Sylvain ETIENNE
PLC1
etiennesy@wanadoo.fr

PGCD ET PPCM DE DEUX ENTIERS NATURELS. NOMBRES PREMIERS ENTRE EUX. APPLICATIONS. L'EXPOSE POURRA ETRE ILLUSTRE PAR UN OU DES EXEMPLES FAISANT APPEL A L'UTILISATION DE LA CALCULATRICE.

Niveau : Terminale S.

Pré-requis : Divisibilité dans $\mathbb{Z}$ – Suites –

I INTRODUCTION.

C'est vers 300 avant J.-C. qu'Euclide décrit un algorithme calculant le PGCD de deux nombres entiers. Cette recherche systématique trouve une place dans la résolution d'un certain type d'équations, délicates à résoudre sans cet outil. Nous allons donc définir le PGCD et le PPCM de deux entiers, puis la primalité de deux entiers. Enfin, nous étudierons ces équations.

II PLUS GRAND COMMUN DIVISEUR.

Ce paragraphe a pour but la recherche des diviseurs positifs, communs à deux entiers positifs *a* et *b*.

Par convention, les diviseurs d'un entiers naturel seront toujours des diviseurs positifs.

A) DIVISEURS COMMUNS A DEUX ENTIERS NATURELS.

Pour $a \in \mathbb{N}$, notons $\mathcal{D}(a) = \{x \in \mathbb{N} / x | a\}$ l'ensemble des diviseurs de *a*. Et pour $(a,b) \in \mathbb{N}^2$, notons $\mathcal{D}(a,b) = \{x \in \mathbb{N} / x | a \text{ et } x | b\}$ l'ensemble des diviseurs communs à *a* et *b*.

Ainsi, nous avons $\mathcal{D}(a,b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.

Théorème 1 :

> Soit $(a,b) \in \mathbb{N}^2$. Il existe un et un seul entier naturel δ tel que $\mathcal{D}(a,b) = \mathcal{D}(\delta)$.

Démonstration :

- Existence :

Si $b = 0$, alors $\mathcal{D}(a,0) = \mathcal{D}(a)$. Et si $a = 0$, alors $\mathcal{D}(0,b) = \mathcal{D}(b)$.

Si $a = b = 0$, alors $\mathcal{D}(0,0) = \mathcal{D}(0)$.

Supposons, à présent, $0 < b \leq a$. Si $b | a$, alors $\mathcal{D}(a,b) = \mathcal{D}(b)$. Sinon, écrivons la division euclidienne de *a* par *b*, soit $a = bq + r$ avec $0 \leq r < b$. Il vient alors : $\mathcal{D}(a,b) = \mathcal{D}(b,r)$. Ainsi, nous pouvons changer le couple (a,b) par (b,r).

Si $r=0$, $\mathcal{D}(b,r)=\mathcal{D}(b)$ et nous pouvons arrêter.

Si $r\neq 0$, nous faisons la division euclidienne de b par r, soit $b=q_1 r+r_1$. D'où $\mathcal{D}(a,b)=\mathcal{D}(b,r)=\mathcal{D}(r,r_1)$. Et ainsi de suite.

Cette suite admet un reste nul, car les restes successifs $r, r_1, \ldots$ sont des entiers positifs qui vont en décroissant strictement. Nous obtenons alors : $\mathcal{D}(a,b)=\mathcal{D}(r_n,0)=\mathcal{D}(r_n)$ où r_n est le dernier reste non nul, et dans ce cas, nous posons $\delta=r_n$.

- Unicité :

Nous avons $\mathcal{D}(0,0)=\mathcal{D}(0)$, ce qui donne l'unicité pour $a=b=0$.

Nous pouvons à présent supposer que $a\geq 1$ ou $b\geq 1$. Dans ce cas, si δ est un entier naturel tel que $\mathcal{D}(a,b)=\mathcal{D}(\delta)$, alors $\delta\geq 1$.

Si δ et δ' sont deux entiers naturels tels que $\mathcal{D}(a,b)=\mathcal{D}(\delta)=\mathcal{D}(\delta')$, alors $\delta\,|\,\delta'$ et $\delta'\,|\,\delta$. Il existe donc $(u,v)\in\mathbb{N}^2$ tel que $\delta=u\,\delta'$ et $\delta'=v\,\delta$, d'où $\delta=u\,v\,\delta$, *i.e.* : $u\,v=1$. Or les seuls entiers naturels u et v tels que $u\,v=1$ sont $u=v=1$, ce qui donne $\delta=\delta'$. □

Définition 1 :

> L'entier naturel δ est appelé le plus grand commun diviseur de a et b. Il est noté $\text{pgcd}(a,b)=\delta$.

Remarque :

- La démonstration de l'existence du PGCD de deux entiers naturels fournit un algorithme, qui est « l'algorithme d'Euclide ».

B) PROPRIETES.

Théorème 2 :

> -*i*- Le PGCD est commutatif : $\forall(a,b)\in\mathbb{N}^2,\ \text{pgcd}(a,b)=\text{pgcd}(b,a)$.
>
> -*ii*- $\forall(a,b,c)\in\mathbb{N}^3,\ \text{pgcd}(c\,a,c\,b)=c\,\text{pgcd}(a,b)$.
>
> -*iii*- Le PGCD est associatif :
>
> $\forall(a,b,c)\in\mathbb{N}^3,\ \text{pgcd}(\text{pgcd}(a,b),c)=\text{pgcd}(a,\text{pgcd}(b,c))$.

Démonstration :

-*i*- L'égalité vient de $\mathcal{D}(a,b)=\mathcal{D}(a)\cap\mathcal{D}(b)=\mathcal{D}(b)\cap\mathcal{D}(a)=\mathcal{D}(b,a)$.

-*ii*- Si $c=0$, il n'y a rien à montrer. Sinon, il suffit de multiplier chacune des divisions euclidiennes par c. Nous avons alors $\text{pgcd}(x\,a,x\,b)=\text{pgcd}(x\,b,x\,r)=\ldots=x\,r_n=x\,\text{pgcd}(a,b)$.

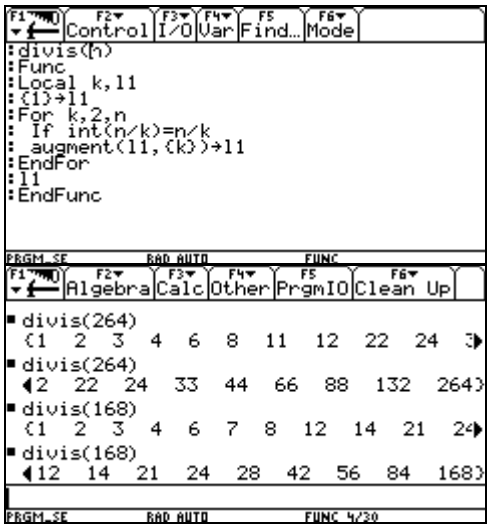
-*iii*- Nous avons, par associativité de l'intersection :

$(\mathcal{D}(a)\cap\mathcal{D}(b))\cap\mathcal{D}(c)=\mathcal{D}(a)\cap(\mathcal{D}(b)\cap\mathcal{D}(c))$. □

C) RECHERCHE DU PGCD.

Une première méthode consiste à trouver tous les diviseurs de a et de b, puis de prendre le plus grand des diviseurs communs !

Il est possible de trouver les diviseurs d'un entier grâce à un algorithme utilisant une boucle « FOR » et l'idée suivante : si k divise n, alors la partie entière de n/k est égale à n/k.



Exemple :

Cherchons le PGCD de 168 et 264 par cette méthode. Nous trouvons la décomposition ci-contre. Nous en déduisons que $\text{pgcd}(264,168)=24$.

Cependant cette méthode peut se révéler très longue, car dès que a ou b est grand, la recherche des différents diviseurs peut prendre un certain temps !

L'algorithme d'Euclide peut être facilement mis en œuvre sur une calculatrice comme c'est le cas ci-contre avec une T.I. Voyage 200.

Calculons le PGCD de 168 et 264 grâce à ce programme :
Nous trouvons que $\text{pgcd}(264,168)=24$.

III THEOREME DE BEZOUT.

Définition 2:

> Deux entiers naturels sont dits premiers entre eux lorsque leur PGCD est égal à 1.

Théorème 3 : théorème de Bézout.

> Soit a et b deux entiers naturels non nuls. a et b sont premiers entre eux si et seulement s'il existe $(u,v)\in\mathbb{Z}^2$ tels que : $au+bv=1$.

Démonstration :

- Supposons qu'il existe $(u,v)\in\mathbb{Z}^2$ tels que : $au+bv=1$. Alors le PGCD de a et b, qui divise a et b, divise tout nombre $au+bv$ où $(u,v)\in\mathbb{Z}^2$, donc divise 1. Ainsi $\text{pgcd}(a,b)=1$.

- Réciproquement, si $\text{pgcd}(a,b)=1$, alors considérons l'ensemble $\mathcal{E}$ des entiers naturels non nuls de la forme $au+bv$ avec $(u,v)\in\mathbb{Z}^2$.

  $\mathcal{E}$ contient a car $a=a\times 1+b\times 0$. $\mathcal{E}$ contient alors un plus petit élément $m=au_0+bv_0$, où $(u_0,v_0)\in\mathbb{Z}^2$.

  Montrons que m divise a et b ; nous aurons alors que $m=1$, et donc $au_0+bv_0=1$.

  La division euclidienne de a par m donne : $a=(au_0+bv_0)q+r$ avec $0\le r<m$.

  D'où $r=a(1-qu_0)+b(-qv_0)=au+bv$, avec $(u,v)\in\mathbb{Z}^2$.

  Si $r>0$, alors $r\in\mathcal{E}$, et dans ce cas $r\ge m$ par définition de m. Or $r<m$, donc $r=0$ et m divise a.

  De même, nous montrons que m divise b. □

Théorème 4 : théorème de Gauss.

> Soit $(a,b,c)\in\mathbb{N}^3$. Si a divise bc et si a est premier avec b, alors a divise c.

Démonstration :

Par le théorème 2, comme a est premier avec b, soit $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$. D'où $auc+bvc=c$. Or a divise évidemment acu et a divise bcv par hypothèse, donc a divise leur somme, *i.e.* : a divise c. □

Corollaire 1 :

> Si n, un entier naturel est divisible par deux entiers naturels a et b premiers entre eux, alors n est divisible par le produit ab.

Démonstration :

Par hypothèse, nous pouvons écrire $n=ap$ et $n=bq$ avec $(p,q)\in\mathbb{N}^2$. Donc $ap=bq$ et comme b divise ap et qu'il est premier avec a, il divise donc p. Par suite, nous pouvons écrire $p=bp'$ avec $p'\in\mathbb{N}$, donc $n=abp'$. D'où le résultat. □

IV PLUS PETIT COMMUN MULTIPLE.

Pour $a\in\mathbb{N}$, notons $\mathcal{M}(a)=\{x\in\mathbb{N}/a|x\}$ l'ensemble des multiples de a.

Théorème 5 :

> Soit $(a,b)\in\mathbb{N}^2$. Il existe un unique entier naturel μ tel que : $\mathcal{M}(a)\cap\mathcal{M}(b)=\mathcal{M}(\mu)$.

Démonstration :

Si $a=b=0$, alors nous avons existence et unicité du théorème avec $\mu=0$.

Nous pouvons, dès lors, supposer a ou b différent de 0. Dans ce cas, si μ existe, alors, il est non nul.

- Existence :

Nous avons : $m \in \mathcal{M}(a) \cap \mathcal{M}(b) \Leftrightarrow \exists (u,v) \in \mathbb{N}^2 / m = au = bv$.

Soit $\delta = \text{pgcd}(a,b)$, alors soit $(a',b') \in \mathbb{N}^2$ tel que $a = \delta a'$ et $b = \delta b'$. L'égalité $au = bv$ devient alors $a'u = b'v$, et par le théorème de Gauss, il existe un entier naturel w tel que $u = wb'$, d'où $m = ua = w\delta a'b'$.

Réciproquement, l'égalité $m = w\delta a'b'$ entraîne l'existence de deux entiers naturels tels que : $m = au = bv$.

Nous venons donc de montrer que : $\exists (u,v) \in \mathbb{N}^2 / m = au = bv \Leftrightarrow \exists w \in \mathbb{N} / m = w\delta a'b'$.

Or $\exists w \in \mathbb{N} / m = w\delta a'b' \Leftrightarrow m \in \mathcal{M}(\delta a'b')$.

Il ne reste plus qu'à poser $\mu = \delta a'b'$.

- Unicité :

Soit $(\mu,\mu') \in \mathbb{N}^2$ vérifiant l'égalité : $\mathcal{M}(a) \cap \mathcal{M}(b) = \mathcal{M}(\mu) = \mathcal{M}(\mu')$. Il existe alors $(u,v) \in \mathbb{N}^2$ tel que $\mu = u\mu'$ et $\mu' = v\mu$, d'où $\mu = uv\mu$, et par suite $u = v = 1$ (car $\mu \neq 0$), et ainsi : $\mu = \mu'$. □

Définition 3 :

L'entier naturel μ est appelé le plus petit commun multiple de *a* et *b*. Il est noté $\text{ppcm}(a,b) = \mu$.

Théorème 6 :

Soit $(a,b) \in \mathbb{N}^2$. Nous avons alors la relation : $\text{pgcd}(a,b)\text{ppcm}(a,b) = ab$.

Démonstration :

Si *a* ou *b* est nul, alors la relation est vraie.

Supposons *a* et *b* non nul. Dans la preuve du théorème 5, nous avons : $\mu = \delta a'b'$, *i.e.* : $\mu = \delta \frac{a}{\delta}\frac{b}{\delta}$, d'où $\mu\delta = ab$. □

Théorème 7 :

-i- Le PPCM est commutatif : $\forall (a,b) \in \mathbb{N}^2$, $\text{ppcm}(a,b) = \text{ppcm}(b,a)$.

-ii- $\forall (a,b,c) \in \mathbb{N}^3$, $\text{ppcm}(ca,cb) = c\,\text{ppcm}(a,b)$.

-iii- Le PPCM est associatif :

$\forall (a,b,c) \in \mathbb{N}^3$, $\text{ppcm}(\text{ppcm}(a,b),c) = \text{ppcm}(a,\text{ppcm}(b,c))$.

Démonstration :

-i- - L'égalité vient de $\mathcal{M}(a,b) = \mathcal{M}(a) \cap \mathcal{M}(b) = \mathcal{M}(b) \cap \mathcal{M}(a) = \mathcal{M}(b,a)$.

-ii- L'égalité se montre grâce au théorème 6 et au point *-ii-* du théorème 2.

-iii- Nous avons, par associativité de l'intersection :

$(\mathcal{M}(a) \cap \mathcal{M}(b)) \cap \mathcal{M}(c) = \mathcal{M}(a) \cap (\mathcal{M}(b) \cap \mathcal{M}(c))$. □

V APPLICATIONS.

A) FRACTIONS RATIONNELLES.

Théorème 8 :

> Toute fraction positive est égale à une fraction du type $\frac{a}{b}$, avec $(a,b)\in\mathbb{N}\times\mathbb{N}^*$, avec *a* et *b* premiers entre eux.

Démonstration :

Soit une fraction positive $\frac{c}{d}$ avec $(c,d)\in\mathbb{N}\times\mathbb{N}^*$. Soit $\delta=\text{pgcd}(c,d)$, alors $c=\delta a$ et $d=\delta d$ avec $(a,b)\in\mathbb{N}\times\mathbb{N}^*$ et a et b premiers entre eux. D'où en simplifiant par δ, $\frac{c}{d}=\frac{a}{b}$. □

B) EQUATIONS DIOPHANTIENNES : *a x + b y = c.*

1) METHODE DE RESOLUTION.

Nous recherchons ici toutes les solutions entières de l'équation $a\,x+b\,y=c$ avec $(a,b,c)\in\mathbb{Z}^3$.

Nécessairement, s'il existe une solution dans $\mathbb{Z}^2$, et si $\delta=\text{pgcd}(a,b)$, alors $\delta\,|\,c$. En prenant la contraposée, si δ ne divise pas *c*, alors l'équation n'a pas de solution dans $\mathbb{Z}^2$.

Dans le cas contraire, nous pouvons nous ramener à la résolution de l'équation $a\,x+b\,y=c$ avec a et b premiers entre eux.

En effet, si $\delta\,|\,c$, alors soit $(a',b',c')\in\mathbb{N}^3$ tel que $a=\delta\,a'$, $b=\delta\,b'$, $c=\delta\,c'$ et a' et b' premiers entre eux. L'équation devient alors : $a'\,x+b'\,y=c'$ avec a' et b' premiers entre eux.

La donnée d'une solution particulière $(x_0,y_0)\in\mathbb{Z}^2$ permet de déterminer toutes les solutions car : $a\,x+b\,y=c\Leftrightarrow a(x-x_0)=-b(y-y_0)$.

Cette dernière équation se résout à l'aide du théorème de Gauss (théorème 4) : *a* divise $(y-y_0)$. Par suite, il existe $w\in\mathbb{Z}$ tel que $y-y_0=wa$ et $x-x_0=wb$. La réciproque est évidente.

En conclusion, nous avons donc :

$$a\,x+b\,y=c\Leftrightarrow\exists w\in\mathbb{Z}\begin{cases}x=x_0+b\,w,\\ y=y_0-a\,w.\end{cases}$$

De plus, il suffit de connaître une solution particulière de l'équation $a\,\tilde{x}+b\,\tilde{y}=1$, avec *a* et *b* premiers entre eux, car les solutions de l'équation initiale sont données par : $\begin{cases}x=c\,\tilde{x},\\ y=c\,\tilde{y}.\end{cases}$

2) ALGORITHME DE CALCUL D'UNE SOLUTION PARTICULIERE.

Si a et b sont premiers entre eux, le théorème de Bézout (théorème 3) donne l'existence d'une solution, au moins, de l'équation $a\,x+b\,y=c$.

Nous allons donner un algorithme permettant d'obtenir une solution particulière. Le principe tient au fait que dans l'algorithme d'Euclide, nous calculons les restes successifs jusqu'à trouver un reste nul. Nous définissons par la suite une suite récurrente :

$$\begin{cases} r_0 = a,\ r_1 = b, \\ r_{i+2} = r_i - r_{i+1}q_{i+1},\ \forall i \in [\![0, n-1]\!], \\ r_{n+1} = 0. \end{cases} \qquad (1)$$

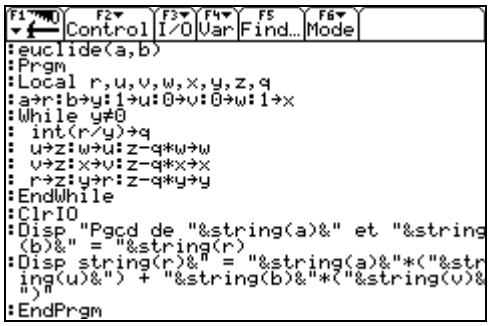
Cette suite permet d'obtenir $r_i,\ \forall i \in [\![0, n-1]\!]$, comme une combinaison linéaire de a et b ; i.e. : $\forall i \in [\![0, n-1]\!],\ \exists (u_i, v_i) \in \mathbb{Z}^2$ tel que $r_i = u_i\,a + v_i\,b$.

Nous définissons alors deux nouvelles suites récurrentes déduites immédiatement de (1) :

$$\begin{cases} u_0 = 1,\ u_1 = 0, \\ u_{i+2} = u_i - u_{i+1}q_{i+1},\ \forall i \in [\![0, n-1]\!], \end{cases} \text{ et } \begin{cases} v_0 = 0,\ v_1 = 1, \\ v_{i+2} = v_i - v_{i+1}q_{i+1},\ \forall i \in [\![0, n-1]\!]. \end{cases}$$

Nous avons, en effet, $r_0 = 1a + 0b$ et $r_1 = 0a + 1b$.

Nous obtenons alors le programme suivant, sur une T.I. Voyage 200. Une « sauvegarde » de valeur est nécessaire pour écrire les trois relations de récurrence.

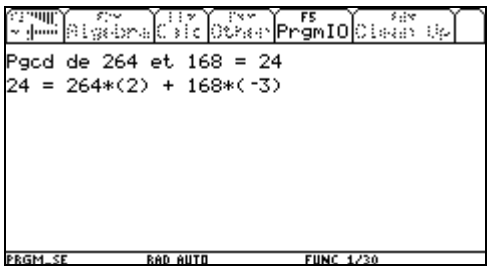


Revenons à l'exemple 1 :

Nous cherchons une solution particulière de l'équation : $264\,x + 168\,y = 24$.

Le programme nous répond qu'une solution particulière est $(x_0, y_0) = (2, -3)$. Les solutions entières sont donc :

$$\begin{cases} x = 2 + 168\,w, \\ y = -3 - 264\,w, \end{cases} \quad w \in \mathbb{Z}.$$



VI CONCLUSION.

Nous avons défini et donné quelques propriétés du PGCD et PPCM et leur principale application qui consiste grâce à la primalité entre deux entiers naturels, la résolution des équations diophantiennes. Il est possible, néanmoins, d'étendre les définitions et propriétés du PGCD et PPCM à deux entiers relatifs.