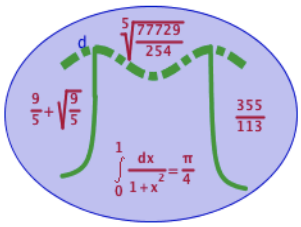



# Les nombres premiers

## 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.<br><br>*On utilise ici la fonction partie entière de x notée E(x) et on considère que nous ne disposons pas d'une liste des nombres premiers*<br><br>Lignes 4 et 5, on commence par tester si l'entier est pair ou non<br><br>Lignes 7 à 13 :<br>Si l'entier est impair, on teste ensuite les entiers impairs (I+2→I)<br><br>Lignes 15 à 18 :<br>Si l'entier est premier, le compteur des diviseurs doit rester à 1 | 1 Lire N<br>2 2 → I<br>3 1 → compteur<br>4 Si E(N/I)=N/I alors<br>5 compteur = compteur+1<br>6 Sinon<br>7 I+1 → I<br>8 Tant que I ≤ $\sqrt{N}$ faire<br>9 Si E(N/I)=N/I alors<br>10 compteur = compteur+1<br>11 Fin Si<br>12 I+2 → I<br>13 Fin Tant que<br>14 Fin Si<br>15 Si compteur > 1 alors<br>16 afficher N, « n'est pas premier »<br>17 Sinon<br>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 $p_{1,}p_{2,}p_{3,...,}p_n$ . Considérons alors le nombre a = $p_1p_2p_{3...}p_n+1$ . Cet entier naturel est supérieur à 2, il admet donc au moins un diviseur premier $p_i$ de l'ensemble des nombres $p_{1,}p_{2,}p_{3,...,}p_n$ . Cet entier $p_i$ divise a et divise $p_1p_2p_{3...}p_n$ donc il divise $a-p_1p_2p_{3...}p_n$ c'est à dire 1 ce qui est impossible. L'hypothèse de départ est donc fausse 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 ≥ 2 peut se décomposer de manière unique en produit de facteurs premiers

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

où $p_{1,...,}p_m$ sont des nombres premiers distincts et $\alpha_1,....,\alpha_m$ des entiers naturels non nuls

**Démonstration :** Raisonnons par l'absurde

La propriété est vérifiée pour les premiers entiers : 2 ; 3 ; 4 = $2^2$ ; 5 ; 6 = 2 $\times$ 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 $\times$ 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 $\times$ 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 | |

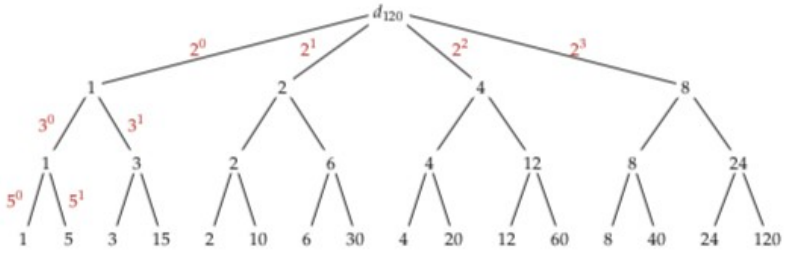
On obtient ainsi

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

## II-2 Nombre de diviseurs

**Propriété** Soit n un entier naturel supérieur ou égal à 2 admettant comme décomposition en facteurs premiers $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ . Le nombre de diviseurs de n 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

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

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

### Une démonstration intéressante

Considérons les p-1 premiers multiples de a : a , 2a , 3a , ... , (p-1)a

Si on appelle $r_1, r_2$ , ... , $r_{p-1}$ 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 $ai - aj \equiv r_i - r_j$ (p) c'est à dire $a(i-j) \equiv 0$ (p) donc $a(i-j)$ serait multiple de p ce qui est impossible

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

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

d'où

$$a \times 2a \times \ldots \times (p-1)a \equiv (p-1)! \text{ (p)}$$

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

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

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

### Une conséquence du petit théorème de Fermat

Soit p un nombre premier et un entier naturel a On a alors : $a^p \equiv a$ (p)

**Démonstration :** Deux cas sont à envisager selon que a soit multiple de p ou non

- Supposons a non multiple de p . D'après le petit théorème de Fermat, $a^{p-1} \equiv 1$ (p)
  on a donc par produit par a : $a \times a^{p-1} \equiv 1 \times a$ (p) cad $a^p \equiv a$ (p)
- Supposons maintenant a multiple de p . On a alors $a \equiv 0$ (p) et la règle reste valable