

LEÇON N° 11 :

PGCD de deux entiers naturels. Nombres premiers entre eux. Applications. L'exposé pourra être illustré par un ou des exemples faisant appel à l'utilisation d'une calculatrice.

Pré-requis :

- \mathbb{Z} ainsi que la division euclidienne dans \mathbb{Z} ;
- \mathbb{Z} est un anneau principal (i.e. intègre dont tous les idéaux sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$).

11.1 PGCD de deux entiers relatifs

11.1.1 Définition et propriétés

Soient $a, b \in \mathbb{Z}$. Il existe $\delta \in \mathbb{Z}$ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$. L'entier relatif δ n'est pas unique, mais $\delta\mathbb{Z} = \delta'\mathbb{Z} \Leftrightarrow \delta' = \pm\delta$, de sorte que l'on puisse définir :

Définition 1 : Le plus grand commun diviseur (PGCD) de a et b est l'unique entier positif δ qui vérifie $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$. On le note

$$\delta = \text{PGCD}(a, b) = a \wedge b.$$

Théorème 1 : Soient $\delta \in \mathbb{N}$ et $a, b, d \in \mathbb{Z}$. On a :

$$\delta = \text{PGCD}(a, b) \Leftrightarrow (d|\delta \Leftrightarrow d|a \text{ et } d|b) \Leftrightarrow \begin{cases} \delta \text{ divise } a \text{ et } b & (\alpha) \\ d|a \text{ et } d|b \Rightarrow d|\delta & (\beta) \end{cases}$$

démonstration : La seconde équivalence est triviale. Montrons la première : si $\delta = \text{PGCD}(a, b)$,

$$d|\delta \Leftrightarrow \delta\mathbb{Z} \subset d\mathbb{Z} \Leftrightarrow a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z} \Leftrightarrow a\mathbb{Z} \subset d\mathbb{Z} \text{ et } b\mathbb{Z} \subset d\mathbb{Z} \Leftrightarrow d|a \text{ et } d|b.$$

Réciproquement, si $(d|\delta \Leftrightarrow d|a \text{ et } d|b)$, notons $\delta_0 = \text{PGCD}(a, b)$. Le sens direct montre que $(d|\delta_0 \Leftrightarrow d|a \text{ et } d|b)$, de sorte que $(d|\delta \Leftrightarrow d|\delta_0)$ et que l'on ait simultanément $\delta_0|\delta$ (en effet, $\delta_0|a$ et $\delta_0|b$, donc par hypothèse, $\delta_0|\delta$) et $\delta|\delta_0$. Cela prouve que $\delta = \delta_0$, puisque δ et δ_0 appartiennent à \mathbb{N} . ■

Remarques :

La relation $|$ est une relation de préordre sur \mathbb{Z} car elle est réflexive et transitive, et les conditions (α) et (β) montrent que δ (comme $-\delta$) est "une" borne inférieure de la partie de $\{a, b\}$ de \mathbb{Z} pour la relation $|$. Cette borne inférieure n'est pas unique dans \mathbb{Z} car la relation $|$ n'est pas antisymétrique. Cependant, l'unicité de la borne inférieure δ est acquise si l'on se place dans \mathbb{N} , la relation $|$ devenant alors une relation d'ordre dans \mathbb{N} .

Si l'on choisit des entiers naturels a et b non simultanément nuls, alors $\delta = \text{PGCD}(a, b)$ n'est pas nul et vérifie

$$\begin{cases} \delta \text{ divise } a \text{ et } b \\ d|a \text{ et } d|b \Rightarrow d|\delta \Rightarrow d \leq \delta. \end{cases}$$

δ est donc aussi le plus grand élément de l'ensemble des diviseurs communs à a et b pour la relation d'ordre usuelle \leq dans \mathbb{N} , ce qu'on écrit $\delta = \max\{d \in \mathbb{N}/d|a \text{ et } d|b\}$. La dénomination « plus grand commun diviseur » peut ainsi être comprise indifféremment pour la relation d'ordre $|$ dans \mathbb{N} ou pour la relation habituelle \leq .

Théorème 2 : A multiplication près par un élément inversible,

1. $\forall a, b \in \mathbb{Z}, \quad a \wedge b = b \wedge a \quad (\text{comutativité du PGCD})$;
2. $\forall a, b, x \in \mathbb{Z}, \quad (xa) \wedge (xb) = x(a \wedge b)$;
3. $\forall a, b, c \in \mathbb{Z}, \quad (a \wedge b) \wedge c = a \wedge (b \wedge c) \quad (\text{associativité du PGCD})$.

démonstration : 1. est trivial. Les assertions 2. et 3. proviennent de

$$(xa)\mathbb{Z} + (xb)\mathbb{Z} = x[a\mathbb{Z} + b\mathbb{Z}] = x[(a \wedge b)\mathbb{Z}] = (x(a \wedge b))\mathbb{Z}$$

et

$$((a \wedge b) \wedge c) = (a \wedge b) + (c) = (a) + (b) + (c) = (a) + (b \wedge c) = (a \wedge (b \wedge c)),$$

où (a) représente l'idéal $a\mathbb{Z}$. ■

11.1.2 Calcul pratique du PGCD

• **Algorithme d'Euclide** : Supposons $a \geq b$. Si $b = 0$, $a \wedge 0 = a$. Sinon écrivons les divisions euclidiennes suivantes :

$$\left\{ \begin{array}{ll} a = bq + r & 0 \leq r < b \\ b = r_1q_1 + r_1 & 0 \leq r_1 < r \\ r = r_1q_2 + r_2 & 0 \leq r_2 < r_1 \\ \vdots & \vdots \\ r_k = r_{k+1}q_{k+2} + r_{k+2} & 0 \leq r_{k+2} < r_{k+1}. \\ \vdots & \vdots \end{array} \right.$$

Si l'on avait $r_k \neq 0$ pour tout k , on construirait une suite (r_k) strictement décroissante d'entiers naturels, ce qui est impossible. Le reste r_k s'annule donc au bout d'un nombre fini d'itérations, et l'on obtient ainsi :

$$\left\{ \begin{array}{ll} \vdots & \vdots \\ r_{n-2} = r_{n-1}q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1} & r_{n+1} = 0. \end{array} \right.$$

On remarque que $a \wedge b = b \wedge r = r \wedge r_1 = \dots = r_n \wedge 0 = r_n$. Ainsi, le PGCD de a et b est le dernier reste non nul obtenu dans l'algorithme.

Exemple : $\text{PGCD}(168, 98) = 14$ puisque

$$168 = 98 \times 1 + 70, \quad 98 = 70 \times 1 + 28, \quad 70 = 28 \times 2 + 14, \quad 28 = 14 \times 2 + 0.$$

• **Factorialité de \mathbb{Z} :** Si $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $b = p_1^{\beta_1} \dots p_n^{\beta_n}$, où les p_i sont des nombres premiers distincts (quelques α_i ou β_i pouvant être nuls), on vérifie que

$$\text{PGCD}(a, b) = p_1^{\inf(\alpha_1, \beta_1)} \dots p_n^{\inf(\alpha_n, \beta_n)}.$$

11.1.3 Nombres premiers entre eux

Définition 2 : Les entiers a et b sont dits *premiers entre eux* si $a \wedge b = 1$.

Théorème 3 (Théorème de Bézout) : Les entiers a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

démonstration : $a \wedge b = 1 \Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \Leftrightarrow \exists u, v \in \mathbb{Z}, au + bv = 1$. ■

Corollaire 1 : Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$.

démonstration : Le théorème de Bézout montre l'existence de quatre entiers relatifs u, v, u', v' tels que $au + bv = 1$ et $au' + cv' = 1$. Par multiplication des deux égalités, on en déduit que $a(auu' + ucv' + u'bv) + (bc)vv' = 1$, de sorte que a et bc sont bien premiers entre eux. ■

Théorème 4 (Théorème de Gauss) : Si a divise bc et si a est premier avec b , alors a divise c .

démonstration : $au + bv = 1$ entraîne $auc + bvc = c$ et puisque $a|b$, a divise le premier membre égal à c . ■

Corollaire 2 : Si $b_1 \wedge b_2 = 1$, si $b_1|a$ et si $b_2|a$, alors $b_1b_2|a$.

démonstration : Il existe $u \in \mathbb{Z}$ tel que $a = b_1u$. Par le théorème de Gauss, $b_2|u$, donc il existe un entier relatif v tel que $u = b_2v$, et l'on obtient $a = b_1b_2v$, donc $b_1b_2|a$. ■

11.2 Equation diophantienne $ax + by = c$

11.2.1 Principe de résolution

On désire obtenir toutes les solutions entières de l'équation $ax + by = c$, où $(a, b, c) \in \mathbb{Z}^3$.

• S'il existe une solution $(x, y) \in \mathbb{Z}^2$, et si $\delta = a \wedge b$, alors $\delta | c$. Par conséquent, si δ ne divise pas c , l'équation ne possède aucune solution dans \mathbb{Z}^2 .

• Supposons maintenant que $\delta | c$. En notant $a = \delta a'$, $b = \delta b'$ et $c = \delta c'$, on se ramène à

$$a'x + b'y = c', \quad \text{où } a' \wedge b' = 1.$$

• Résolvons donc l'équation $ax + by = c$, où $a \wedge b = 1$. La connaissance d'une solution particulière de cette équation nous permet de trouver toutes les autres solutions. Supposons en effet que (x_0, y_0) vérifie $ax_0 + by_0 = c$. Alors

$$ax + by = c \Leftrightarrow ax + by = ax_0 + by_0 \Leftrightarrow a(x - x_0) = b(y_0 - y). \quad (11.1)$$

Donc a divise $b(y_0 - y)$ et a est premier avec b , donc a divise $y_0 - y$ d'après le théorème de Gauss. Il existe ainsi $u \in \mathbb{Z}$ tel que $y_0 - y = au$, et par suite, $x - x_0 = bu$. Réciproquement, si $y_0 - y = au$ et $x - x_0 = bu$, alors (x, y) vérifie (11.1). En conclusion,

$$ax + by = c \Leftrightarrow \exists u \in \mathbb{Z}, \begin{cases} x = x_0 + bu \\ y = y_0 - au. \end{cases}$$

11.2.2 Recherche d'une solution particulière : algorithme d'Euclide étendu

Une solution de l'équation $ax + by = 1$ existe d'après le théorème de Bézout puisque l'on suppose $a \wedge b = 1$. Voyons la méthode sur un exemple : cherchons une solution particulière de $385x + 156y = 1$. L'algorithme d'Euclide nous donne

Dividende	Diviseur	Reste	Quotient	Relation
385	156	73	2	$73 = a - 2b$
156	73	10	2	$10 = b - 2 \times 73 = b - 2(a - 2b) = -2a + 5b$
73	10	3	7	$3 = 73 - 7 \times 10 = (a - 2b) - 7(-2a + 5b) = 15a - 37b$
10	3	1	3	$1 = 10 - 3 \times 3 = (-2a + 5b) - 3(15a - 37b) = -47a + 116b$
3	1	0	3	

Pour démontrer ce procédé par récurrence et le systématiser, reprenons les notations de l'algorithme d'Euclide :

$$\left\{ \begin{array}{l} a = bq + r \\ b = r_1q_1 + r_1 \\ r = r_1q_2 + r_2 \\ \vdots \\ r_k = r_{k+1}q_{k+2} + r_{k+2} \\ \vdots \\ r_{n-2} = r_{n-1}q_n + r_n \\ r_{n-1} = r_nq_{n+1}. \end{array} \right. \quad (*)$$

On sait que $r_n = \text{PGCD}(a, b)$. Posons $r_k = au_k + bv_k$.

* Premier pas : $a = bq + r$ entraîne $r = r_0 = a - bq$. On choisit $(u_0, v_0) = (1, -q)$.

* Deuxième pas : $b = r_0q_1 + r_1$ entraîne $r_1 = b - (au_0 + bv_0)q_1 = a(-u_0q_1) + b(1 - v_0q_1)$. On choisit $(u_1, v_1) = (-u_0q_1, 1 - v_0q_1)$.

* Troisième pas : $r_0 = r_1q_2 + r_2$ entraîne

$$\begin{aligned} r_2 &= r_0 - r_1q_2 = (au_0 + bv_0) - (au_1 + bv_1)q_2 \\ &= a(u_0 - u_1q_2) + b(v_0 - v_1q_2). \end{aligned}$$

* A chaque pas de calcul, on détermine q_k et r_k , mais aussi le couple

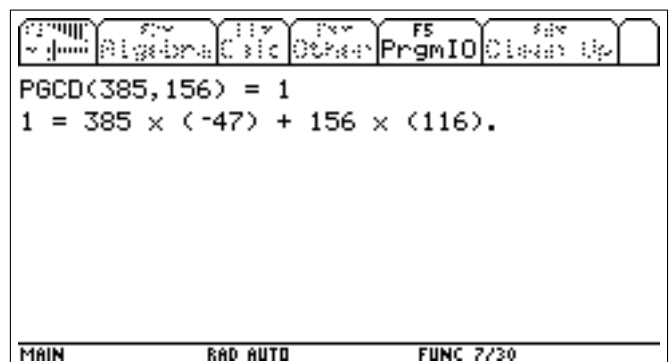
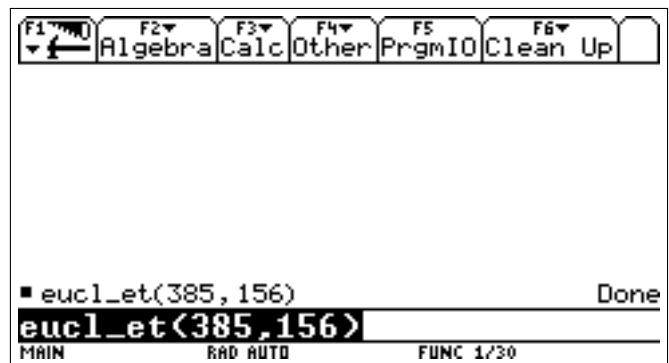
$$(u_k, v_k) = (u_{k-2} - u_{k-1}q_k, v_{k-2} - v_{k-1}q_k).$$

Programme sur la calculatrice TI Voyage 200

À gauche, le programme et à droite, le résultat affiché pour l'exemple précédent :

```

F1 F2 F3 F4 F5 F6
Control I/O Var Find... Mode
:eucl_et(n,p)
:Prgm
:Local a,b,q,r,u,v,i
:ClrIO:n→a[1]:p→b[1]
:
:mod(a[1],b[1])→r[1]
:int(a[1]/(b[1]))→q[1]
:1→u[1]:-q[1]→v[1]
:
:If mod(b[1],r[1])=0 Then
:  Goto 11
:EndIf
:b[1]→a[2]:r[1]→b[2]
:mod(a[2],b[2])→r[2]
:int(a[2]/(b[2]))→q[2]
:-q[2]*u[1]→u[2]:1-q[2]*v[1]→v[2]
:
:3→i
:While mod(b[i-1],r[i-1])≠0
:  b[i-1]→a[i]:r[i-1]→b[i]
:  mod(a[i],b[i])→r[i]
:  int(a[i]/(b[i]))→q[i]
:  u[i-2]-q[i]*u[i-1]→u[i]
:  v[i-2]-q[i]*v[i-1]→v[i]
:  i+1→i
:EndWhile
:Lbl 11
:Disp "PGCD("&string(a[1])&","&string(b[1])&") = "&string(r[i-1])
:Disp string(r[i-1])& " = "&string(a[1])&
" x ("&string(u[i-1])&") + "&string(b[1])&
" x ("&string(v[i-1])&")."
:
:EndPrgm
MAIN RAD AUTO FUNC
  
```



11.2.3 Interprétation géométrique

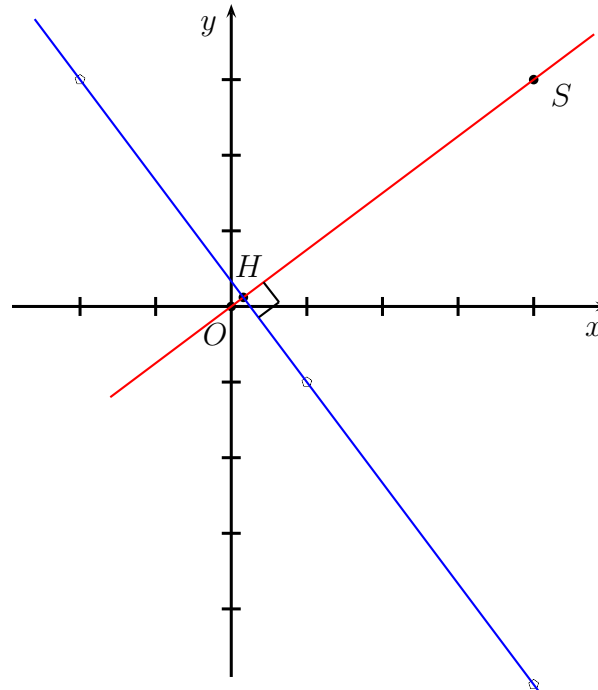
Rapportons le plan euclidien à un repère orthonormé d'origine O . Notons S le point de coordonnées (a, b) et M un point de coordonnées (x, y) . On a alors

$$ax + by = 1 \Leftrightarrow \overrightarrow{OM} \cdot \overrightarrow{OS} = 1.$$

L'unique point H de la droite (OS) vérifiant $\overrightarrow{OH} \cdot \overrightarrow{OS} = 1$ est donné par $\overrightarrow{OH} = \overrightarrow{OS}/OS^2$, donc

$$ax + by = 1 \Leftrightarrow \overrightarrow{OM} \cdot \overrightarrow{OS} = \overrightarrow{OH} \cdot \overrightarrow{OS} \Leftrightarrow \overrightarrow{HM} \cdot \overrightarrow{OS} = 0.$$

Ainsi, chercher les solutions entières (x, y) de l'équation $ax + by = 1$ revient à chercher les points M à coordonnées entières appartenant à la droite passant par H et perpendiculaire à (OS) .



Pour l'exemple, on a choisi $4x + 3y = 1$.

11.3 Autres applications

11.3.1 Fraction irréductible

Théorème 8 : Tout rationnel r s'écrit de façon unique $r = a/b$, avec $(a, b) \in \mathbb{Z} \times \mathbb{N}$ et $a \wedge b = 1$.

démonstration :

Existence : Soit $r \in \mathbb{Q}$. Il existe $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que $r = a/b$. On peut se ramener à $b \in \mathbb{N}^*$ en posant $a = -a$ et $b = -b$ puisque $(a, b) \mathbb{R} (-a, -b)$ d'après la remarque. Soit alors $d = |a| \wedge b$. Alors il existe a', b' tels que $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$, d'où

$$r = \frac{a}{b} = \frac{da'}{db'} \stackrel{r\grave{a}d}{=} \frac{a'}{b'},$$

avec $(a', b') \in \mathbb{Z} \times \mathbb{N}^*$.

Unicité : Soit $r = a/b = c/d$, avec $a \wedge b = c \wedge d = 1$. Or $a/b = c/d \Leftrightarrow ad = bc$, et d'après le théorème de Gauss, on a d'une part que $d|bc$ et $c \wedge d = 1 \Rightarrow d|b$, et d'autre part $b|ad$ et $a \wedge b = 1 \Rightarrow b|d$. Au final, $b = d$ car ils sont tous les deux éléments de \mathbb{N}^* , et il en découle que $a = c$. Les deux fractions sont les mêmes.

L'unicité justifie alors la définition de fraction irréductible. ■

11.3.2 Éléments inversibles (resp. générateurs) de $\mathbb{Z}/n\mathbb{Z}$

Théorème 9 : Soit $n \in \mathbb{N} \setminus \{0, 1\}$. L'élément \bar{x} est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ (resp. un générateur de $\mathbb{Z}/n\mathbb{Z}$) si et seulement si x est premier avec n .

démonstration :

$$\begin{aligned} \bar{x} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \exists \bar{y} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{x} \cdot \bar{y} = \bar{1} \\ &\Leftrightarrow \exists x, y \in \mathbb{Z} \mid x \equiv y \pmod{n} \\ &\Leftrightarrow \exists x, y, u \in \mathbb{Z} \mid xy + un = 1 \\ &\stackrel{\text{Bézout}}{\Leftrightarrow} x \wedge n = 1. \end{aligned}$$

■