PGCD – PPMC - Théorèmes de Bézout – Gauss – Petit théorème de Fermat

Deux nombres sont ***premiers entre eux*** , si et seulement si 1 est leur seul diviseur commun : **$(a\,;\,b)$ premiers entre eux $\Leftrightarrow$ PGCD$(a\,;\,b)=1$.**

Les diviseurs communs de deux nombres sont les diviseurs de leur PGCD : $x \mid a$ et $x \mid b \Leftrightarrow x \mid \delta$ ou $\delta = \text{PGCD}(a\,;\,b)$.

Les multiples communs de deux nombres sont les multiples de leur PPMC : $x = ka$ et $x = k'b \Leftrightarrow x = k''\mu$ ou $\mu = \text{PPMC}(a\,,\,b)$.

$\delta = \text{PGCD}(a\,,\,b) \Leftrightarrow a = \delta\, a'$ et $b = \delta\, b'$ avec $\text{PGCD}(a'\,,\,b') = 1$ $\qquad$ **$\mu = \text{PPMC}(a\,,\,b) \Leftrightarrow \mu = k.a$ et $\mu = k'.b$ avec $\text{PGCD}(k\,,\,k') = 1$.**

$\text{PGCD} \times \text{PPMC} = \delta \times \mu = a \times b = \delta^2\, a'b' \Rightarrow$ **$\mu = \delta\, a'b'$** .

Théorème de Bézout Si deux entiers relatifs a , b admettent δ pour PGCD, il existe deux entiers relatifs u et v tels que : $au + bv = \delta$.

une démonstration possible est basée sur la *remontée à l'envers* de l'algorithme d'Euclide

$65 = 3\times18 + 11$, $18 = 1\times11 + 7$, $11 = 1\times7 + 4$, $7 = 1\times4 + \mathbf{3}$, $4 = 1\times3 + \mathbf{1}$, $3 = 3\times1 + 0$: PGCD$(65\,,\,18) = \mathbf{1}$ (premiers entre eux)

$\mathbf{1 = 4 - 1\times3}$, $\mathbf{3 = 7 - 1\times4} \Rightarrow 1 = 4 - (7 - 1\times4) \Rightarrow \mathbf{1} = -1\times7 + 2\times4$, $\mathbf{4 = 11 - 1\times7} \Rightarrow 1 = -1\times7 + 2(11 - 1\times7) \Rightarrow \mathbf{1} = 2\times11 - 3\times7$

$\mathbf{7 = 18 - 1\times11} \Rightarrow 1 = 2\times11 - 3(18 - 1\times11) \Rightarrow \mathbf{1} = -3\times18 + 5\times11 \Rightarrow \mathbf{11 = 65 - 3\times18} \Rightarrow 1 = -3\times18 + 5(65 - 3\times18) \Rightarrow 1 = 5\times65 - 18\times18$

***au + bv* = 1** $\Leftrightarrow$ $65u + 18v = 1$ $\Leftrightarrow$ **$(u\,;\,v) = (5\,;\,-18)$** : *Remarque* : **$au + bv = 1 \Leftrightarrow (a\,;\,b)$ premiers entre eux**

Théorème de Gauss **Si un nombre entier a divise exactement le produit bc , en étant premier avec b , alors il divise c :**

$a \mid bc$ et $\text{PGCD}(a\,;\,b) = 1 \Rightarrow a \mid c$.

Tout nombre premier est premier avec tout entier qu'il ne divise pas exactement : Si $x \mid bc$ et x premier, alors $x \mid b$ ou $x \mid c$.

Petit théorème de Fermat **p nombre premier et a entier naturel non divisible par $p \Rightarrow a^{p-1} - 1$ est divisible par p (soit $a^{p-1} \equiv 1\ [p]$).**

Vidéos **Maths et Tiques (Yvan MONKA)** : Cours PDF Exemple (1) Exemple (2) Exemple (3) Exemple (4) Exemple (5)

Exercices **JMedu** **Enoncés** e1220 e1815 e3702 e4251 e2550 **Corrigés** s1220 s1815 s3702 s4251 s2550