ; y)$ tels que $x^2 - y^2 = p$

Exercice 15 (voir réponses et correction)

Résoudre l'équation $x^2 + 2x = y^2 + 40$ où x et y sont deux entiers naturels.

Exercice 16 (voir réponses et correction)

En utilisant un crible d'Eratosthène, ou une liste de nombres premiers, donner :

- une suite de 2 entiers consécutifs non premiers
- une suite de 3 entiers consécutifs non premiers
- une suite de 4 entiers consécutifs non premiers
- une suite de 5 entiers consécutifs non premiers
- une suite de 6 entiers consécutifs non premiers
- une suite de 7 entiers consécutifs non premiers

Soit N un entier naturel supérieur à 2.
Démontrer qu'il existe une suite de N entiers naturels consécutifs dont aucun n'est premier.