1. Plus grand commun diviseur

1.1 Diviseurs communs à deux entiers positifs

Pour tout entier naturel n, on note D(n) l'ensemble des diviseurs de n.

On note D(a; b) l'ensemble des diviseurs communs à a et b, c'est-à-dire $D(a; b) = D(a) \cap D(b)$.

Le plus grand élément de D(a; b) est appelé PGCD de a et b , noté PGCD(a; b).

Exemple: Le PGCD de 24 et 36 est 12; celui de 25 et 12 est 1.

Propriétés:

Pour tout entier naturel n, $D(n; 0) = D(n)$. En effet, $D(n; 0) = D(n) \cap \mathbb{N} = D(n)$.

$\text{PGCD}(a; b) \leqslant a$ et $\text{PGCD}(a; b) \leqslant b$. En effet, les diviseurs de a sont inférieurs à a , de même pour b.

Si b divise a, alors $\text{PGCD}(a; b) = b$. En effet, Si b divise a, $b \in D(a; b)$.

$\text{PGCD}(a; b) = \text{PGCD}(b; a)$.

$\text{PGCD}(a; 1) = 1$.

$\text{PGCD}(a; a) = a$.

Pour tout k entier naturel non nul, $\text{PGCD}(ka; kb) = k \times \text{PGCD}(a; b)$. Démonstration à l'aide de l'algorithme d'Euclide, vu juste après.

1.2 Recherche du PGCD : Algorithme d'Euclide:

a) Propriété : Soit $a = bq + r$ la division euclidienne de a par b . Alors $D(a; b) = D(b; r)$.

Si $r = 0$, alors $\text{PGCD}(a; b) = b$.

Si $r \neq 0$, alors $\text{PGCD}(a; b) = \text{PGCD}(b; r)$.

Démonstration : Soit c un diviseur commun de a et de b. Il existe deux entiers a' et b' tels que $a = ca'$ et $b = cb'$.
Si $a = bq + r$ est la division euclidienne de a par b , alors $r = a - bq = ca' - cb'q = c(a' - b'q)$, et c divise r, donc est un diviseur commun de b et de r. Ainsi $D(a; b) \subset D(b; r)$.

Réciproquement, soit d un diviseur commun de b et de r. Il existe deux entiers b' et r' tels que $b = db'$ et $r = dr'$.
Si $a = bq + r$ est la division euclidienne de a par b , alors $a = db'q + dr' = d(b'q + r')$, et d divise a, donc est un diviseur commun de a et de b. Ainsi $D(b; r) \subset D(a; b)$.

Finalement, $D(a; b) = D(b; r)$, et $\text{PGCD}(a; b) = \text{PGCD}(b; r)$.

b) Algorithme d'Euclide:

Pour rechercher le PGCD de a et de b, on effectue les divisions euclidiennes successives :
$a = bq + r$ avec $0 \leqslant r < b$; puis $b = rq_1 + r_1$ avec $0 \leqslant r_1 < r$; puis $r = r_1 q_2 + r_2$ avec $0 \leqslant r_2 < r_1$; etc... jusqu'à ce que le reste soit nul. Alors le PGCD de a et de b est le dernier reste non nul.

Exemple : On cherche PGCD(48; 63) : On a successivement :

$63 = 1 \times 48 + 15$, puis $48 = 3 \times 15 + 3$, puis $15 = 5 \times 3 + 0$. Donc $\text{PGCD}(48; 63) = 3$.

c) Propriété : $D(a; b) = D(g)$ où g est le PGCD de a et de b.

2. Nombres premiers entre eux

Définition: Soient a et b deux entiers naturels non nuls.

On dit que a et b sont premiers entre eux si $\text{PGCD}(a; b) = 1$.

Propriété: Soit a un entier naturel non nul. Si p est un nombre premier qui ne divise pas a, alors a et p sont premiers entre eux.

Soient a et b deux entiers naturels non nuls et d leur PGCD. Alors $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

3. Théorème de Bezout :

Théorème : Soient a et b deux entiers relatifs non nuls.
a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que $au + bv = 1$.
Démonstration : Supposons a et b sont premiers entre eux; considérons l'ensemble E des nombres $au + bv$ avec u et v entiers relatifs. E contient des entiers naturels non nuls : si a l'est, E contient $a = a\times 1 + b\times 0$. si a est négatif, E contient $-a = a\times(-1) + b\times 0$. Donc E contient un plus petit entier naturel $m = au_1 + bv_1$. Montrons que m divise a et b: La division de a par m donne $a = mq + r = (au_1 + bv_1)q + r$, avec $0 \leqslant r < m$.
Or $r = (au_1 + bv_1)q - a = a(u_1q - 1) + b(v_1q)$ de la forme $au + bv$. Comme m est le plus petit entier naturel de la forme $au + bv$, alors $r = 0$. Donc m divise a. De la même manière, m divise b. Or a et b sont premiers entre eux, donc $m = 1$.
Supposons qu'il existe des entiers relatifs u et v tels que $au + bv = 1$. Le pgcd$(a; b) = g$ divise a et b et tout nombre de la forme $au + bv$. Donc $g = 1$, et a et b sont premiers entre eux.

Corollaire: Soient a et b deux entiers relatifs et d leur PGCD. Alors il existe des entiers relatifs u et v tels que $au + bv = d$.

4. Théorème de Gauss :

Théorème : Soient a et b deux entiers relatifs non nuls et c un entier relatif. Si a divise bc et si a est premier avec b alors a divise c.
Démonstration : Comme a et b sont premiers entre eux, il existe des entiers relatifs u et v tels que $au + bv = 1$. Donc $auc + bvc = c$. Or a divise auc et divise bc, donc a divise $auc + bvc = c$.

Corollaires:

- Si un entier relatif c est divisible par deux entiers a et b premiers entre eux, alors c est divisible par le produit ab.
- Si un nombre premier p divise le produit ab, alors il divise au moins l'un des facteurs a et b.

5. Plus petit commun multiple

2.1 Multiples communs à deux entiers positifs

Pour tout entier naturel n, on note M(n) l'ensemble des multiples de n. M$(n) = \{k\ ,\ k = nq$ avec $q \in \mathbb{Z}\ \}$.
On note M$(a; b)$ l'ensemble des multiples communs à a et b, c'est-à-dire M$(a; b)$ = M$(a) \cap$ M(b).
Le plus petit élément de M$(a; b)$ est appelé PPCM de a et b , noté PPCM$(a; b)$.
Exemple: Le PPCM de 24 et 36 est 72; celui de 25 et 12 est 300.

2.2 Propriétés : Le PGCD$(a; b)$ divise le PPCM$(a; b)$.
PGCD$(a; b) \times$ PPCM$(a; b) = ab$.
Pour tout k entier naturel non nul, PPCM$(ka; kb) = k \times$PPCM$(a; b)$.
M$(a; b)$ = M(PPCM$(a ; b)$).