PGCD PPCM et applications

1. Le PGCD
   1. Définition

*Remarque préliminaire* : l’ensemble des diviseurs D(*a*) d’un nombre entier naturel *a* est un ensemble fini non vide, puisqu’il contient 1, et admettant un élément maximal, qui est *a*. De même, l’ensemble des diviseurs D(*a*, *b*) communs à deux entiers naturels *a* et *b* est un ensemble fini non vide, puisqu’il contient 1, et admettant un élément maximal, qui est inférieur ou égal au minimum de *a* et de *b*.

*Définition* : le plus grand commun diviseur de deux entiers naturels non nuls est le plus grand élément de l’ensemble des diviseurs D(*a*, *b*) communs à *a* et *b*. On note  ou [[1]](#footnote-1).

*Propriété immédiate* : 

*Généralisation* : cette notion se généralise à deux entiers relatifs non nuls.

*Exemples*:

* 
* 
* 
* Si alors 

*définition* : *a* et *b* sont dits premiers entre eux si leur pcgd vaut 1.

* 1. Méthodes de calcul du pgcd
     1. Ensembles des diviseurs.

*Exemple* : on veut déterminer le pgcd de 378 et 525.

D(378) = {1, 2, 3, 6, 7, 9, 14, 18, 21, 27, 42, 54, 63, 126, 189, 378}

D(525) = {1, 3, 5, 7, 15, 21, 25, 35, 75, 105, 175, 525}

D(378)  D(525) = {1,  3, 7, 21} donc 

On remarque que D(378)  D(525) = D(21) : l’ensemble des diviseurs communs est l’ensemble des diviseurs du pgcd.

* + 1. Soustractions successives d’Euclide.

*Théorème* : si , alors .

*Démonstration* : on utilise les propriétés de la divisibilité.

 , donc l’ensemble des diviseurs communs à *a* et à *b* est égal à l’ensemble des diviseurs communs à  et à *b*. En particulier le plus grand élément de cet ensemble est le  et également celui de .

*Méthode* : en se basant sur la propriété précédente, on ramène le calcul du pgcd de deux nombres au calcul du pgcd de deux nombres dont l’un des deux est strictement plus petit.

Comme la suite des calculs de  est strictement décroissante dans , elle admet un plus petit élément et s’arrête.

*Exemple* : calcul de .



*Remarque* : essayez le calcul de  avec cette méthode, c’est très long et peu efficace.

* + 1. Algorithme d’Euclide

C’est la méthode la plus rapide en général.

On effectue une suite de divisions euclidiennes pour calculer  :

On divise *a* par *b* : 

Puis *b* par  : 

Puis  par  : 

…

Puis  par  : 

Jusqu’à ce que l’on obtienne un reste nul. Le pgcd est le dernier reste non nul.

*Démonstration :*

* Par définition de la division euclidienne, . La suite  des restes est une suite d’entiers naturels strictement décroissante, elle est donc finie. Donc l’algorithme s’arrête.
* Si *d* est un diviseur de *a* et de *b*, alors *d* divise toute combinaison linéaire de *a* et *b*. En particulier *d* divise , c’est-à-dire que  et .

Réciproquement si  et , alors , c’est à dire que *d* divise *a.*

Donc D(*a*, *b*) = D(*b*, ).

* Finalement, soit  le dernier reste non nul

On a D(*a*, *b*) = D(*b*, ) = D(,) = … = D(,)  d’après ce qui précède.

Et par définition de  : , soit  divise  .

Donc  ◼

*Remarque*: cet algorithme est très rapide, voir l’exercice XXXV sur la page <http://www.maths-info-lycee.fr/exos_arithmetique.html>

*Exemple*: calcul de pgcd(5525, 1989)



Le pgcd vaut 221

* 1. Propriétés du pgcd

*Propriétés* : soient *a*, *b* et *k* trois entiers naturels non nuls. Alors :

* 
* Si  alors 
* 

*Démonstrations*:

* Pour .
  + 1ère méthode : on reprend la suite des divisions euclidiennes et on les multiplie par *k* :

|  |  |  |
| --- | --- | --- |
| …    d’où |  | …    d’où |

CQFD

* + 2ème méthode : on utilise les propriétés de la divisibilité

Soit . Alors 

Réciproquement, soit *q* tel que 

 CQFD

* Pour : Si  alors 

Immédiat d’après la propriété précédente. Presque immédiat… pas si simple à rédiger, poser  et  et conclure :

* Pour 



*Contre-exemple* : la propriété précédente est fausse avec  .

 et 

*Corollaire important* :

Si  alors  , c’est à dire que  et  sont premiers entre eux.

1. Le PPCM

De même que l’on a défini l’ensemble des diviseurs communs à deux entiers naturels non nuls, on peut définir l’ensemble des multiples communs non nuls à deux entiers naturels non nuls *a* et *b*. Cet ensemble est non vide, puisqu’il contient *ab*, et c’est un ensemble d’entiers naturels : il admet donc un plus petit élément.

*Définition* : soient *a* et *b* deux entiers naturels non nuls. Le plus petit commun multiple de *a* et *b* est le plus petit élément non nul de l’ensemble des multiples communs à *a* et *b*.

Cette notion se généralise à deux entiers relatifs non nuls, le ppcm étant positif par définition.

On le note  ou plus rarement [[2]](#footnote-2).

*Exemple* : 

*Théorème* : l’ensemble des multiples communs à *a* et à *b* est l’ensemble des multiples de .

*Démonstration* :

* Soit 

Si *m* est multple de **, comme ** est multiple de *a*, alors *m* est multiple de *a*.

De même *m* est un multiple de *b*.

Donc tout multiple de *m* est un multiple commun à *a* et *b*.

* Réciproquement, si *m* est un multiple commun à *a* et *b*, effectuons la division euclidienne de *m* par ** :  avec .

*m* et ** sont des multiples de *a* donc  est un multiple de *a*, donc *r* est un multiple de *a*.

De même, *r* est un multiple commun à *a* et *b* avec . Comme ** est le plus petit multiple commun non nul de *a* et *b*, alors *r* = 0 et  : *m* est un multiple de **.

CQFD

*Corollaire* :



*Lemme* : Soit , soient ** et ** tels que . Alors 

*Démonstration* :

Soit *d* un diviseur commun à ** et **.

, or , donc .

Donc  est entier, et .

De même .

Donc  est un multiple commun à *a* et *b*, donc un multiple de leur ppcm. Par ailleurs *d* ≥ 1, donc  . Comme ** est le plus petit des multiples communs, on a forcément *d* = 1. CQFD

*Théorème* : Soient *a* et *b* deux entiers naturels non nuls. Alors .

*Démonstration* : on utilise les notations et le résultat du lemme précédent.

On part de 

On multiplie les deux membres par *ab* :

 CQFD

*Propriétés* : soient *a*, *b* et *k* trois entiers naturels non nuls.

* 
* Si  alors 

*Démonstration*: pour 

On utilise le théorème précédent, , en remplaçant *a* par *ka* et *b* par *kb*.

****

****  ◼

*Remarques* :

* La démonstration de la deuxième propriété ci-dessus peut se faire sur le modèle de la preuve de la propriété similaire pour le pgcd.
* Si  ,  ,  , alors 
* Propriétés similaires avec .

1. ThEorEme de Bezout

*Théorème* : soient *a* et *b* deux entiers naturels non nuls, et soit ** leur pgcd. Alors il existe deux entiers relatifs *u* et *v* tels que .

*Démonstration* :

* Si  alors  , d’où *u* =  et *v* = donnent  .
* De même si.
* Sinon, on reprend les divisions successives de l’algorithme d’Euclide  pour l’obtention du pgcd :







…

 ligne 

 ligne 

 ligne 

avec

On parcourt le calcul à l’envers, de l’avant-dernière à la première ligne, en exprimant  en fonction des restes et quotients successifs :

 donne 

En substituant  obtenu dans la ligne  :  on obtient



On remplace ensuite  à l’aide de la ligne précédente, etc. jusqu’à la ligne de départ, où l’on obtient alors  ◼

*Remarques* :

* le couple  n’est pas unique. En effet, si alors 
* Ce théorème est une implication, pas une équivalence. *Contre-exemple* :

 et 

*Exemple* : On a vu que pgcd(5525, 1989) = 221

 d’ où 

*Théorème* : deux entiers naturels non nuls *a* et *b* sont premiers entre eux si et seulement si il existe deux entiers relatifs *u* et *v* tels que .

*Démonstration* :

* Implication : d’après le théorème de Bézout, *a* et *b* sont premiers entre eux implique qu’il existe deux entiers relatifs *u* et *v* tels que .
* Réciproque : Soit , et soient *u* et *v* tels que . Comme **divise *a* et *b*, ** divise  , donc ** divise 1, d’où ** = 1. ◼

*Remarques :*

* On en déduit que *a* et *v* sont premiers entre eux, de même que *u* et *b*, ainsi que *u* et *v*.
* Important : on déduit du théorème de Bézout que l’équation  admet des solutions si et seulement si .
  + Faire la preuve en exercice.
  + Comme précédemment, le couple  n’est pas unique.

1. ThEorEme de Gauss

*Théorème* : Soient *a*, *b* et *c* trois entiers relatifs non nuls. Si *a* divise *bc* et si *a* et *b* sont premiers entre eux, alors *a* divise *c*.

*Démonstration* :

* *a* divise *bc* donc il existe *k* entier relatif tel que .
* par ailleurs, comme , il existe *u* et *v* entiers relatifs tels que  d’après le théorème de Bezout.

D’où 





Donc *a* divise *c*.

◼

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

* Si *a* divise *b*, *a* divise *c* et si *a* et *b* sont premiers entre eux, alors *ab* divise *c*;
* Si un nombre *p* premier divise le produit *ab* alors *p* divise *a* ou *p* divise *b*;
* Si *a* est premier avec le produit *bc*, alors *a* est premier avec *b* et *a* est premier avec *c* ;
* Si *a* est premier avec *c*, alors PGCD(a , b) = PGCD(a, bc)

1. Application aux equations diophantiennes

Une équations diophantienne est une équations dont la ou les inconnues sont des entiers.

* 1. Résolution dans  d’équations du type , où *a*, *b*, *c* sont des entiers relatifs fixés.

Il y a trois cas à envisager

* Si *c* n’est pas un multiple de  :

Alors il n’y a pas de solution d’après le théorème de Bezout.

*Exemple* : 

* Si  :

Il y a une infinité de solutions d’après le théorème de Bezout.

*Exemple* : 

* + On simplifie par le pgcd pour avoir un des nombres plus petits et des calculs plus simples :

 .

* + On cherche une solution particulière grâce à l’algorithme d’Euclide :



Une solution particulière est 

*On peut également trouver une solution évidente, par exemple ici  convient.*

* + On trouve ensuite les solutions potentielles en utilisant à la fois la solution particulière et l’équation générale. *Les solutions sont potentielles car il s’agît ici d’une condition nécessaire et non d’une condition « nécessaire et suffisante »*.

 

On applique le théorème de Gauss :

11 divise , et 11 et 3 sont premiers entre aux, donc 11 divise .

D’où  , puis en reportant dans  :

.

On a donc  et  , 

* + On vérifie que ces solutions conviennent (condition suffisante) :

On remplace *x* et *y* dans l’équation initiale

 donc les valeurs trouvées conviennent.

* + Conclusion 
* Si *c* est un multiple de  :

La méthode ressemble beaucoup au cas précédent, il y a également une infinité de solutions.

*Exemple* : 

, 14 est un multiple de 7 donc il y a une infinité de solutions et .

Dans un premier temps, on raisonne comme pour le cas précédent et l’on cherche une solution particulière à , grâce à l’algorithme d’Euclide ou par intuition.

Ici  convient.

On multiplie ces solutions par 2 pour avoir une solution particulière de  :



On trouve les solutions potentielles (condition nécessaire) :

 

Puis, par le théorème de Gauss : 7 divise , et 7 et 3 sont premiers entre aux, donc 7 divise .

D’où  , puis en reportant dans  :

.

D’où  et  , 

On vérifie que ces solutions conviennent (condition suffisante), en remplace *x* et *y* dans l’équation initiale

 donc les valeurs trouvées conviennent.

Conclusion 

* 1. Résolution dans  d’équations du type .

On remarque que , ce qui rappelle le théorème de Bézout.

Il y a de même trois cas à envisager

* Si *b* n’est pas un multiple de  :

Il n’y a pas de solution d’après le théorème de Bézout.

* Si *a* et *c* sont premiers entre eux :

Il y a une infinité de solution d’après le théorème de Bézout.

*Exemple* : résoudre dans  l’équation .

D’après le théorème de Bézout, il existe au moins un couple d’entiers  tel que :

.

On applique l’algorithme d’Euclide :

 d’où 

De on déduit 

On multiplie alors les deux membres de  par –19 :



(1) on rappelle que 

Les solutions sont 

* Si *a* et *c* sont ne sont pas premiers entre eux, et si *b* est un multiple de  :

On pose ,  et  ; on est alors ramené au cas précédent, l’équation devenant  avec .

*Remarque* : un cas particulier est la recherche d’un inverse de *a* modulo *c*, c’est-à-dire d’un nombre *x* tel que  . On constate que ce n’est pas toujours possible ; étudiez les cas suivants :

* 
* 

Cours de Frédéric Mandon sous licence Creative Commons BY NC SA, <https://creativecommons.org/licenses/by-nc-sa/3.0/fr/>

1. Cette dernière notation est moins utilisée, elle utilise la notation du « et » en logique. [↑](#footnote-ref-1)
2. Comme ci-dessus pour le pgcd, cette notation est celle du « ou » en logique. [↑](#footnote-ref-2)