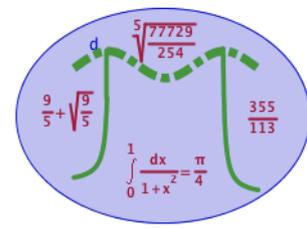


## Les nombres premiers



### I- Définition et premières propriétés

#### I-1 Définition

Un entier naturel  $n$  est premier s'il admet exactement deux diviseurs positifs distincts, 1 et lui-même

#### Remarques :

- 1 n'est pas premier car il n'a qu'un diviseur positif.
- Le plus petit nombre premier est 2. Mis à part 2, les nombres premiers sont impairs
- Il existe 15 nombres premiers inférieurs à 50 :

#### I-2 Test de primalité

Un entier naturel qui n'est pas premier est appelé un nombre composé.

#### Propriété:

- Tout entier naturel  $n$  admet un diviseur premier  $p$
- Si  $n$  n'est pas premier alors il admet un diviseur premier  $p$  tel que  $2 \leq p \leq \sqrt{n}$

#### Démonstration :

- Si  $n$  est premier, il admet pour diviseur premier lui-même.
- Si  $n$  n'est pas premier, l'ensemble des diviseurs  $d$  de  $n$  tel que  $2 \leq d < n$  n'est pas vide. Il possède donc un plus petit élément  $p$ . Si  $p$  n'était pas premier, il serait alors divisible par un entier  $k$  tel que  $2 \leq k < p$  qui diviserait  $n$  ce qui contredit  $p$  plus petit diviseur de  $n$  donc  $p$  est premier
- On a donc  $p$  premier et  $n$  qui peut s'écrire  $n = p \times q$  avec  $p \leq q$ . En multipliant par  $p$  cette inégalité, on obtient donc  $p^2 \leq pq$  c'est à dire  $p^2 \leq n$  d'où  $p \leq \sqrt{n}$

#### Conséquence : Test de primalité

En écrivant la contraposée de la propriété précédente, il en découle un test de reconnaissance d'un nombre premier :

Si tous les nombres premiers inférieurs à  $\sqrt{n}$  ne sont pas des diviseurs de  $n$  alors  $n$  est un nombre premier

151 est-il un nombre premier ?

$\sqrt{151} \approx 12,28$ . Il faut donc diviser 151 par les nombres premiers inférieurs à 12

Les critères de divisibilité classiques permettent d'affirmer que 2, 3, 5 ne divisent pas 151.

Reste donc à tester 7 et 11 :

$$151 = 7 \times 21 + 4$$

$$151 = 11 \times 13 + 8$$

Ces divisions n'étant pas exactes, 151 n'est pas divisible par 7 et 11 donc il est premier

### I-3 En algorithmique

Voici un algorithme permettant de déterminer si un entier $N > 2$ est premier ou non.	1 Lire N
<i>On utilise ici la fonction partie entière de <math>x</math> notée <math>E(x)</math> et on considère que nous ne disposons pas d'une liste des nombres premiers</i>	2 $2 \rightarrow I$
Lignes 4 et 5, on commence par tester si l'entier est pair ou non	3 $1 \rightarrow$ compteur
Lignes 7 à 13 : Si l'entier est impair, on teste ensuite les entiers impairs ( $I+2 \rightarrow I$ )	4 Si $E(N/I)=N/I$ alors
Lignes 15 à 18 : Si l'entier est premier, le compteur des diviseurs doit rester à 1	5       compteur = compteur+1
	6 Sinon
	7 $I+1 \rightarrow I$
	8       Tant que $I \leq \sqrt{N}$ faire
	9           Si $E(N/I)=N/I$ alors
	10               compteur = compteur+1
	11           Fin Si
	12 $I+2 \rightarrow I$
	13       Fin Tant que
	14 Fin Si
	15 Si compteur $> 1$ alors
	16       afficher N, « n'est pas premier »
	17 Sinon
	18       afficher N , « est premier »

### I-4 Infinité

**L'ensemble des nombres premiers est infini**

#### Démonstration

Supposons qu'il existe un nombre fini de nombres premiers que nous noterons  $p_1, p_2, p_3, \dots, p_n$ . Considérons alors le nombre  $a = p_1 p_2 p_3 \dots p_n + 1$ . Cet entier naturel est supérieur à 2, il admet donc au moins un diviseur premier  $p_i$  de l'ensemble des nombres  $p_1, p_2, p_3, \dots, p_n$ . Cet entier  $p_i$  divise  $a$  et divise  $p_1 p_2 p_3 \dots p_n$  donc il divise  $a - p_1 p_2 p_3 \dots p_n$  c'est à dire 1 ce qui est impossible. L'hypothèse de départ est donc fautive c'est à dire : il existe un nombre infini de nombres premiers.

## II- Décomposition en facteurs premiers

### II-1 Théorème fondamental de l'arithmétique

Tout entier naturel  $n \geq 2$  peut se décomposer de manière unique en produit de facteurs premiers

$$n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$$

où  $p_1, \dots, p_m$  sont des nombres premiers distincts et  $\alpha_1, \dots, \alpha_m$  des entiers naturels non nuls

**Démonstration :** Raisonnons par l'absurde

La propriété est vérifiée pour les premiers entiers : 2 ; 3 ; 4 = 2<sup>2</sup> ; 5 ; 6 = 2 × 3 .....

Supposons qu'il existe un entier n qui ne soit ni premier , ni produit de nombres premiers. On sait que cet entier admet au moins un diviseur premier . Notons le d . On a alors n = d × d' avec 1 < d' < n. Or n est le premier entier ne satisfaisant pas à la propriété donc d' la satisfait . L'écriture n = d × d' mène donc à une contradiction

**Exemple :**

Décomposons en facteur premier 16758. On divise successivement par les nombres premiers dans l'ordre croissant :

16758	2	
8379	3	
2793	3	
931	7	
133	7	
19	19	
1		

On obtient ainsi

$$16758 = 2 \times 3^2 \times 7^2 \times 19$$

**II-2 Algorithme de décomposition en facteurs premiers**

Voici un algorithme permettant d'obtenir la décomposition en facteurs premiers d'un entier.

Celui de gauche est « basique » dans le sens où il ne soigne pas l'affichage. Les deux suivants sont optimisés pour l'affichage sur TI et Casio à condition que la décomposition ne dépasse pas la largeur de l'écran et avec des nombres premiers < 100. Quoi qu'il en soit, on doit toujours vérifier le calcul affiché par la calculatrice en mode calcul

Programmer le sur votre calculatrice et retrouver le résultat suivant : 47 432 = 2<sup>3</sup> × 7<sup>2</sup> × 11<sup>2</sup>

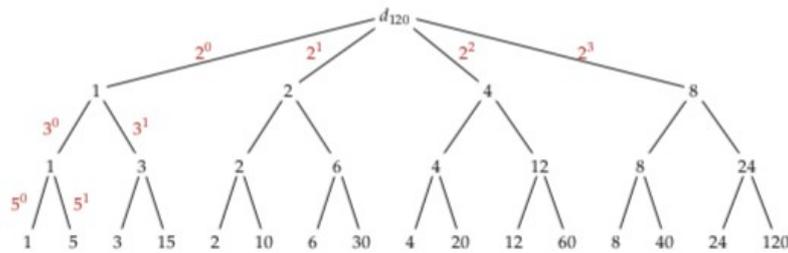
<p><b>Entrées :</b> Saisir n ≥ 2</p> <p><b>Traitement :</b></p> <p>D prend la valeur 2</p> <p>Tant que N ≠ 1</p> <p style="padding-left: 20px;">Tant que D divise N</p> <p style="padding-left: 40px;">Afficher D</p> <p style="padding-left: 40px;">N prend la valeur N/D</p> <p style="padding-left: 20px;">Fin Tant que</p> <p style="padding-left: 20px;">D prend la valeur D + 1</p> <p>Fin Tant Que</p>	<p><b>TI</b></p> <div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">       NOM VAR : FACTEURP     </div> <pre style="font-family: monospace; font-size: small;"> 001 1→A 002 EffÉcran 003 Input N 004 2→D 005 While N≠1 006 Ø→I 007 While N/D-partEnt(N/D)=Ø 008 I+1→I 009 N/D→N 010 End 011 If I≠Ø 012 Then 013 If D&lt;1Ø 014 Then 015 Output(2,A,D) 016 Output(2,A+1,"^") 017 Output(2,A+2,I) 018 Output(2,A+3,"*") 019 A+4→A 020 Else 021 Output(2,A,D) 022 Output(2,A+2,"^") 023 Output(2,A+3,I) 024 Output(2,A+4,"*") 025 A+5→A 026 End 027 End 028 D+1→D 029 End 030</pre>	<p><b>CASIO</b></p> <pre style="font-family: monospace; font-size: small;"> 1 → A Cls ? → N 2 → D While N ≠ 1 0 → I While N/D-Int(N/D)=0 I+1 → I N/D → N WhileEnd If I ≠ 0 Then If D &lt; 10 Then Locate A,2,D Locate A+1,2,"^" Locate A+2,2,I Locate A+3,2,"x" A+4 → A Else Locate A,2,D Locate A+2,2,"^" Locate A+3,2,I Locate A+4,2,"x" A+5 → A IfEnd IfEnd D+1 → D WhileEnd</pre>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### II-3 Nombre de diviseurs

**Propriété** Soit  $n$  un entier naturel supérieur ou égal à 2 admettant comme décomposition en facteurs premiers

$$n = p_1^{\alpha_1} \dots p_m^{\alpha_m}. \text{ Le nombre de diviseurs de } n \text{ est : } (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$$

Une propriété facile à comprendre si on réalise un arbre. Par exemple,  $120 = 2^3 \times 3 \times 5$ . Ainsi dans un diviseur de 120, on va retrouver  $2^0$  ou  $2^1$  ou  $2^2$  ou  $2^3$  de même pour 3 :  $3^0$  ou  $3^1$  et pour 5 :  $5^0$  ou  $5^1$  d'où le nombre de diviseurs de 120 :  $(3+1) \times (1+1) \times (1+1) = 16$  diviseurs



Préciser le nombre de diviseurs de 47 432 :

### III- Le petit théorème de Fermat - Hors programme

Soit  $p$  un nombre premier et un entier naturel  $a$  non multiple de  $p$ . On a alors :

$$a^{p-1} \equiv 1 \pmod{p}$$

#### Une démonstration intéressante

Considérons les  $p-1$  premiers multiples de  $a$  :  $a, 2a, 3a, \dots, (p-1)a$

Si on appelle  $r_1, r_2, \dots, r_{p-1}$  les restes dans la division par  $p$  de ces entiers ces restes sont deux à deux distincts. En effet, supposons que  $r_i = r_j$  pour  $i \neq j$ .

On a alors  $ai - aj \equiv r_i - r_j \pmod{p}$  c'est à dire  $a(i-j) \equiv 0 \pmod{p}$  donc  $a(i-j)$  serait multiple de  $p$  ce qui est impossible

$r_1, r_2, \dots, r_{p-1}$  sont donc des restes non nuls et deux à deux distincts on a alors

$$r_1 \times r_2 \times \dots \times r_{p-1} = 1 \times 2 \times \dots \times (p-1) = (p-1)!$$

d'où  $a \times 2a \times \dots \times (p-1)a \equiv (p-1)! \pmod{p}$

$$(p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$$

$$(p-1)! (a^{p-1} - 1) \equiv 0 \pmod{p}$$

$(p-1)! (a^{p-1} - 1)$  est donc multiple de  $p$  or  $p$  et  $(p-1)!$  sont premiers entre eux donc d'après le th de

Gauss  $p$  divise  $a^{p-1} - 1$  d'où  $a^{p-1} \equiv 1 \pmod{p}$