

Nombres premiers. pgcd et ppcm

Table des matières

1	Multiples et diviseurs	2
2	Nombres premiers	2
2.1	Définition	2
2.2	Test de primalité ou critère d'arrêt	2
2.3	Décomposition en nombres premiers	3
2.4	Nombres de diviseurs	3
2.5	Application	4
3	pgcd et ppcm	5
3.1	Définition	5
3.2	L'algorithme d'Euclide	5
3.3	Nombres premiers entre eux	6
3.4	Utilisation du pgcd et du ppcm	7

1 Multiples et diviseurs

Définition 1 : On dit que a est un **multiple** de b , si et seulement si, il existe un entier k tel que :

$$a = kb$$

D'autres formulations sont possibles : a est **divisible** par b , b est un **diviseur** de a ou b **divise** a .

Exemple :

54 est un multiple de 6 et de 9 car : $54 = 6 \times 9$

26 est un multiple de 2 et de 13 : car $26 = 2 \times 13$

Remarque : 0 est multiple de tout entier et 1 divise tout entier.

2 Nombres premiers

2.1 Définition

Définition 2 : On dit d'un entier a est un nombre premier, si et seulement si il admet exactement deux diviseurs 1 et lui-même.

Remarque : 1 n'est pas un nombre premier car il n'a qu'un seul diviseur : lui-même.

Les 25 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.

2.2 Test de primalité ou critère d'arrêt

Théorème 1 : Un nombre n n'est pas premier, si et seulement si, il existe un facteur premier p tel que :

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

Remarque : Si l'on ne peut pas trouver un tel nombre p , alors le nombre est premier.

Exemple :

- Montrons que 109 est premier.

On effectue un encadrement : $10 < \sqrt{109} < 11$

On essaie les diviseurs premiers jusqu'à 11 exclus, c'est à dire 2, 3, 5 et 7. Aucun de ces nombres ne divise 109 donc 109 est premier.

- Montrons que 323 n'est pas premier
 On effectue un encadrement : $17 < \sqrt{323} < 18$
 323 n'est pas divisible par : 2, 3, 5, 7, 11, et 13.
 Par contre, il est divisible par 17 car : $323 = 17 \times 19$.
 Donc 323 n'est pas premier.

2.3 Décomposition en nombres premiers

Théorème 2 : Tout nombre entier supérieur ou égal à deux peut se décomposer de façon unique en produit de facteurs premiers.

Pour décomposer un nombre entier en produit de facteurs premiers, on teste les nombres premiers dans l'ordre croissant. On commence à 2 puis 3, 5, ...

Exemple : Décomposons 16 758 en nombres premiers

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

On présente la décomposition avec une barre verticale où l'on écrit à droite, les diviseurs premiers et, à gauche le quotient des diviseurs premiers pris dans l'ordre croissant.

$$16\,758 = 2 \times 3^2 \times 7^2 \times 19$$

2.4 Nombres de diviseurs

Théorème 3 : Soit un entier n dont la décomposition en facteurs premiers est :

$$n = a^\alpha \times b^\beta \times c^\gamma \dots$$

Le nombre de diviseurs N est alors : $N = (\alpha + 1)(\beta + 1)(\gamma + 1) \dots$

Exemple :

- 1) Déterminer le nombre de diviseurs de 120.
- 2) En déduire tous les diviseurs de 120.



- 1) Décomposition de 120 en nombres premiers :

120	2
60	2
30	2
15	3
5	5
1	

On obtient alors : $120 = 2^3 \times 3^1 \times 5^1$

$$(3 + 1)(1 + 1)(1 + 1) = 4 \times 2 \times 2 = 16$$

120 possède donc 16 diviseurs.

2) On peut trouver les diviseurs de 120 de plusieurs façons :

- 1^{re} méthode :

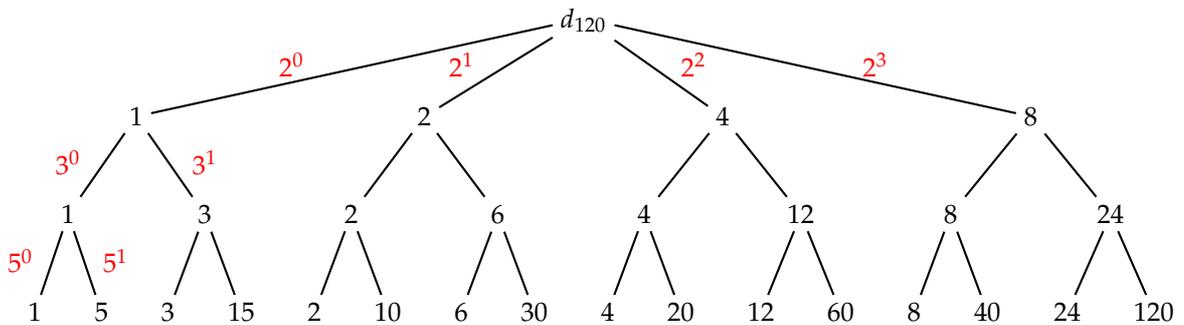
On commence par écrire dans deux colonnes 1 et 120 puis on teste si les nombres à partir de 2 sont diviseurs de 120 en s'arrêtant lorsque le nombre de la colonne de droite est plus petit que celui de la colonne de gauche.

Diviseur	Quotient
1	120
2	60
3	40
4	30
5	24
6	20
8	15
10	12

$$D_{120} = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$$

- 2^e méthode :

On utilise un arbre pondéré dont les coefficients sont les facteurs premiers possibles.



2.5 Application

Déterminer le nombre entier n satisfaisant simultanément aux trois conditions ci-dessous :

- n est divisible par 6
- n n'est pas divisible par 8.
- n a exactement 15 diviseurs.



Si n a exactement 15 diviseurs et si la décomposition en nombres premiers de n est : $n = a^\alpha \times b^\beta \times c^\gamma \dots$, alors on a :

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \dots = 15$$

La seule décomposition de 15 est : $15 = 3 \times 5$

Donc n n'admet que deux diviseurs premiers dans sa décomposition. De plus n est divisible par 6 et $6 = 2 \times 3$, les deux facteurs premiers de n sont nécessairement 2 et 3.

$$n = 2^\alpha 3^\beta \quad \text{avec} \quad (\alpha + 1)(\beta + 1) = 15$$

Comme n n'est pas divisible par 8 on a : $\alpha < 3 \Leftrightarrow \alpha + 1 < 4$

D'où : $\alpha + 1 = 3$ et $\beta + 1 = 5$. On trouve alors : $\alpha = 2$ et $\beta = 4$

Le nombre cherché est : $n = 2^2 \times 3^4 = 4 \times 81 = 324$

3 pgcd et ppcm

3.1 Définition

Définition 3 : pgcd et ppcm.

On appelle $\text{pgcd}(a, b)$ le plus grand commun diviseurs des entiers a et b .

On appelle $\text{ppcm}(a, b)$ le plus petit commun multiple des entiers a et b .

Théorème 4 : Entre le $\text{pgcd}(a, b)$ et le $\text{ppcm}(a, b)$, on a la relation suivante :

$$\text{ppcm}(a, b) = \frac{a \times b}{\text{pgcd}(a, b)}$$

Exemples :

- $\text{pgcd}(28, 77) = 7$ et $\text{ppcm}(28, 77) = \frac{28 \times 77}{7} = 28 \times 11 = 308$
- $\text{pgcd}(18, 42) = 6$ et $\text{ppcm}(18, 42) = \frac{18 \times 42}{6} = 18 \times 7 = 126$

Dans ces deux exemples, le pgcd est immédiat car les nombres ne sont pas trop grands. Lorsque cela n'est plus aussi immédiat, deux méthodes sont possibles : l'algorithme d'Euclide ou la décomposition en nombres premiers.

3.2 L'algorithme d'Euclide

Théorème 5 : Soit deux entiers a et b , pour connaître le $\text{pgcd}(a, b)$, on effectue les divisions euclidiennes successives suivantes :

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0q_1 + r_1 && \text{division de } b \text{ par } r_0 \\ r_0 &= r_1q_2 + r_2 && \text{division de } r_0 \text{ par } r_1 \\ r_1 &= r_2q_3 + r_3 && \text{division de } r_1 \text{ par } r_2 \\ \dots & \dots \end{aligned}$$

Le dernier reste non nul correspond au $\text{pgcd}(a, b)$

Exemples :

- Déterminons le $\text{pgcd}(945, 882)$

On effectue les divisions suivantes :

$$945 = 882 \times 1 + 63$$

$$882 = 63 \times 14 + 0$$

Donc $\text{pgcd}(945, 882) = 63$

- Déterminons le pgcd(935, 561)

On effectue les divisions suivantes :

$$935 = 561 \times 1 + 374$$

$$561 = 374 \times 1 + 187$$

$$374 = 187 \times 2 + 0$$

Donc $\text{pgcd}(935, 561) = 187$

Remarque : On s'aperçoit sur ces deux exemples de l'efficacité de cet algorithme. Il sera donc à préférer à la méthode par décomposition en facteurs premiers

A titre de comparaison, utilisons la méthode de décomposition pour déterminer le pgcd(945, 882).

$$\begin{array}{r|l} 945 & 3 \\ 315 & 3 \\ 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

$$\begin{array}{r|l} 882 & 2 \\ 441 & 3 \\ 147 & 3 \\ 49 & 7 \\ 7 & 7 \\ 1 & \end{array}$$

On a donc :

$$945 = 3^3 \times 5 \times 7$$

$$882 = 2 \times 3^2 \times 7^2$$

Pour déterminer le pgcd, il suffit de prendre les facteurs en commun, donc :

$$\text{pgcd}(945, 882) = 3^2 \times 7 = 63$$

3.3 Nombres premiers entre eux

Définition 4 : Deux entiers a et b sont premiers entre eux si, et seulement si,

$$\text{pgcd}(a, b) = 1$$

Exemples :

- $\text{pgcd}(9, 16) = 1$ car $9 = 3^2$ et $16 = 4^2$.
9 et 16 sont premiers entre eux.
- Déterminons le pgcd(1 600, 229) par l'algorithme d'Euclide :

$$1\ 600 = 229 \times 6 + 226$$

$$229 = 226 \times 1 + 3$$

$$226 = 3 \times 75 + 1$$

$$3 = 1 \times 3 + 0$$

Donc $\text{pgcd}(1\ 600, 229) = 1$,

Les nombres 1 600 et 229 sont donc premiers entre eux.

3.4 Utilisation du pgcd et du ppcm

Soit le problème suivant :

- 1) On veut découper un rectangle de 24 cm sur 40 cm en carrés dont le côté est le plus long possible, sans perte. Quel doit être le côté du carré ?
- 2) On dispose d'un grand nombre de rectangles du type précédent que l'on veut assembler bord à bord pour former un carré le plus petit possible. Quel doit être le côté du carré ?



- 1) On peut faire le schéma ci-contre :

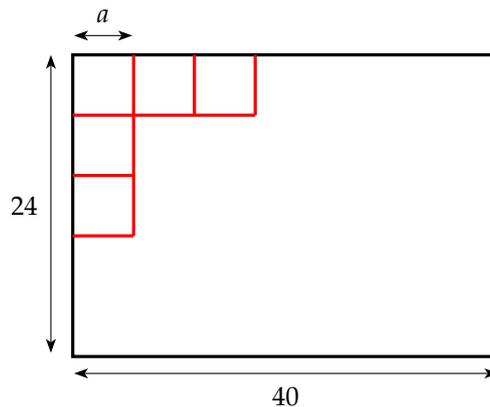
Soit a la longueur du côté du carré.

S'il n'y a pas de perte, a doit diviser 24 et 40. Donc a est un diviseur commun à 24 et 40.

Comme a doit être le plus grand possible, on a :

$$a = \text{pgcd}(40, 24) = 8$$

Le carré le plus grand possible mesure de 8 cm de côté.



- 2) On peut faire le schéma ci-contre :

Soit b la longueur du côté du carré.

Si les rectangles sont mis bout à bout,

b doit être un multiple de 24 et 40.

Donc b est un multiple commun à 24 et 40.

Comme b doit être le plus petit possible, on a :

$$b = \text{ppcm}(40, 24) = \frac{40 \times 24}{\text{pgcd}(40, 24)} = \frac{40 \times 24}{8} = 40 \times 3 = 120$$

Le carré le plus petit possible mesure de 120 cm de côté.

