I - Algorithme d'Euclide

Définition 1 : PGCD de deux entiers

Soient a et b deux entiers relatifs non simultanément nuls.
Le **plus grand diviseur commun de a et b** et le plus grand élément de l'ensemble des diviseurs communs à a et b. Il est noté $\text{PGCD}(a;b)$.

Remarque

On utilise implicitement le résultat fondamental suivant : "Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément".

Propriété 1 : propriétés du PGCD

Soient a et b deux entiers relatifs non simultanément nuls. Alors

1. $\text{PGCD}(a;b) = \text{PGCD}(|a|;|b|)$
2. et, pour tout couple $(a;b) \in \mathbb{N}^2$ où $a \neq 0$,
   (a) $\text{PGCD}(a;b) \geq 1$, $\text{gcd}(0;a) = a$, $\text{PGCD}(1;a) = 1$
   (b) $a|b \iff \text{PGCD}(a;b) = a$
   (c) $\text{PGCD}(a;b) = \text{PGCD}(a-b;b)$

Exemples

— $\text{gcd}(12;18) = 6$
— $\text{gcd}(229;225) = \text{gcd}(229-225;225) = \text{gcd}(4;225) = 1$

Propriété 2 : Lemme d'Euclide

Si a et b sont deux entiers naturels non nuls avec $a > b$ alors

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

où r est le reste de la division euclidienne de a par b.

Démonstration :

— Soit d un diviseur commun à a et b. Ainsi $a = bq + r$, où q est le quotient de la division euclidienne, et donc $r = a - bq$. r s'écrit comme une combinaison linéaire à coefficients entiers de a et b et de plus d divise a et b donc d divise r. Autrement dit d est un diviseur commun à b et r.
— De même, a est une combinaison linéaire de b et r, donc tout diviseur commun à b et r divise a.

Finalement, l'ensemble des diviseurs communs à a et b est confondu avec l'ensemble des diviseurs communs à b et r. Ils ont donc le même plus grand élément, d'où $\text{PGCD}(a;b) = \text{PGCD}(b;r)$.

Exemple

$546 = 60 \times 9 + 6$ donc $\text{PGCD}(546;60) = \text{PGCD}(60;6) = 6$

Propriété 3 : Algorithme d'Euclide

Soient a et b deux entiers naturels tels que $0 < b \leq a$.

1. Calculer le reste r de la division euclidienne de a par b.
2. — Si $r = 0$ alors $\text{PGCD}(a;b) = b$
   — Sinon remplacer a par b et b par r puis revenir en 1.

Exemple

$1551 = 11 \times 132 + 99$
$132 = 1 \times 99 + 33$
$99 = 3 \times 33 + 0$

donc $\text{PGCD}(1551;132) = 33$.

Propriété 4 : Corollaires de l'algorithme d'Euclide

1. Pour tous entiers naturels non nuls a, b et k on a

$$\text{PGCD}(ka;kb) = k \times \text{PGCD}(a;b)$$

2. Pour tous entiers a et b non simultanément nuls

$$d \text{ est un diviseur commun à } a \text{ et } b \iff d \mid \text{PGCD}(a;b)$$

II - Entiers premiers entre eux

Définition 2 : Entiers premiers entre eux

On dit que deux entiers relatifs non nuls a et b sont **premiers entre eux** lorsque $\text{PGCD}(a;b) = 1$.

Exemple

$\text{PGCD}(13;6) = 1$ donc 13 et 6 sont premiers entre eux.

Propriété 5 : Factorisations et entiers premiers entre eux

Soient a et b deux entiers naturels non nuls.

$d = \text{PGCD}(a;b)$ si et seulement si il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Remarque

Cette propriété implique l'existence pour tout nombre rationnel d'une forme irréductible $\frac{a}{b}$ où a et b sont premiers entre eux.

Démonstration :

— d divise a et b donc il existe deux entiers relatifs a' et b' tels que $a = da'$ et $b = db'$. $d = \text{PGCD}(a;b) = \text{PGCD}(da';db') = d \times \text{PGCD}(a';b')$, donc $\text{PGCD}(a';b') = 1$ car $a \neq 0$.

— Réciproquement, si $\text{PGCD}(a';b') = 1$ alors $\text{PGCD}(a;b) = \text{PGCD}(da';db') = d \times \text{PGCD}(a';b') = d$.

III - Théorème de Bézout

Propriété 6 : Identité de Bézout

Soient a et b deux entiers relatifs non nuls.

Il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + bv = \text{PGCD}(a;b)$

Remarques

1. La réciproque est fausse : $3 \times 2 - 2 \times 2 = 2$ mais $\text{PGCD}(3;2) \neq 2$!
2. u et v ne sont pas uniques.

Exemple

1. $\text{PGCD}(6;15) = 3$ et $3 = 6 \times \underbrace{3}_{u} + 15 \times \underbrace{(-1)}_{v} = 15 \times \underbrace{3}_{u} + 6 \times \underbrace{(-7)}_{v}$
2. $\text{PGCD}(22;15) = 1$ et $1 = 15 \times \underbrace{3}_{u} + 22 \times \underbrace{(-2)}_{v}$

Méthode : Comment déterminer u et v ?

Déterminons deux entiers u et v tels que $38u + 15v = 1$.

1. On applique l'algorithme d'Euclide et on isole les restes obtenus :

$38 = 2 \times 15 + 8$	$8 = 38 - 2 \times 15$
$15 = 1 \times 8 + 7$	$7 = 15 - 1 \times 8$
$8 = 1 \times 7 + 1$	$1 = 8 - 1 \times 7$
$7 = 7 \times 1 + 0$	

2. On "remonte" l'algorithme d'Euclide en partant du dernier reste non nul :

$$\begin{aligned} 1 &= 8 - 1 \times 7 = 8 - 1(15 - 1 \times 8) \\ &= 2 \times 8 - 1 \times 15 = 2 \times (38 - 2 \times 15) - 1 \times 15 \\ &= 2 \times 38 - 5 \times 15 \end{aligned}$$

Ainsi le couple $(u;v) = (2;-5)$ convient.

Propriété 7 : Théorème de Bézout

Deux entiers naturels a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que

$$\boxed{au + bv = 1}$$

Démonstration :

— Si a et b sont premiers entre eux alors d'après la propriété précédente, il existe u et v tels que $au + bv = \text{PGCD}(a;b) = 1$.

— Réciproquement, si $au + bv = 1$ alors $d = \text{PGCD}(a;b)$ divise a et b et donc divise $au + bv$ qui est égal à 1. Ainsi $d = 1$ et a et b sont premiers entre eux.

IV - Théorème de Gauß

Propriété 8 : Théorème de Gauss

Soient a, b et c trois entiers naturels.

Si a divise bc et si a est premier avec b, alors a divise c.

Démonstration : Si a divise bc alors il existe $q \in \mathbb{N}$ tel que $bc = aq$. De plus $\text{PGCD}(a;b) = 1$ donc d'après le théorème de Bézout il existe deux entiers relatifs u et v tels que $au+bv = 1$. Ainsi $c = cau + cbv = acu + aqv = a(cu + qv)$ d'où $c = a\underbrace{(cu + qv)}_{\in\mathbb{Z}}$ donc a divise c.

Exemple

Soit n un diviseur impair de $210 = 105 \times 2$. Comme n est premier avec 2, le théorème de Gauss nous affirme que n divise 105.

Propriété 9 : Corollaire du théorème de Gauss

Soient a, b et c trois entiers relatifs non nuls.

Si a et b divisent c et sont premiers entre eux, alors ab divise c.

Démonstration : Puisque a divise c, il existe $k \in \mathbb{Z}$ tel que $c = ak$. Puisque b divise c, il existe $k' \in \mathbb{Z}$ tel que $c = bk'$.
On en déduit que $ak = bk'$, d'où a divise bk'. Or a et b sont premiers entre eux par hypothèse donc d'après le théorème de Gauß, a divise k'.
Il existe donc $k" \in \mathbb{Z}$ tel que $k' = ak"$ et donc $c = bk' = bak"$, donc ab divise c.

Exemple

Soit $n \in \mathbb{N}^*$. $n(n^2-1) = (n-1)n(n+1)$ est le produit de trois entiers consécutifs donc $n(n^2-1)$ est divisible par 2 et 3. Puisque 2 et 3 sont premiers entre eux, d'après le corollaire ci-dessus $n(n^2-1)$ est divisible par 6.

V - Résolution d'équations diophantiennes

Définition 3 : Équation diophantienne

Soient a et b deux entiers non nuls et c un entier quelconque.
Une **équation diophantienne** est une équation de la forme $\boxed{ax + by = c}$, d'inconnues entières x et y.

Exemple

$12x+4y = 32$ est une équation diophantienne d'inconnues x et y. D'un point de vue géométrique : étant donnée une droite du plan, on cherche les points de **coordonnées entières** appartenant à celle-ci.

Méthode : Résolution d'une équation diophantienne

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

   On sait d'après le théorème de Bézout qu'il existe au moins une solution qu'on peut obtenir grâce à l'algorithme d'Euclide.

   Par exemple, l'équation $390x + 104y = 26$ admet comme solution particulière $(x;y) = (-1;4)$. Si $(x;y)$ est une solution on obtient :

   $$\begin{cases} 390x + 104y &= 26 \\ 390 \times (-1) + 104 \times 4 &= 26 \end{cases}$$

   Donc, en soustrayant ces deux lignes, $390(x+1) + 104(y-4) = 0$ et en divisant par $\text{PGCD}(390;104) = 26$, $15(x+1) = 4(-y+4)$.

   15 et 4 sont premiers entre eux, donc d'après le théorème de Gauß, 15 divise $-y+4$ autrement dit il existe $k \in \mathbb{Z}$ tel que $y = 4 - 15k$.

   On obtient

   $$\begin{aligned} 15(x+1) = 4(-4+15k+4) &\iff 15(x+1) = 4 \times 15k \\ &\iff x = 4k-1 \end{aligned}$$

   Pour résumer, si $(x;y)$ est solution alors $x = -1+4k$ et $y = 4-15k$ avec k entier relatif.

   Réciproquement, on vérifie que les couples de la forme $(-1+4k;4-15k)$ avec k entier relatif sont solutions.

   Finalement, l'ensemble S des solutions est

   $$S = \{(-1+4k;4-15k), k \in \mathbb{Z}\}$$

2. Lorsque c est un multiple de $\text{PGCD}(a;b)$.

   Prenons par exemple $390x + 104y = 52 = 2 \times \text{PGCD}(390;104)$. On cherche une solution particulière à $390x + 104y = \text{PGCD}(390;104)$. On a vu que $(-1;4)$ convient. Ainsi,

   $$390 \times (-1) + 104 \times 4 = 26 \iff 390 \times (-2) + 104 \times 8 = 52$$

   Si $(x;y)$ est une solution, on obtient :

   $$\begin{cases} 390x + 104y &= 52 \\ 390 \times (-2) + 104 \times 8 &= 52 \end{cases}$$

   et de nouveau en soustrayant les deux lignes, $390(x+2)+104(y-8) = 0$ et en divisant par $\text{PGCD}(390;104) = 26$ puis en appliquant le théorème de Gauß, $x = -2+4k$ et $y = 8-15k$ où k est un entier relatif.

   Réciproquement, on vérifie que que l'ensemble des solutions est

   $$S = \{(-2+4k;8-15k), k \in \mathbb{Z}\}$$

3. Lorsque c n'est pas un multiple de $\text{PGCD}(a;b)$, l'équation n'a pas de solution.

   En effet, s'il existe une solution $(x;y)$ alors $d = \text{PGCD}(a;b)$ divise a et b donc divise $ax+by$ et donc d divise c, ce qui est contradictoire.