Qu'est-ce qu'est le PGCD ?

Définition : Soit a et b deux entiers naturel non nuls,
Le PGCD(a ; b) est le **P**lus **G**rand **D**iviseur **C**ommun (en anglais l'adjectif est avant)à la fois à a et à b.

a et b sont deux **nombres premiers entre eux** signifie que PGCD(a;b) = 1.

Exemple : PGCD(13;5) = 1 car 13 et 5 sont deux nombre premiers entre eux.

Exemple: PGCD(12;8) = 4
Pour trouver le PGCD de nombres a et b peu élevé on peut faire une courte liste des diviseurs communs.
12 et 8 ont comme diviseurs communs 1,2,4 et 4>2>1

Remarque :
Ne pas confondre le PGCD des nombres premiers et le PGCD des nombres premiers entre eux. Si on prend 5 (nombre premier) et 15 on a PGCD(5;15) = 5 ≠ 1

Le PGCD est en lien avec le PPCM qui est le plus petit commun multiple non nul noté PPCM(a;b)

Exemple :
PPCM(12;15) = 60 car tout multiple de 60 est multiple de 12 et de 15.

Calcul du pgcd : Méthode des soustractions successives

PGCD (448 ; 350) = ? On soustrait jusqu'à arriver à 0 la différence positive (valeur absolue) de la soustraction précédente avec les deux plus petits nombres.

448 - 350 = 98

350 - 98 = 252

252 - 98 = 154

154 - 98 = 56

98 - 56 = 42

56 - 42 = 14

42 - 14 = 28

28 - 14 = 14

14 - 14 = 0 Le dernier résultat non nul est le pgcd : ici, pgcd(448 ; 350) = 14

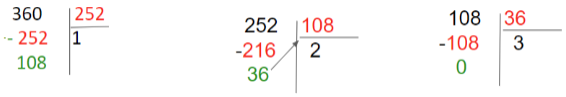
Calcul du pgcd : Méthode de l'algorithme d' Euclide

$\exists a, b \in \mathbb{N}^{*2} / b \nmid a$

La suite des **divisions** euclidiennes des **diviseurs par le reste** de la division précédente finit par s'arrêter. (On appelle cela un algorithme récursif). Le **dernier reste non nul** est alors PGCD(a , b).
On rappelle que la division euclidienne de a par b se note : $a = bq + r$, où a est le dividende, b le diviseur, q le quotient et r le reste.
On a donc :

$$
\begin{array}{llllll}
a & = & bq_0 + r_0 & \text{avec} & b > r_0 \geqslant 0 \\
b & = & r_0q_1 + r_1 & \text{avec} & r_0 > r_1 \geqslant 0 \\
r_0 & = & r_1q_2 + r_2 & \text{avec} & r_1 > r_2 \geqslant 0 \\
\vdots & & \vdots & & \vdots \\
r_{n-2} & = & r_{n-1}q_n + r_n & \text{avec} & r_{n-1} > r_n \geqslant 0 \\
r_{n-1} & = & r_nq_{n+1} + 0 & \text{avec} & \text{on a alors : PGCD}(a\ ,\ b) = r_n
\end{array}
$$

Exemple : Calculer le pgcd avec l'algorithme d'Euclide : Calculer le PGCD de 252 et 360.



Le PGCD est le dernier reste non nul, soit PGCD (252,360)=36

Théorème de Bézout : Si deux entiers relatifs a et b ont pour pgcd(a ; b) = D alors il existe deux entiers relatifs u et v tels que : au + bv = D

Remarque : Les entiers relatifs u et v ne sont pas uniques, ils se nomment les coefficients de Bézout ou couple de Bézout.

Méthode : Retrouver le couple de Bézout à partir du PGCD D'Euclide

Reprenons les valeurs précédentes: 360 et 252

On refait le PGCD avec un notation

360 = 1 * 252+108

252=2*108+36

108=36*3+0

donc 36 est le PGCD de 360 et 252

Maintenant nous pouvons retrouver le couple de Bézout

36 = 252 - 2 * 108

36 = 252 - 2 (360 - 252)

36 = -2 * 360 + 3 * 252

On peut donc choisir u = -2 et v = 3

Identité de Bézout : Deux entiers relatifs a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que : au + bv = 1

Exercice : Démontrer que pour tout entier naturel n, 2n+3 et 5n+7 sont premiers entre eux
On cherche les coefficients de Bézout tels que : au + bv = 1, on commence par travailler sur le membre de gauche de l'équation :
(2n+3)u + (5n+7)v = 5(2n+3)+(-2)(5n+7) On raisonne ici par intuition pour éliminer les n.
= 10n+15-10n-14
= 15-14 = 1 On retrouve 1 donc 2n+3 et 5n+7 sont premiers entre eux

Corollaire du théorème de Bézout : L'équation ax + by = c admet des solutions entières si et seulement si le nombre c est un multiple du pgcd(a, b).

Exercice : Les équations 4x + 9y = 2 et 9x - 15y = 2 admettent-elles des solutions ?
Par le corollaire du théorème de Bézout,
L'équation 4x + 9y = 2 admet des solutions car pgcd(4,9) = 1 et 1 est un multiple de 2
L'équation 9x - 15y = 2 n'admet pas de solution car pgcd(9,15) = 3 et 3 n'est pas un multiple de 2

Théorème de Gauss : Soient a, b et c trois entiers relatifs non nuls. Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c.

Exercice : Déterminer les solutions dans $\mathbb{Z}^2$ de l'équation 7(x-2) = 9(y+1)
Soit (x ; y) une solution de l'équation. Comme 7 divise 7(x-2) il divise aussi 9(y+1).
Comme PGCD(7 ; 9) = 1, le théorème de Gauss affirme que 7 divise y+1. Donc il existe $k \in \mathbb{Z}$ tel que y+1 = 7k, soit y = 7k-1. En remplaçant dans l'équation initiale, on a :
7(x-2) = 9*7k $\Leftrightarrow$ x-2 = 9k $\Leftrightarrow$ x = 9k+2
Ainsi, si (x ; y) est un couple solution, alors : x = 9k+2 y = 7k-1 où $k \in \mathbb{Z}$

Réciproquement, on vérifie que les couples (9k+2 ; 7k-1) sont solutions :
On a 7(x-2) = 7 × 9k = 63k et 9(y+1) = 9 × 7k = 63 k

Corollaire du théorème de Gauss : Si b et c divisent a et si b et c sont premiers entre eux alors bc divise a

Applications :
Equation diophantienne : *ax + by = c*, avec *a*, *b* et *c* entiers relatifs

a. Déterminer les entiers x et y tels que 7x – 9 y = 1
b. Déterminer les entiers x et y tels que 7x – 9 y = 12

a) Comme pgcd(7 ; 9)=1 par le corollaire du théorème de Bézout, l'équation possède des solutions entières.
- On trouve une solution particulière : en remontant l'algorithme d'Euclide par exemple. $1 = 7 - 2 \times 3 = 7 - (9 - 7) \times 3 = 7 \times 4 - 9 \times 3$ donc (4 ; -3) est une solution particulière. Attention cette solution n'est pas unique.
- On remplace le 1 par le calcul de la solution particulière puis on tri selon les multiples de 7 et 9 : $7x - 9y = 7 \times 4 - 9 \times 3$
  $7(x - 4) = -9(3 - y)$ *Attention aux signes !*
- A l'aide du théorème de Gauss, (voir rédaction à l'exemple précédent), on conclut.
  $$x = 4 + 9k \; et \; y = 7k - 3 \; où \; k \in \mathbb{Z}$$
- Réciproquement, on vérifie que les solutions trouvées fonctionnent bien.

b) C'est le même problème que a) en ayant multiplié x, y et 1 par 12 ainsi :
$$x = 48 + 108k \; et \; y = 84k - 36 \; où \; k \in \mathbb{Z}$$

Détermination des racines rationnelles d'un polynôme à coefficients entiers

Polynôme à coefficients entiers sous la forme $P(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0$, avec $n \in \mathbb{N}$ et les $(a_n, a_{n-1}, a_{n-2}, \ldots, a_1, a_0) \in \mathbb{N}^{n+1}$
Nombres rationnels irréductibles : nombres s'écrivant sous la forme p/q avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et PGCD(p;q)=1
Racines : solutions à une équation f(x)=0

Méthode: On remplace x par $\frac{p}{q}$ et on multiplie par la plus grande puissance de x (si on a un polynôme de degré 3 alors en multiplie par q^3). On isole la plus grande puissance de p et on simplifie le reste par q. Avec le résultat on peut conclure si la racine du polynôme est rationnelle ou non.

Le Lemme chinois ou Théorème des restes chinois

Soit $m_1, m_2, \ldots, m_r$ une suite d'entiers positifs premiers entre eux deux a deux. Alors le système de congruences : $\begin{cases} x \equiv a_1 \; [m_1] \\ x \equiv a_2 \; [m_2] \\ x \equiv a_3 \; [m_3] \\ \quad \ldots \\ x \equiv a_r \; [m_r] \end{cases}$ a une unique solution x modulo M tels que $M = m_1 \times m_2 \times \ldots \times m_r$:

Alors $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r$ avec : $M_i = M/m_i$ et $y_i M_i \equiv 1 \; [m_i]$