PGCD	
Théorème1	Soit a un entier relatif et b un entier naturel. Soit (q,r) le couple issu de la division euclidienne de a par b tel que $a = bq + r$ avec $r < b$. Alors $div(a) \cap div(b) = div(b) \cap div(r)$

Preuve

Soit $p \in div(a) \cap div(b)$. $a = pa'$ et $b = pb'$
Donc $a = bq + r \Longrightarrow pa' = pb'q + r \Longrightarrow p(a' - b'q) = r \Longrightarrow p \in div(r) \Longrightarrow p \in div(b) \cap div(r) \Longrightarrow$
$$div(a) \cap div(b) \subset div(b) \cap div(r)$$
Réciproquement si $p \in div(b) \cap div(r)$. $r = pr'$ et $b = pb'$
Donc $a = bq + r \Longrightarrow a = pb'q + pr' \Longrightarrow a = p(b'q + r') \Longrightarrow p \in div(a) \Longrightarrow p \in div(b) \cap div(a) \Longrightarrow$
$$div(b) \cap div(r) \subset div(a) \cap div(b)$$
En résumé $div(a) \cap div(b) = div(b) \cap div(r)$

Exemple	$28 = 2 * 12 + 4$ donc $div(28) \cap div(12) = div(12) \cap div(4)$. Je vous propose de le vérifier
Théorème2	Soient a et b deux entiers relatifs. Alors il existe un entier naturel d unique tel que $$div(a) \cap div(b) = div(d)$$ Ce nombre est appelé PGCD de a et de b et se note $a \wedge b$

Preuve

La preuve de ce théorème s'appuie sur l'algorithme d'euclide.
Nous nous restreignons pour l'instant au cas où $a > b \geq 0$.

Montrons d'abord l'existence d'un tel nombre.

Nous avons avons vu que si (q,r) est le couple issu de la division euclidienne de a par b $(a = bq + r)$
Alors $div(a) \cap div(b) = div(b) \cap div(r)$
Notons (r_0, r_1) le couple (a,b).
Notons aussi $q_2$et r_2 tels que $a = bq_2 + r_2$ et $div(a) \cap div(b) = div(b) \cap div(r_2)$ soit
$$div(r_0) \cap div(r_1) = div(r_1) \cap div(r_2)$$

L'algorithme d'euclide nous propose de réitérer l'opération et de réaliser la division euclidienne de b par r_2

$b = r_2q_3 + r_3$ avec $0 \leq r_3 < r_2$ et $div(b) \cap div(r_2) = div(r_2) \cap div(r_3)$ soit :
$$div(r_1) \cap div(r_2) = div(r_2) \cap div(r_3)$$
Et ainsi de suite …..
$r_2 = r_3 * q_4 + r_4$ avec $0 \leq r_4 < r_3$ et $div(r_2) \cap div(r_3) = div(r_3) \cap div(r_4)$

Nous obtenons donc une famille $(q_2, q_3, q_4 \ldots)$ et une famille $(r_0, r_1, r_2 \ldots)$ telle que $0 \leq r_{n+1} < r_n$. La famille (r_n) étant strictement décroissante et minorée par 0 nous avons l'existence d'un entier N tel que $r_N = 0$

D'après le théorème1 :
$div(a) \cap div(b) = div(b) \cap div(r_2) \Leftrightarrow div(r_0) \cap div(r_1) = div(r_1) \cap div(r_2) = \cdots div(r_{N-1}) \cap div(r_N) = div(r_{N-1}) \cap div(0) = div(r_{N-1})$

En posant $r_{N-1} = d$ nous avons donc prouvé l'existence de ce nombre.
Montrons maintenant l'unicité.
Si $div(d) = div(d')$ alors nous en déduisons que $d \mid d'$ et $d' \mid d$ donc $d' = \mp d$.
Or d et d' sont des entiers naturels donc $d = d'$. L'unicité est ainsi montrée.

Il reste à élargir la démonstration au cas où $b = a$. Dans ce cas, c'est évident $d = b = a$
Dans le cas où $b > a \geq 0$. Il suffit d'inverser la démonstration et de faire la division euclidienne de b par a. Nous arriverons au même résultat.
Dans le cas où b ou a seraient négatifs la relation $div(b) = div(-b)$ et $div(a) = div(-a)$ nous permet de réétablir cette demonstration sur des nombres positifs et donc de conclure.

Exemple	Grâce à l'algorithme d''euclide trouvons le PGCD de 1071 et 462 $1071 = 2 \times 462 + 147$ $462 = 3 \times 147 + 21$ $147 = 7 \times 21 + 0$ Donc $PGCD(1071, 462) = 21$
Théorème3	Le théorème2 s'étend à une liste finie d'entiers relatifs. Soient $a_1, a_2 \dots a_n$ n entiers relatifs. Alors Il existe un entier naturel d unique tel que $div(a_1) \cap div(a_2) \dots \cap div(a_n) = div(d)$. Ce nombre est appelé PGCD de $a_1, a_2 \dots a_n$ et se note $a_1 \Lambda a_2 \dots \Lambda a_n$

Preuve

L'existence se montre par récurrence sur n :

- Si $n = 2$ nous l'avons déjà démontré
- Supposons l'hypothèse de récurrence valable pour $n = p$ et démontrons la pour $n = p + 1$
  $div(a_1) \cap div(a_2) \dots \cap div(a_{p+1})$
  $= \{div(a_1) \cap div(a_2) \dots \cap div(a_p)\} \cap div(a_{p+1})$
  $= div(a_1 \Lambda a_2 \dots \Lambda a_p) \cap div(a_{p+1})$ (Application de l'hypothèse de récurrence)
  $= div\left[(a_1 \Lambda a_2 \dots \Lambda a_p) \Lambda a_{p+1}\right]$ (Application du théorème dans le cas de 2 entiers relatifs)

Donc le nombre $(a_1 \Lambda a_2 \dots \Lambda a_p) \Lambda a_{p+1}$ soit $a_1 \Lambda a_2 \dots \Lambda a_p \Lambda a_{p+1}$ convient très bien. L'existence est démontrée. L'unicité se démontre de la même manière que le théorème2.

Propriété	Factorisation du PGCD Soient $a_1, a_2 \dots a_n, k \quad n + 1$ entiers relatifs. Alors $(ka_1 \Lambda ka_2 \dots \Lambda ka_n) = k(a_1 \Lambda a_2 \dots \Lambda a_n)$
Preuve	$(ka_1 \Lambda ka_2 \dots$ $\Lambda ka_n) = div(ka_1) \cap div(ka_2) \dots \cap div(ka_n) = k\, div(a_1) \cap div(a_2) \dots \cap div(a_n) = kdiv(a_1 \Lambda a_2 \dots \Lambda a_n)$
Exemple	$12 \Lambda 18 = 6(2 \Lambda 3) = 6$