NOMBRES PREMIERS

Les nombres premiers ont un rôle fondamental en arithmétique. L'étude des propriétés des nombres entiers naturels impose souvent la décomposition en facteurs premiers.

Les nombres premiers ont aussi un rôle prépondérant en cryptographie. Autant la multiplication de deux nombres entiers, même très grands, n'est pas compliquée (avec un ordinateur, le calcul est immédiat…), autant l'opération inverse, c'est-à-dire l'identification des facteurs dans un produit est difficile, même avec les calculateurs les plus rapides.

En 1977, Martin Gardner posa la question aux lecteurs de « Pour la Science », dans sa rubrique « Jeux Mathématiques », de la décomposition en facteurs premiers d'un très grand nombre (129 chiffres). Une réponse ne fut donnée que 16 ans plus tard, grâce au travail collaboratif de quelques 600 ordinateurs…

La cryptographie à clé publique est basée sur ce principe : le cryptage est rapide, mais le décryptage est quasi impossible dans la pratique (tout du moins dans un laps de temps court…).

I) DEFINITION ET PROPRIETES IMMEDIATES

1) Définition

DEFINITION

Un nombre premier est un entier naturel qui admet ***exactement deux diviseurs*** : **1 et lui-même**.

CONSEQUENCE

- 1 n'est pas un nombre premier (***il n'a qu'un seul diviseur***).
- Un nombre premier p est un naturel supérieur ou égal à 2, soit $p \geq 2$.
- Les nombres premiers inférieurs à 100 sont :

2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 ; 47 ; 53 ; 59 ; 61 ; 67 ; 71 ; 73 ; 79 ; 83 ; 89 ; 97

2) Critère d'arrêt

THEOREME

Tout entier naturel n, $n \geq 2$, admet un diviseur premier.

Si n ***n'est pas premier*** (appelé ***nombre composé***), alors il admet un diviseur premier p tel que :

$$\mathbf{2 \leq p \leq \sqrt{n}}.$$

DEMONSTRATION

- Si n est premier, il admet donc un diviseur premier : lui-même.
- ……

……

……

……

- .....

.....

.....

EXEMPLE

Montrer que 109 est un nombre premier.

EXERCICE

Créer un algorithme pour déterminer si un nombre *N* est premier.
N'ayant pas à votre disposition la liste des nombres premiers, on teste si *N* est divisible par 2, puis on teste les diviseurs impairs par ordre croissant tant que ceux-ci sont inférieur à $\sqrt{N}$.

Variables : *N*, *I* entiers

Initialisation :

Lire *N*

$2 \rightarrow$ I

Traitement :

$si\ E\left(\frac{N}{I}\right) = \frac{N}{I}\ alors$

afficher *N*, « divisible par : », *I*

stop

fin

$I + 1 \rightarrow I$

Tant que $I \leq \sqrt{N}$ faire

$si\ E\left(\frac{N}{I}\right) = \frac{N}{I} alors$

afficher *N*, « divisible par : », *I*

stop

fin

$I + 2 \rightarrow I$

fin

Sorties : afficher *N*, « est premier ».

Exemples :

- 527 est divisible par 7
- 719 est premier
- 11 111 est divisible par 41
- 37 589 est premier

3) Infinité des nombres premiers

THEOREME

Il existe une infinité de nombres premiers.

DEMONSTRATION : ROC

.....
.....
.....
.....
.....
.....
.....
.....
.....

4) Le Crible d'Eratosthène

Le crible D'Ératosthène

Eratosthène est un mathématicien de l'antiquité (276 194 av.JC).
On cherche à connaître le début de la liste des nombres premiers. On utilisera pour cela la propriété suivante que nous admettrons : **un entier naturel non premier autre que 1 possède toujours un diviseur premier qui lui est strictement inférieur** (appelé **diviseur strict**).

On considère le début de la liste des nombres naturels.
0 et 1 ne sont pas premiers : barrons-les. 2 est premier : entourons-le. Ses multiples 4; 6; 8; 10; etc ne le sont pas : barrons-les.
Le premier nombre non barré après 2, c'est-à-dire 3 est premier puisqu'il n'a pas de diviseur premier strict. 3 est premier : entourons-le. Ses multiples 6; 9; 12; 15; etc ne le sont pas : barrons-les.

Le premier nombre non barré après 3, c'est-à-dire 5, est premier car il n'a pas de diviseur premier strict. 5 est premier : entourons-le. Ses multiples 10; 15; 20; etc ne le sont pas : barrons-les.
Remarque: 2×5; 3×5 ; 4×5 étant déjà barrés, le premier multiple de 5 non encore barré est 25.
Plus généralement, le premier nombre non encore barré parmi les multiples du nombre premier p sera: $\boldsymbol{p^2}$

Conséquence: Dans la recherche des nombres premiers jusqu'à 100, on peut cesser de barrer après avoir entouré .... dont le carré dépasse 100.
Compléter la grille jointe afin de trouver tous les nombres premiers jusqu'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

5) Nombres de Mersenne

DEFINITION

On appelle ***nombres de Mersenne***, les nombres M_n de la forme :

$$\boldsymbol{M_n = 2^n - 1} \qquad \boldsymbol{avec\ n \in \mathbb{N}^*}$$

EXEMPLES :

• **Calculer les 6 premiers nombres de Mersenne**.

$M_1 =$ … … … … … … … … … … ; $M_2 =$ … … … … … … … … … … …. ; $M_3 =$ … … … … … … … … … … ….

$M_4 =$ … … … … … … … … … … …. ; $M_5 =$ … … … … … … … … … … …. ; $M_6 =$ … … … … … … … … … … ….

On constate que pour les n égaux à 2, 3, 5, les nombres de Mersenne sont premiers.

Est-ce que si n est premier, M_n est premier ?

Cela permettrait de connaitre un nombre premier aussi grand que l'on veut.

REMARQUE : Actuellement (en janvier 2013), le plus grand nombre premier trouvé (nombre de Mersenne) est :

$$2^{57\,885\,161} - 1 \quad qui\ possède \quad 17\,425\,170\ chiffres \text{ !!!}$$

• **Montrons que si n n'est pas premier alors M_n ne l'est pas non plus**.

On a l'égalité suivante :

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

Si n n'est pas premier, alors il existe d, diviseur strict de n tel que :

$$n = d\,q \qquad avec \quad q > 1$$

Factorisons alors M_n :

$$M_n = 2^n - 1$$

$$M_n = \left(2^d\right)^q - 1$$

$$M_n = \left(2^d - 1\right)\left[\left(2^d\right)^{q-1} + \left(2^d\right)^{q-2} + \cdots + 2^d + 1\right]$$

Donc $2^d - 1$ est un diviseur strict de M_n et donc M_n n'est pas premier.

Conclusion : Si n n'est pas premier, alors M_n ne l'est pas non plus.

On peut aussi utiliser la contraposée : Si M_n est premier alors n l'est également.

• **La réciproque est-elle vraie ?**

Malheureusement, la réciproque est fausse, ce qui met à mal une formule permettant de trouver un nombre premier aussi grand que l'on veut.

En effet, si $n = 11$ alors $M_{11} = 2^{11} - 1 = 2\,047$ or $2\,047 = 23 \times 89$

M_{11} n'est pas premier mais 11 l'est.

II) DIVISIBILITE ET NOMBRES PREMIERS

1) Théorème de Gauss et nombres premiers

C'est une reformulation du théorème de Gauss et de ses conséquences dans le cas particulier des nombres premiers.

THEOREME

Un nombre premier divise un produit de facteurs si et seulement si il divise l'un de ces facteurs.

Si p divise a b ⇔ p divise a ou p divise b.

En particulier, si p premier divise une puissance a^k, alors nécessairement p divise a, d'où découle que p^k divise a^k.

2) Conséquences

• Si un nombre premier p divise un produit de facteurs premiers, alors p est l'un de ces facteurs premiers.

• Soit $p_1, p_2, \dots, p_k$ des nombres premiers distincts et $\alpha_1, \alpha_2, \dots, \alpha_k$ des entiers naturels non nuls.
Si pour tout $i \in \{1, 2, \dots, k\}$, $p_i^{\alpha_i}$ divise un entier n alors le produit $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ divise aussi l'entier n.

III) DECOMPOSITION, DIVISEURS D'UN ENTIER

1) Théorème fondamental de l'arithmétique

THEOREME

Tout entier $n \geq 2$ peut se décomposer de ***façon unique*** (à l'ordre des facteurs près) en produit de facteurs premiers.

$$\boldsymbol{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m}}$$

EXEMPLE

Décomposons 16 758 en produit de facteurs premiers :

16 758	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

Pour décomposer un entier, on effectue des divisions successives par des nombres premiers dans l'ordre croissant.

On a donc $\mathbf{16\,758 = 2 \times 3^2 \times 7^2 \times 19}$

ALGORITHME

Créer un algorithme pour déterminer les facteurs premiers d'un entier $N \geq 2$.
On teste si D est un diviseur de N en commençant par 2, puis les nombres impairs dans l'ordre croissant, en appliquant le critère d'arrêt $D \leq \sqrt{N}$. On réinitialise N en prenant le quotient $\frac{N}{D}$. Le dernier nombre qui ne vérifie pas le test d'arrêt est alors premier et on le rajoute à la liste des diviseurs.

Variables : N, D, I, C entiers

L_1 liste

Initialisation :

Lire N

$2 \to D$

$1 \to I$

$1 \to C$

Traitement :

$Tant\ que\ D \leq \sqrt{N}\ faire$

$si\ E\left(\frac{N}{D}\right) = \frac{N}{D}$

alors

$D \to L_1(I)$

$I + 1 \to I$

$\frac{N}{D} \to N$

sinon

$D + C \to D$

$2 \to C$

fin

fin

$N \to L_1(I)$

Sorties : Afficher L_1.

Exemples :

- 16 758 on obtient : $L_1 = \{2, 3, 3, 7, 7, 19\}$
- 87 616 on obtient : $L_1 = \{2, 2, 2, 2, 2, 37, 37\}$
- 77 986 545 on obtient : $L_1 = \{3, 5, 7, 13, 19, 31, 97\}$

APPLICATION

Calculer le PGCD et le PPCM de 126 et 735.

- *Décomposons les deux nombres en produit de facteurs premiers* :

126	2

735	3

On a donc :

$126 = \ldots \times \ldots \times \ldots$

$735 = \cdots \times \ldots \times \ldots$

- *On déterminer les facteurs communs pour le PGCD et les facteurs utilisés pour le PPCM* :

$PGCD\ (126\ ;\ 735) =$ et $PPCM\ (126\ ;\ 735) =$

2) Diviseurs d'un entier

THEOREME

Soit un nombre n $(n \geq 2)$ dont la décomposition en facteurs premiers est :

$$\boldsymbol{n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}}$$

Alors tout diviseur d de n a pour décomposition :

$$\boldsymbol{d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_m^{\beta_m}} \quad \text{avec} \quad 0 \leq \beta_i \leq \alpha_i \quad \text{et} \quad i \in \{1, 2, \ldots, m\}.$$

Le nombre de diviseurs *N* est alors :

$$\boldsymbol{N = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_m + 1)}$$

EXEMPLE

Trouver le nombre de diviseurs de 120 puis déterminer tous ces diviseurs.

• On décompose 120 en produit de facteurs premiers : $120 = 2^3 \times 3 \times 5$

On a alors $(\ldots + 1)(\ldots + 1)(\ldots + 1) = \ \ldots \times \ldots \times \ldots = \ \ldots.$

Il y a donc … diviseurs pour 120.

• Pour déterminer tous ces diviseurs, on peut utiliser un tableau double entrée en séparant les puissances de 2 et les puissances de 3 et 5. On obtient alors :

×				

• On peut aussi utiliser un arbre pondéré dont les coefficients sont les facteurs premiers possibles :

• Les …… diviseurs de 120 sont donc :

IV) PROBLEMES

1) ***Un entier naturel n a 15 diviseurs. On sait de plus que n est divisible par 6 mais pas par 8. Déterminer cet entier n.***

2) ***Déterminer le plus petit entier naturel possédant 28 diviseurs***

3) ***Un entier n a 5 diviseurs positifs. Quel peut-il être ?***