

Théorème de Gauss: pour tout nombre entier $n \in \mathbb{N}^*$
il existe une décomposition en facteurs premiers unique.

Comment les trouve-t-on? Trial & Error

- 1) fait une liste de premiers de $2, \dots, \sqrt{N}$
- 2) On divise par le plus petit premier restant tant que c'est possible, sinon on passe au suivant.

Exemple: 3724

1) ~~2~~, ~~3~~, ~~5~~, 7, 11, 13, 17, 19, 23, 29, 31

2) $3724 / 2 \Rightarrow 1862 / 2 = 931$

$$3724 = 2 \times 2 \times 931$$

$$= 2 \times 2 \times 7 \times 133$$

$$= 2 \times 2 \times 7 \times 7 \times \underline{19}$$

STOP

Exercice: décompose 70 en facteurs premiers

$$70 = 2 \times 35 = 2 \times 5 \times 7$$

Définitions:

Plus Grand Commun Diviseur de deux nombres entiers $A, B \in \mathbb{N}$ est noté $\text{PGCD}(A, B)$. Par convention on suppose $A \geq B$.

Si $\text{PGCD}(A, B) = 1$ on dit que A et B sont PREMIERS ENTRE EUX.

⚠ A et B peuvent être premiers entre eux SANS pour autant être des nombres premiers !!!

Exemple: $\text{PGCD}(4, 9) = 1$ mais $4 = 2 \times 2$ pas premier |
 $9 = 3 \times 3$ pas premier .

Comment calculer le $\text{PGCD}(A, B)$?

Méthode 1: Factorisation

On factorise A et B en produit de facteurs premiers,

et $\text{PGCD}(A, B) =$ produit des facteurs communs.

Ex: $\text{PGCD}(42, 30) = 2 \times 3 = 6$

$$42 = 2 \times 21 = 2 \times 3 \times 7$$

$$30 = 2 \times 15 = 2 \times 3 \times 5$$

↑

Pour chaque paire commune,
ne l'utiliser qu'une fois dans le PGCD !

$$\text{PGCD}(18, 27) = 3 \times 3 = 9$$

$$18 = 2 \times 3 \times 3$$

$$27 = 3 \times 3 \times 3$$

Méthode 2: Euclide

$$\text{PGCD}(42, 30)$$

$$\begin{array}{r|l} 42 & 30 \\ \hline r=12 & 1 \end{array} \rightarrow \begin{array}{r|l} 30 & 12 \\ \hline r=6 & 2 \end{array} \rightarrow \begin{array}{r|l} 12 & 6 \\ \hline r=0 & 2 \end{array}$$

PGCD STOP

$$\text{PGCD}(42, 30) = 6$$

Exercice:

$$\text{PGCD}(770, 168) = ?$$

$$\begin{array}{r|l} 770 & 168 \\ \hline r=98 & 4 \end{array} \rightarrow \begin{array}{r|l} 168 & 98 \\ \hline 70 & 1 \end{array} \rightarrow \begin{array}{r|l} 98 & 70 \\ \hline 28 & 1 \end{array}$$

$$\begin{array}{r|l} 70 & 28 \\ \hline 14 & 2 \end{array} \rightarrow \begin{array}{r|l} 28 & 14 \\ \hline r=0 & 2 \end{array}$$

STOP

$$\text{PGCD}(770, 168) = 14$$