TS spécialité

PGCD et PPCM

Plan du chapitre :

Toutes les démonstration des propriétés du chapitre sont à connaître (c'est-à-dire qu'il faut savoir les refaire), sauf la démonstration du sens difficile pour le théorème de Bezout dans le paragraphe **VIII** ainsi que celle du 6°) du paragraphe **X**.

Le 27-2-2024

Cours sur le PGCD

On reprend les programmes Python permettant d'obtenir les diviseurs d'un entier.
Autre idée :
On crée la liste des diviseurs de a et la liste des diviseurs de b puis on sélectionne les éléments qui sont communs aux deux listes.

Le lundi 15 février 2021

Le cours de Pouliquen sur le PGCD est vraiment super du point de vue des équations diophantiennes.

Quelques repères historiques : Bezout ; Gauss ; Diophante

Étienne Bezout (1730-1783) : mathématicien français

Carl Friedrich Gauss (1777-1855) : mathématicien allemand

Diophante d'Alexandrie vécut entre le I^{er} et le IV^{e} siècle, peut-être au II^{e} ou au III^{e} siècle après Jésus-Christ. C'est l'un des plus remarquables mathématiciens grecs de l'Antiquité. Il s'intéressa aux nombres entiers et fractionnaires et étudia la résolution de nombreuses équations.
Son plus célèbre ouvrage s'appelle *Les Arithmétiques* (*Arithmetica*).

Diophante ce génie

Diophante a vécu à Alexandrie entre le I^{er} et le IV^{e} siècle. Il est considéré par certains comme le père de l'algèbre. Son plus célèbre ouvrage *Les Arithmétiques* comprend 13 livres dont 4 d'entre eux n'ont été retrouvés qu'en 1972 !
Diophante avait une conception algébrique de la résolution des problèmes lorsque ses contemporains n'en avaient qu'une interprétation géométrique.
Trouver deux nombres dont la somme est 22 et le produit 112.
Diophante écrit ces deux nombres sous la forme $11+a$ et $11-a$ et ramène donc le problème de deux inconnues à un problème à une seule inconnue.

Rappel de notations :

Pour tout entier relatif a,
$D(a)$ désigne l'ensemble des diviseurs de a ;
$D^{+}(a)$ désigne l'ensemble des diviseurs positifs ou nuls de a ;
$D^{-}(a)$ désigne l'ensemble des diviseurs négatifs ou nuls de a.

I. Généralités sur le PGCD

1°) Ensemble des diviseurs communs à deux entiers relatifs

a et b sont deux entiers relatifs.

L'ensemble des diviseurs communs à a et b est l'ensemble $E = \mathbf{D}(a) \cap \mathbf{D}(b)$.
L'ensemble des diviseurs positifs ou nuls communs à a et b est $E^+ = \mathbf{D}^+(a) \cap \mathbf{D}^+(b)$.

On va étudier E.

1 et – 1 appartiennent tous les deux à E donc E contient toujours 1 et – 1.

On en déduit au passage que E est toujours non vide.

1er cas : a et b ne sont pas tous les deux nuls ($a \neq 0$ ou $b \neq 0$).

Dans ce cas, l'un au moins des ensembles $\mathbf{D}(a)$ ou $\mathbf{D}(b)$ est fini.
Donc E est un ensemble fini.

2e cas : a et b sont tous les deux nuls ($a = b = 0$).

Dans ce cas, $\mathbf{D}(a) = \mathbf{D}(b) = \mathbf{D}(0) = \mathbb{Z}$.
Donc $E = \mathbb{Z}$.

Conséquence

Lorsque a et b ne sont pas tous les deux nuls, l'ensemble E admet un plus grand élément d.
Puisque $1 \in E$, $d \geqslant 1$.
On en déduit que d est positif et est aussi le plus grand élément de E^+.

L'étude de E sera poursuivie plus loin dans le chapitre.

Remarque : Le plus petit diviseur commun positif à deux entiers non tous les deux nuls est 1.

On note :
$\mathbf{D}(a,b)$ l'ensemble des diviseurs communs à a et b ;
$\mathbf{D}^+(a,b)$ l'ensemble des diviseurs positifs ou nuls communs à a et b.
$\mathbf{D}^-(a,b)$ l'ensemble des diviseurs négatifs ou nuls communs à a et b.

Ainsi : $E = \mathbf{D}(a,b)$ et $E^+ = \mathbf{D}^+(a,b)$.

Propriétés :

a et b sont deux entiers relatifs quelconques.

$\mathbf{D}(a,b) = \mathbf{D}(a) \cap \mathbf{D}(b)$; $\mathbf{D}^+(a,b) = \mathbf{D}^+(a) \cap \mathbf{D}^+(b)$

Si a et b ne sont pas tous les deux nuls, $\mathbf{D}(a,b)$ est un ensemble fini.

$\{-1;1\} \subset \mathbf{D}(a,b)$

$\mathbf{D}(a,a) = \mathbf{D}(a)$

$\mathbf{D}(a,0) = \mathbf{D}(a)$

$\mathbf{D}(a,1) = \mathbf{D}(1) = \{-1,1\}$

Si $a \mid b$, alors $\mathbf{D}(a,b) = \mathbf{D}(a)$.

$\mathbf{D}(a,b) = \mathbf{D}(a,-b) = \mathbf{D}(-a,b) = \mathbf{D}(-a,-b) = \mathbf{D}(|a|,|b|)$

Soit d un entier relatif quelconque.
Si $d \in \mathbf{D}(a,b)$, alors d divise toute combinaison linéaire à coefficient entiers relatifs de a et b.

Lemme d'Euclide (version ensembles)

a, b, c, d sont des entiers relatifs tels que $a = bc + d$.
On a : $\mathbf{D}(a,b) = \mathbf{D}(b,d)$.

Il s'agit d'une égalité d'ensembles.

Autre version du lemme d'Euclide :

a et b sont deux entiers relatifs.
Pour tout entier relatif λ, on a : $\mathbf{D}(a,b) = \mathbf{D}(a - \lambda b, b)$.

2°) Définition

a et b sont deux entiers relatifs non tous les deux nuls.

Le **plus grand commun diviseur** à a et b, noté **PGCD$(a\,;b)$** ou PGCD$(b\,;a)$, est – comme son nom l'indique – le plus grand élément de $\mathbf{D}(a) \cap \mathbf{D}(b)$ (ou encore $\mathbf{D}^+(a) \cap \mathbf{D}^+(b)$).

Par suite, le PGCD est un entier strictement positif (supérieur ou égal à 1).

3°) Exemple

Déterminons le PGCD de 18 et de 66.

On reprend les notations du **1°)**.

On a $D^+(18)=\{1;2;3;6;9;18\}$ et $D^+(66)=\{1;2;3;6;11;22;33;66\}$.
Donc $E^+=D^+(18)\cap D^+(66)=\{1;2;3;6\}$.

On en déduit que $\text{PGCD}(18;66)=6$.

On peut remarquer dans notre exemple que les éléments de E^+ sont les diviseurs positifs de 6.
Nous verrons plus loin dans le cours qu'il s'agit d'une propriété générale qui sera donnée et démontrée plus loin dans le cours : « Les diviseurs communs à deux entiers relatifs sont les diviseurs de leur PGCD ».

4°) Obtention du PGCD de deux entiers

Le 1-3-2024

Il n'existe pas de formule permettant d'exprimer le PGCD de deux entiers *a* et *b* non tous les deux nuls en fonction de *a* et *b*.

Il y a, en gros, deux méthodes : « à la main » ou à l'aide d'outils de calcul.

• On peut rechercher le PGCD en établissant la liste des diviseurs des deux entiers, comme dans l'exemple précédent. Mais cette méthode s'avère fastidieuse en général.

• On peut utiliser « l'algorithme d'Euclide » qui sera étudié dans le paragraphe **IV**.

• On verra également dans le prochain chapitre une méthode utilisant la décomposition en facteurs premiers.

• Sinon, on peut utiliser la calculatrice (voir paragraphe 8°)).

5°) Généralisation au cas de plusieurs nombres

La définition s'étend au cas du plus grand commun diviseur de plusieurs entiers relatifs non tous nuls. Nous y reviendrons dans le paragraphe **XII**.
Le PGCD de plusieurs entiers naturels non tous nuls est un diviseur de chacun des entiers et est donc toujours inférieur ou égal à chacun des entiers.

6°) Utilisation du PGCD pour la résolution de problèmes concrets

On utilise le PGCD pour la résolution :
- de problèmes de partages équitables (voir exercices) ;
- de pavages d'un rectangle par des carrés (cf. visualisation géométrique de l'algorithme d'Euclide dans le **IV. 7°)**).

Il est à noter que, pour les problèmes de partages équitables, on peut être amené à considérer le PGCD de plusieurs entiers.

8°) Utilisation de la calculatrice

Toutes les calculatrices de lycée actuelles ont une commande intégrée permettant de calculer le PGCD de deux entiers naturels que l'on rentre. Elles utilisent un programme de calcul qui donne le résultat extrêmement rapidement. L'algorithme du PGCD utilisé est en général l'algorithme d'Euclide ou l'algorithme du PGCD binaire (de Stein).
Les calculatrices en français utilisent la notation pgcd.
En anglais, le PGCD est appelé *great common divisor* et est noté gcd. Cette notation est utilisée pour les calculatrices en anglais et dans le langage Python (fonction prédéfinie du « module math »).

Calculatrice Numworks

Boîte à outils

Partie Arithmétique

gcd(p,q) PGCD de p et q
lcm(p,q) PPCM de p et q

Calculatrice TI-83 Plus

Choisir math puis sélectionner NBRE et enfin descendre jusqu'à 9 : pgcd(.

Syntaxe : pgcd(nombre 1, nombre 2) [calculatrice en français]

gcd(nombre 1, nombre 2) [calculatrice en anglais]

Les deux nombres doivent être positifs ou nuls (et non tous les deux nuls).
Les deux nombres sont séparés par une virgule.

Fonctions Python déjà prêtes à l'emploi

Fonctions gcd et lcm à importer du module math

I bis. Premiers algorithmes et programmes Python autour du PGCD

1°) Programme 1

Programme Python qui demande de rentrer deux entiers naturels non tous les deux nuls et qui affiche tous leurs diviseurs positifs communs :

On utilise la fonction Python `min(a,b)`.
$\min(a,b)$ désigne le minimum des entiers *a* et *b*, c'est-à-dire le plus petit des nombres *a* et *b*.

a et *b* sont des entiers naturels non tous les deux nuls.

```
a=int(input(" nbr1 : "))
b=int(input(" nbr2 : "))
for i in range(1,min(a,b)+1):
    if a%i==0 and b%i==0:
       print(i)
```

On reprend le programme fondamental permettant d'afficher les diviseurs positifs d'un entier naturel non nul.

On peut évidemment proposer une version fonction de ce programme.

Le 27-2-2024

Cours sur le PGCD
On reprend les programmes Python permettant d'obtenir les diviseurs d'un entier.

Autre idée :
On crée la liste des diviseurs de *a* et la liste des diviseurs de *b*, puis on sélectionne les éléments qui sont communs aux deux listes.

Avec une liste :

```
a=int(input(" nbr1 : "))
b=int(input(" nbr2 : "))
L=[]
for i in range(1,min(a,b)+1):
    if a%i==0 and b%i==0:
       L.append(i)
print(L)
```

Pour avoir le PGCD :

On utilise la fonction donnant le maximum d'une liste.

```
a=int(input(" nbr1 : "))
b=int(input(" nbr2 : "))
L=[]
for i in range(1,min(a,b)+1):
    if a%i==0 and b%i==0:
       L.append(i)
print(max(L))
```


2°) Programme 2

Programme Python qui demande de rentrer deux entiers naturels non tous les deux nuls et qui affiche leur PGCD :

On modifie le programme 1 de manière à faire afficher le PGCD.

```
a=int(input(" nbr1 : "))
b=int(input(" nbr2 : "))
d=0
for i in range(1,min(a,b)+1):
    if a%i==0 and b%i==0:
       d=i
print(d)
```

Version avec un while:

```
a=int(input(" nbr1 : "))
b=int(input(" nbr2 : "))
d=0
while a%i!=0 and b%i==0:
      d=i
print(d)
```

3°) Programme 3

On propose une variante du programme un avec une liste.
Si on fait afficher la liste, on peut modifier le programme en demandant l'affichage du maximum de cette liste (dernier élément de la liste, car les éléments de la liste sont rangés dans l'ordre croissant).

4°) Programme 4

Les variables *a* et *b* saisies en entrée sont des entiers naturels non nuls.

On commence par remarquer que le PGCD est inférieur ou égal à *a* et *b* (puisque c'est un diviseur de chacun des deux entiers) donc à leur minimum. Ce résultat sera énoncé dans le **III. 1°)**.

Entrées :
Saisir *a* et *b*

Initialisation :
$d \leftarrow \min(a, b)$

Traitement :
Tantque $d \not| a$ ou $d \not| b$ **Faire**
    $d \leftarrow d - 1$
FinTantque

Sortie :
Afficher *d*

$\min(a,b)$ désigne le minimum des entiers *a* et *b*, c'est-à-dire le plus petit des nombres *a* et *b*. déjà dit

```
a=int(input(" nbr1 : "))
b=int(input(" nbr2 : "))
d=min(a,b)
while a%d !=0 or b%d!=0:
      d=d-1
print(d)
```

Programme Python en version fonction :

```
def pgcd(a,b) :
    d=min(a,b)
    while a%d !=0 or b%d!=0:
          d=d-1
    return d
```

Remarque :
Lorsque *a* divise *b* ou *b* divise *a*, alors *d* divise *a* et *d* divise *b*.
Dès le début, la condition « $d \nmid a$ ou $d \nmid b$ » est donc fausse puisque c'est la négation de « *d* divise *a* et *d* divise *b* ». Par conséquent, il n'y a pas de boucle.
L'algorithme fournit le minimum de *a* et de *b* en sortie, qui est bien le PGCD de *a* et de *b*.

Il est facile de programmer cet algorithme sur calculatrice en utilisant par exemple la fonction reste(pour traduire la non divisibilité dans la condition du test.

Compte tenu du nombre important d'opérations à effectuer, le programme présente peu d'intérêt en pratique mais est intéressant sur le plan théorique.
Dans la suite du cours, nous allons étudier l'algorithme d'Euclide bien plus intéressant aussi bien sur le plan pratique que sur le plan théorique.

II. Rappels sur les nombres premiers entre eux et lien avec le PGCD

1°) Définition [nombres premiers entre eux]

On dit que deux entiers relatifs *a* et *b* sont **premiers entre eux** pour exprimer que leurs seuls diviseurs communs sont 1 et – 1.

2°) Exemple

25 et 42 sont premiers entre eux.

3°) Équivalences à retenir

a et *b* sont premiers entre eux ⇔ les seuls diviseurs communs à *a* et *b* sont – 1 et 1.

a et *b* sont premiers entre eux ⇔ leur seul diviseur commun positif est 1.

4°) Propriété [lien avec le PGCD]

a et *b* sont deux entiers relatifs quelconques.

Par définition, *a* et *b* sont premiers entre eux ⇔ $\mathcal{D}(a) \cap \mathcal{D}(b) = \{1;-1\}$.

On peut donc énoncer la propriété suivante :

a et *b* sont premiers entre eux si et seulement si leur PGCD est égal à 1.

Autrement dit, *a* et *b* sont premiers entre eux ⇔ $\text{PGCD}(a;b) = 1$.

5°) Rappel d'un résultat [combinaison linéaire égale à 1]

_a_ et _b_ sont deux entiers relatifs.
S'il existe des entiers relatifs _u_ et _v_ tels que $au+bv=1$, alors _a_ et _b_ sont premiers entre eux.

On a $\mathcal{D}(a,b) \subset \mathcal{D}(au+bv) = \mathcal{D}(1)$ donc $\mathcal{D}(a,b) = \{1;-1\}$.
On en déduit que *a* et *b* sont premiers entre eux.

Application :

Deux entiers consécutifs sont premiers entre eux donc le PGCD de deux entiers consécutifs est égal à 1.

III. Premières propriétés du PGCD

1°) Propriété 1

Le PGCD de deux entiers naturels non nuls est un diviseur de chacun de ces entiers naturels. Il est donc inférieur ou égal à chacun des deux entiers.

Cette propriété se généralise à plusieurs entiers naturels.

2°) Propriété 2

• Énoncé

a et *b* sont deux entiers relatifs non tous les deux nuls.

On a : $\text{PGCD}(a;b) = \text{PGCD}(|a|;|b|)$.

• Démonstration

On a les égalités suivantes d'ensembles $D(a) = D(|a|)$ et $D(b) = D(|b|)$.

Le résultat en découle immédiatement.

• Utilisation

Cette propriété permet de toujours se ramener au PGCD de deux entiers naturels.

• Complément

Avec les notations précédentes, on a : $\text{PGCD}(a\,;b) = \text{PGCD}(a\,;-b) = \text{PGCD}(-a\,;b) = \text{PGCD}(-a\,;-b)$.

3°) Propriété 3

• Énoncé

a est un entier relatif non nul. On a : $\textbf{PGCD}(a\,;0) = \lvert a \rvert$.

• Démonstration

$D(a) \cap D(0) = D(a) \cap \mathbb{Z} = D(a)$

Le plus grand élément de $D(a)$ est $|a|$.

4°) Propriété 4 [PGCD de deux entiers dont l'un divise l'autre]

• Énoncé

a est un entier naturel non nul et b est un entier relatif. Si a divise b, alors $\textbf{PGCD}(a\,;b) = a$.

• Démonstration

On suppose que $a \mid b$.

On a donc $D(a) \subset D(b)$.

D'où $D(a) \cap D(b) = D(a)$. On en déduit le résultat.

5°) Propriété 5

• Énoncé

a est un entier relatif quelconque. On a $\textbf{PGCD}(1\,;a) = 1$.

• Démonstration

$1 \mid a$ donc, d'après la propriété 4, on a $\text{PGCD}(1\,;a) = 1$.
On peut aussi écrire $D(1) \cap D(a) = D(1) = \{1\,;-1\}$.

6°) Propriété 6

• Énoncé

a est un entier naturel non nul. On a $\textbf{PGCD}(a\,;a) = a$.

• Démonstration

$a \mid a$ donc d'après la propriété 3, on a $\text{PGCD}(a\,;a) = a$.

On peut aussi écrire $D(a) \cap D(a) = D(a)$.

IV. Algorithme d'Euclide ou méthode des divisions successives

1°) Principe et exemples

Principe :
On se donne au départ un couple formé de deux entiers naturels.
La méthode consiste à effectuer des divisions euclidiennes successives.
On commence par diviser a par b. On obtient un reste r.
On divise b par r et ainsi de suite jusqu'à obtenir un reste nul.
On s'arrête dès que l'on obtient un reste nul.
Il est évident que si le reste r vaut 0 dès le début, on s'arrête à la première étape.

Exemples :

► couple (1636 ; 1128)

$1636 = 1128 \times 1 + 508$
$1128 = 508 \times 2 + 112$
$508 = 112 \times 4 + 60$
$112 = 60 \times 1 + 52$
$60 = 52 \times 1 + 8$
$52 = 8 \times 6 + 4$
$8 = 4 \times 2 + 0$

Nous verrons que le PGCD de 1636 et 1128 est égal à 4 (dernier reste non nul).

► couple (24 ; 3)

$24 = 3 \times 8 + 0$

2°) Lemme d'Euclide (rappel)

• Énoncé [lemme d'Euclide]

a, *b*, *c*, *d* sont des entiers relatifs tels que $a = bc + d$.

Alors on a l'égalité d'ensembles : $\boldsymbol{D}(a) \cap \boldsymbol{D}(b) = \boldsymbol{D}(b) \cap \boldsymbol{D}(d)$.

• Conséquence

Lorsque *a* et *b* ne sont pas tous les deux nuls, *b* et *d* ne sont pas non plus tous les deux nuls et on a l'égalité : $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;d)$.

On peut limiter les hypothèses à « b non nul ».

L'énoncé et la démonstration du lemme ont été vus dans le chapitre « Multiples et diviseurs ».

3°) Justification de l'algorithme d'Euclide dans le cas général

Considérons deux entiers naturels non nuls *a* et *b* tels que *b* ne divise pas *a*.

On notera que l'on travaille bien avec des entiers naturels.

L'algorithme d'Euclide consiste à remplacer le couple $(a\,;b)$ par des nombres de plus en plus petits qui ont le même ensemble de diviseurs communs.

On peut prendre *a* positif ou négatif.

1er cas : On suppose que *b* ne divise pas *a*

$a = bq_0 + r_0$ avec $0 < r_0 < b$

$b = r_0 q_1 + r_1$ avec $0 < r_1 < r_0$

$r_0 = r_1 q_2 + r_2$ avec $0 < r_2 < r_1$

⋮

$r_{n-2} = r_{n-1} q_n + r_n$ avec $0 < r_n < r_{n-1}$

$r_{n-1} = r_n q_{n+1} + 0$

En poursuivant le processus, on est obligé d'arriver après un nombre fini d'étapes à un reste nul, car les restes sont des entiers positifs qui vont en décroissant.

On peut invoquer le *principe de descente infinie* de Fermat : « Il n'existe pas de suite infinie strictement décroissante d'entiers naturels ».

On a $0 < r_n < r_{n-1} < \ldots < r_1 < r_0 < b$.

On notera que r_n est le dernier reste non nul.

On retiendra que cette présentation en une suite d'égalités de divisions euclidiennes écrites en lignes.

On a donc la chaîne d'égalités d'ensembles :
$\boldsymbol{D}(a) \cap \boldsymbol{D}(b) = \boldsymbol{D}(b) \cap \boldsymbol{D}(r_0) = \boldsymbol{D}(r_0) \cap \boldsymbol{D}(r_1) = \ldots = \boldsymbol{D}(r_{n-1}) \cap \boldsymbol{D}(r_n) = \boldsymbol{D}(r_n) \cap \boldsymbol{D}(0) = \boldsymbol{D}(r_n)$.

Ce principe de chaîne d'égalités d'ensembles avait déjà été abordé dans le chapitre sur « Multiples et diviseurs ».

L'algorithme d'Euclide fait apparaître une suite des restes r_0, r_1, r_2, …, r_n, $r_{n+1} = 0$ et des quotients q_0, q_1, q_2, …, q_n, q_{n+1} que nous allons utiliser dans la suite.

2e cas : On suppose que *b* divise *a*

Dans ce cas, la division euclidienne de *a* par *b* s'écrit $a = bq + 0$ avec *q* entier.
Dans ce cas, on écrit une seule division qui donne un reste nul.
On ne peut pas poursuivre.

L'algorithme d'Euclide est un outil de démonstration comme nous le verrons dans la suite du cours. Pour l'instant, bien que nous ayons employé l'expression « algorithme d'Euclide », nous n'avons pas à proprement parler d'algorithme. Nous avons décrit une méthode algorithmique pour déterminer le PGCD de deux entiers naturels basée sur la division euclidienne de deux entiers d'où son nom de méthode des divisions successives. L'écriture de l'algorithme proprement dit sera faite dans le paragraphe **V**.

4°) Propriété

***a* et *b* sont deux entiers naturels non nuls.**

Lorsque *b* ne divise pas *a*, le PGCD de *a* et *b* est égal au dernier reste non nul obtenu par l'algorithme d'Euclide appliqué au couple $(a\,;b)$.

On retiendra :

PGCD = dernier reste non nul obtenu par l'algorithme d'Euclide lorsqu'aucun entier n'est un multiple de l'autre

ou

PGCD = diviseur de la dernière division euclidienne (division de reste nul)

On reprend l'exemple du couple (1636 ; 1128) étudié dans le **1°)**.
D'après l'algorithme d'Euclide qu'on avait écrit, le PGCD de 1636 et de 1128 est égal à 4.

6°) Visualisation géométrique de l'algorithme d'Euclide

On cherche à paver un rectangle dont les dimensions sont des entiers naturel (pour une unité de longueur donnée) par des carrés dont le côté est un entier naturel.

Voir sur Internet :

• Wikipedia

• site de Thérèse Eveilleau « Mathématiques magiques »

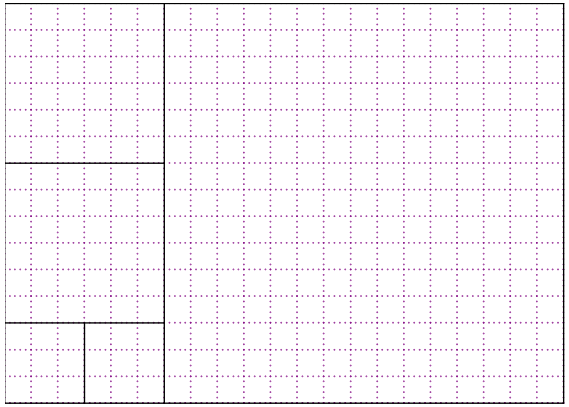
http://therese.eveilleau.pagesperso-orange.fr/pages/truc_mat/textes/euclide.htm

Choisir par exemple les nombres 100 et 45 ; on voit bien ce qui se passe.

• Daniel Mentrard

Dans la tradition grecque de l'Antiquité, un entier naturel était interprété comme une longueur. Un couple d'entiers naturels était considéré comme les longueurs des côtés d'un rectangle. Avec cette interprétation, le PGCD de deux entiers naturels est la longueur du côté du plus grand carré permettant de carreler entièrement ce rectangle. L'algorithme décompose ce rectangle en carrés, de plus en plus petits, par divisions euclidiennes successives, de la longueur par la largeur, puis de la largeur par le reste, jusqu'à un reste nul.

Dans le rectangle de dimensions $L = 21$ par $l = 15$ ci-dessous, par exemple, on peut glisser un carré de côté 15 mais il reste un rectangle de côtés 15 et 6, dans lequel on peut glisser deux carrés de côté 6 mais il reste un rectangle de côtés 6 et 3 que l'on peut carreler entièrement de carrés de côté 3. Les carrés de côté 6 ou 15 peuvent aussi se carreler en carrés de côté 3. Le rectangle entier peut se carreler en carrés de côté 3. Il n'existe pas de carrés plus grand permettant un tel carrelage.

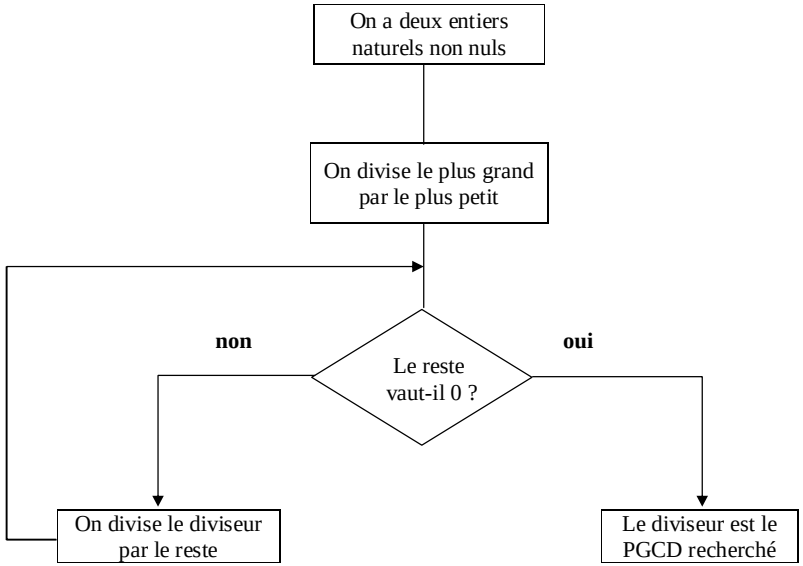


longueur = L = 21 et largeur = $l = 15$

$\mathrm{PGCD}(L\,;l) = 3$ = côté de la plus petite pièce carrée

En histoire des mathématiques, on appelle anthyphérèse ou antiphérèse une méthode qu'Euclide utilise pour calculer le PGCD de deux nombres ou démontrer que deux longueurs sont incommensurables.
Anthyphèrese vient du grec ἀνθυφαιρεῖν qui signifie soustraire alternativement.
La méthode est employée par Euclide une première fois dans le livre VII - proposition II pour calculer le PGCD de deux entiers : il préconise d'ôter au plus grand nombre le plus petit, autant que faire se pourra puis d'ôter le reste au plus petit des nombres etc. Bref, d'ôter systématiquement au plus grand des nombres le plus petit jusqu'à tomber sur un nombre qui mesure (qui divise) le précédent. Cette méthode est l'ancêtre de ce qu'on appelle aujourd'hui l'algorithme d'Euclide.
Elle est de nouveau employée dans le livre X, théorème 2 pour caractériser deux longueurs incommensurables (on parlerait de nos jours de longueurs dont le rapport est irrationnel). Il s'agit d'enlever alternativement à la plus grande longueur la plus petite, si le processus se poursuit indéfiniment, les longueurs sont incommensurables. Cette méthode aurait pu être employée, par exemple, pour démontrer l'irrationalité de la racine carrée de 2, mais il n'existe aucun témoignage de son utilisation pour une telle démonstration chez Euclide ou d'autres auteurs de la Grèce antique (à propos de $\sqrt{2}$ ou d'un autre).

8°) Organigramme de la méthode



Cet organigramme est à savoir par cœur.

V. Propriétés du PGCD

1°) Propriété [propriété fondamentale : ensemble des diviseurs de deux entiers naturels non tous les deux nuls]

• Énoncé

L'ensemble des diviseurs communs à a et b (a et b étant deux entiers non tous les deux nuls) est égal à l'ensemble des diviseurs de leur PGCD $\text{PGCD}(a\,;b)$.

• Démonstration

On peut supposer que a et b sont des entiers naturels non nuls.

1er cas : b ne divise pas a

1er cas : b positif

Cette propriété est un corollaire de la propriété de l'algorithme d'Euclide.
En effet, d'après l'algorithme d'Euclide, les diviseurs communs à a et b sont les diviseurs communs à b et r_0, à r_0 et à r_1, …, à r_{n-1} et à r_n c'est-à-dire les diviseurs de r_n (car r_n divise r_{n-1}).
Or r_n est le PGCD de a et b.

On peut écrire la suite d'égalités d'ensembles :

$$\boldsymbol{D}(a)\cap\boldsymbol{D}(b)=\boldsymbol{D}(b)\cap\boldsymbol{D}(r_0)=\boldsymbol{D}(r_0)\cap\boldsymbol{D}(r_1)=\ldots=\boldsymbol{D}(r_{n-1})\cap\boldsymbol{D}(r_n)=\boldsymbol{D}(r_n).$$

2e cas : b négatif

2e cas : b divise a

On a $\boldsymbol{D}(a)\cap\boldsymbol{D}(b)=\boldsymbol{D}(b)$ car $\boldsymbol{D}(b)\subset\boldsymbol{D}(a)$.
Or b est le PGCD de b et de a.

On peut aussi démontrer la propriété en utilisant l'identité de Bezout.

• Exemple

Si deux entiers ont leur PGCD égal à 6, alors leurs diviseurs communs sont les diviseurs de 6.

2°) Propriété [propriété multiplicative du PGCD ; effet de la multiplication par un entier sur le PGCD]

• Énoncé

a et b sont des entiers relatifs non tous les deux nuls.
k est un entier naturel non nul.
On a : $\text{PGCD}(ka\,;kb)=k\text{PGCD}(a\,;b)$.

Cette propriété peut être appelée « propriété d'homogénéité du PGCD ».

• Démonstration

On se ramène aisément au cas où a et b sont positifs.

Posons $d=\text{PGCD}(a\,;b)$.

On reprend l'algorithme d'Euclide appliqué au couple $(a\,;b)$ et on multiplie les deux membres de chaque égalité par k.

$$ka=kbq_0+kr_0$$

$$kb=kr_0q_1+kr_1$$

$$kr_0=kr_1q_2+kr_2$$

⋮

$$kr_{n-2}=kr_{n-1}q_n+kr_n \quad \text{avec } r_n=d$$

$$kr_{n-1}=kr_nq_{n+1}+0$$

Les égalités traduisent toutes des divisions euclidiennes.
Il s'agit donc de l'algorithme d'Euclide appliqué au couple $(ka\,;kb)$.

Le diviseur de la dernière division euclidienne est kr_n, soit kd.

Or on sait que PGCD = diviseur de la dernière division euclidienne (division euclidienne de reste nul).

On en déduit que $\text{PGCD}(ka\,;kb)=kd$.

• Commentaire

Lorsque $a\in\mathbb{Z}^*$ et $b\in\mathbb{Z}^*$, la propriété reste valable en remplaçant k par $|k|$.

• Exemple

Calcul de $\text{PGCD}(12000\,;32000)$.

On observe que $12000=12\times1000$ et que $32000=32\times1000$.
On utilise la propriété 2.

$$\begin{aligned}\text{PGCD}(12000\,;32000)&=\text{PGCD}(12\times1000\,;32\times1000)\\&=1000\times\text{PGCD}(12\,;32)\\&=1000\times4\qquad\text{(car on trouve aisément que }\text{PGCD}(12\,;32)=4\text{)}\\&=4000\end{aligned}$$

On pourrait aussi mettre 4 en facteur dans $\text{PGCD}(12\,;32)$.

• Propriété (conséquence de la propriété précédente)

a et b sont deux entiers relatifs non tous les deux nuls.
k est un diviseur positif commun à a et b.
Alors $\text{PGCD}\left(\frac{a}{k}\,;\frac{b}{k}\right)=\frac{1}{k}\text{PGCD}(a\,;b)$.

On notera que, comme k divise a et b, $\frac{a}{k}$ et $\frac{b}{k}$ sont des entiers.

Démonstration :

$$\begin{aligned}k\times\text{PGCD}\left(\frac{a}{k}\,;\frac{b}{k}\right)&=\text{PGCD}\left(k\times\frac{a}{k}\,;k\times\frac{b}{k}\right)\\&=\text{PGCD}(a\,;b)\end{aligned}$$

3°) Propriété [factorisation de deux entiers par leur PGCD]

• Énoncé

Soit a et b deux entiers relatifs non tous les deux nuls.
• Si $d=\text{PGCD}(a\,;b)$, alors il existe des entiers relatifs a' et b' premiers entre eux tels que $a=da'$ et $b=db'$.
• Réciproquement, si $a=da'$ et $b=db'$ avec $d\in\mathbb{N}^*$ et a' et b' premiers entre eux, alors $d=\text{PGCD}(a\,;b)$.

• Démonstration

On procède dans les deux sens.
La démonstration est très simple en appliquant les propriétés du paragraphe précédent.

☐ On pose $d=\text{PGCD}(a\,;b)$.
Par définition du PGCD, on a $d\in\mathbb{N}^*$, $d\mid a$ et $d\mid b$.
Il existe donc des entiers a' et b' tels que $a=da'$ et $b=db'$.

On peut appliquer la dernière propriété du paragraphe précédent car $d\neq0$.

$$\begin{aligned}\text{PGCD}(a'\,;b')&=\text{PGCD}\left(\frac{a}{d}\,;\frac{b}{d}\right)\\&=\frac{1}{d}\text{PGCD}(a\,;b)\\&=\frac{d}{d}=1\\&=1\end{aligned}$$

On en déduit que a' et b' sont premiers entre eux.

☐ On suppose que $a=da'$ et $b=db'$ avec $d\in\mathbb{N}^*$ et a' et b' premiers entre eux.

On a alors :

$$\begin{aligned}\text{PGCD}(a\,;b)&=\text{PGCD}(da'\,;db')\\&=d\text{PGCD}(a'\,;b')\\&=d\times1\\&=d\end{aligned}$$

• Conséquence

On peut donc énoncer le résultat suivant sous la forme d'une équivalence :

Soit a et b deux entiers relatifs non nous les deux nuls.
Soit d un entier naturel non nul.

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

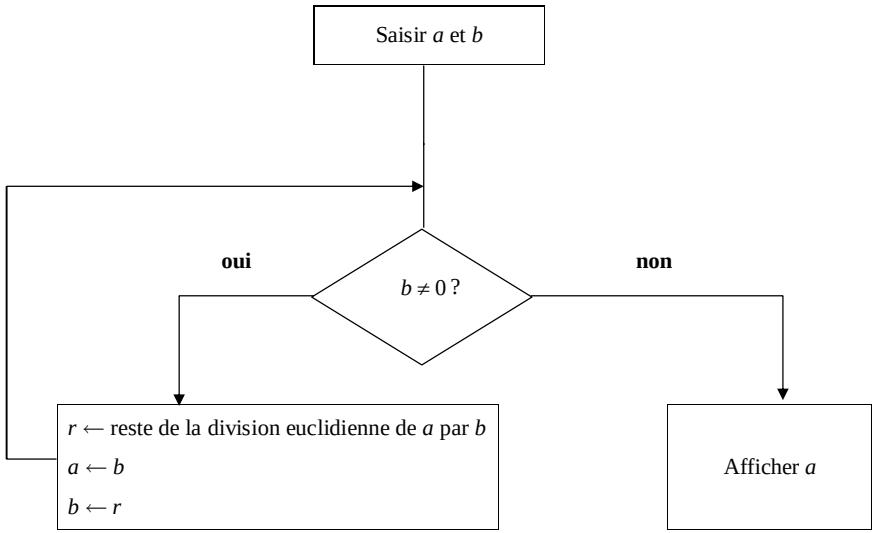
• Exemples d'utilisation

Voir exercices

VI. Algorithme d'Euclide : aspect algorithmique et programmation

1°) Organigramme de l'algorithme d'Euclide

On utilise une boucle avec test d'arrêt. On part de deux entiers relatifs a et b, a de signe quelconque et b positif ou nul.



2°) Écriture de l'algorithme d'Euclide « en langage intermédiaire »

- Effectuer la division euclidienne de a par b et noter r le reste ;
- Remplacer a par b ;
- Remplacer b par r ;
- Recommencer les calculs précédents jusqu'à ce qu'une division euclidienne donne un reste égal à 0.

Le PGCD est le dernier reste non nul.

Il faut connaître cet algorithme par cœur (autrement dit, il faut savoir le réécrire sans hésitation).

3°) Écriture de l'algorithme d'Euclide en langage naturel (formalisé)

Cet algorithme, quoique simple, n'est pas si facile à écrire.
On utilise une boucle « Tantque ».
Pour rédiger les instructions, on peut s'aider du tableau d'évolution des variables qui est présenté à titre d'exemple un peu plus loin.

Les variables sont a, b, r : entiers naturels. Les valeurs de a et b saisies en entrée ne doivent pas être toutes les deux nulles.

Entrée :
Saisir a
Saisir b

Traitement :
Tantque $b \neq 0$ **Faire**
    $r \leftarrow$ reste de la division euclidienne de a par b
    $a \leftarrow b$
    $b \leftarrow r$
FinTantque

Sortie :
Afficher a

On peut aussi utiliser les affectations parallèles, ce qui permet d'éviter d'introduire la variable r.

Entrée :
Saisir a et b

Traitement :
Tantque $b \neq 0$ **Faire**
    $a, b \leftarrow b$, reste de la division euclidienne de a par b
FinTantque

Sortie :
Afficher a

Il faut connaître cet algorithme par cœur (autrement dit, il faut savoir le réécrire sans hésitation).

Commentaires :

Variables :

Les variables sont :
- les deux entiers naturels, a et b, utilisés à chaque étape de l'algorithme (ce sont des variables *globales*) ;
- le reste r de la division euclidienne de a par b (c'est une *variable interne* ou *locale*).

On retiendra que l'on utilise 3 variables (on est obligé d'utiliser la variable r à l'« intérieur » de la boucle).

Entrées et traitement :

On saisit en entrée les deux entiers naturels dont on veut calculer le PGCD, puis on répète la division euclidienne jusqu'à ce que l'on ait un reste nul.

La condition (c'est-à-dire le test d'arrêt) « $b \neq 0$ » peut être remplacée de manière évidente par « $b > 0$ » car b est un entier naturel.

On peut rajouter un compteur afin de connaître le nombre d'étapes dans l'algorithme d'Euclide.

Sortie :

Le PGCD est le dernier reste non nul.
Une fois la boucle achevée, la variable a a pour valeur le dernier reste non nul.

Il est intéressant de faire tourner l'algorithme « à la main » pour deux entiers, par exemple 24 et 18.
Le mieux est d'utiliser un tableau d'évolution des variables.

Étape	$b \neq 0$ **?**	r	a	b
0			24	18
1	V	6	18	6
2	V	0	6	0
3	F			

Le PGCD de 24 et 18 est égal à 6.

Le fait de faire tourner « à la main » l'algorithme d'Euclide permet de voir que le PGCD correspond à la dernière valeur de a.

4°) Nombre d'étapes de l'algorithme d'Euclide ; théorème de Lamé (admis sans démonstration)

Gabriel Lamé, dit Lamé de la Droitière, né le 22 juillet 1795 à Tours, mort le 1er mai 1870 à Paris, est un mathématicien français.

Dans ce paragraphe, nous nous intéressons au « coût » de l'algorithme d'Euclide.

On ne peut pas connaître à l'avance le nombre d'étapes dans l'algorithme d'Euclide.

Cependant, le théorème de Lamé stipule que le nombre d'étapes de l'algorithme d'Euclide exécuté sur deux entiers naturels est inférieur ou égal à cinq fois le nombre de chiffres nécessaires pour écrire (en base dix) le plus petit de ces deux entiers.
On peut en fait être légèrement plus précis : le nombre d'étapes de l'algorithme d'Euclide exécuté sur deux entiers naturels a et b tels que $b \leqslant a$ est majoré par la partie entière de $\frac{\ln b}{\ln \varphi}$, où ln désigne le logarithme népérien et φ est le nombre d'or ($\varphi = \frac{1+\sqrt{5}}{2}$ par définition).

On sait que le nombre de chiffres de l'écriture de b en base dix est égal à $\mathrm{E}(\log b)+1$. Or par définition du logarithme décimal, $\log b = \frac{\ln b}{\ln 10}$. De plus, on peut déterminer le début de l'écriture décimale de la quantité $\frac{\ln 10}{\ln \varphi}$ grâce à la calculatrice. On trouve $\frac{\ln 10}{\ln \varphi} = 4,78497\ldots$. Ainsi, $\frac{\ln 10}{\ln \varphi} \leqslant 5$. Donc on retrouve bien le théorème de Lamé.
On peut noter que cette majoration est la meilleure possible, puisqu'elle est atteinte quand a et b sont deux nombres de Fibonacci consécutifs.

Le théorème des Lamé est donné à titre culturel. Il ne sert pas en pratique.

6°) Programme de la calculatrice pour trouver le PGCD

On peut se demander comment fonctionne la calculatrice pour trouver le PGCD de deux entiers naturels.
La calculatrice utilise un programme plus rapide que l'algorithme de d'Euclide.

7°) Programmation Python (fonction PGCD)

Rédaction en pseudo-code utilisant la possibilité d'affectations parallèles de plusieurs variables (affectations multiples).

Fonction pgcd(a, b)
    Tantque $b \neq 0$ **Faire**
        $a, b \leftarrow b$, reste de la division euclidienne de a par b
    FinTantque
    Renvoyer a

En langage Python (sans utiliser la fonction gcd !) :

L'instruction a%b donne le reste de la division euclidienne de a par b.

```
a=int(input(" nbr1 : "))
b=int(input(" nbr2 : "))
while b!=0:
    r=a%b
    a=b
    b=r
print(a)
```

Version fonction :

```
def pgcd(a,b):
    while b!=0:
          r=a%b
          a=b
          b=r
    return a
```

```
def pgcd(a,b):
    while b!=0:
          a,b=b,a%b
    return a
```

On utilise la possibilité d'une affectation parallèle (double assignation) en langage Python.

On peut échanger : `b,a=a%b,b`.
On peut remplacer l'instruction « `while b != 0 :` » par « `while b :` ».

Le jeudi 16 janvier 2020

La fonction tourne bien pour des négatifs à la condition de mettre une valeur absolue à la fin.
Le programme marche pour a quelconque et b non nul : (a, b) avec $a \in \mathbb{Z}$ et $b \neq 0$.
(0,23) marche.
(0,0), (23,0) ne marche pas.

Version récursive (hors programme) :

```
def pgcd(a,b) :
    r=a%b
    if r==0:
       return b
    else :
       return pgcd(b,r)
```

Julie Fiadino le 1-2-2021

VII. Combinaisons linéaires liées au PGCD

Commencer par un exemple
(fait comme cela le 26-1-2021 en maths experts)

Lemme :

a, b, c, d sont des entiers relatifs tels que $a = bc + d$.
d peut s'écrire comme combinaison linéaire à coefficients entiers relatifs de a et b.

Conséquence :

Soit a et b, deux entiers relatifs avec b non nul.
Le reste de la division euclidienne de a par b peut s'écrire comme combinaison linéaire à coefficients entiers relatifs de a et b.

1°) Lemme fondamental : restes de l'algorithme d'Euclide

● Étude (démonstration)

On considère deux entiers naturels a et b tels que b soit non nul et b ne divise pas a.

L'algorithme d'Euclide appliqué au couple $(a\,;b)$ permet d'écrire les égalités :

$a = bq_0 + r_0 \quad (0)$

$b = r_0q_1 + r_1 \quad (1)$

$r_0 = r_1q_2 + r_2 \quad (2)$

…

$r_{n-2} = r_{n-1}q_n + r_n$ avec $r_n \neq 0$

$r_{n-1} = r_nq_{n+1} + 0$

On avait déjà dit à la fin du chapitre « Multiples et diviseurs » que dans que dans une telle situation, les entiers r_0, r_1, r_2 … peuvent s'exprimer comme combinaisons linéaires à coefficients entiers de a et b.

(0) permet d'écrire $r_0 = a - bq_0$ donc $r_0 = au_0 + bv_0$ avec $u_0 = 1$ et $v_0 = -q_0$ qui sont des entiers.

(1) permet d'écrire $r_1 = b - r_0q_1 = b - (au_0 + bv_0)q_1 = -q_1u_0a + (1 - v_0q_1)b$ donc $r_1 = au_1 + bv_1$ avec $u_1 = -u_0q_1$ et $v_1 = 1 - v_0q_1$ qui sont des entiers.

Pas à pas, on exprime chaque reste comme combinaison linéaire de a et b à coefficients entiers jusqu'à r_n.

En poussant davantage le raisonnement, on peut définir des suites, ce qui permet d'écrire un algorithme qui, pour des valeurs de a et b saisies en entrée, affiche en sortie des valeurs de u et v (voir algorithmes et programmes en appendice).

● Énoncé

Chaque reste de l'algorithme d'Euclide peut s'exprimer comme combinaison linéaire à coefficients entiers relatifs de *a* et *b*.

Le résultat reste valable pour le reste nul de la dernière division euclidienne de l'algorithme d'Euclide, mais cela ne présente pas d'intérêt.

● Utilisation pratique

Nous verrons une présentation pratique permettant d'obtenir facilement ces combinaisons linéaires par descente de l'algorithme d'Euclide.
Cette présentation aura l'avantage de pouvoir être programmée aisément.

2°) Identité de Bezout [théorème]

● Énoncé

***a* et *b* sont des entiers relatifs non tous les deux nuls.**
On note *d* le PGCD de *a* et *b*.

Il existe $(u\,;v)\in\mathbb{Z}^2$ tel que $au+bv=d$.

Autre formulation :

Le PGCD de deux entiers relatifs a et b peut s'exprimer comme combinaison linéaire de a et b à coefficients entiers relatifs.

● Démonstration

On suppose que a et b sont des entiers naturels non tous les deux nuls. On se ramène aisément à ce cas.

1er cas : b est non nul et b ne divise pas a

On sait que dans l'algorithme d'Euclide appliqué à a et b, le dernier reste non nul r_n est égal à d.
Or d'après le lemme du **1°)**, r_n peut s'écrire comme combinaison linéaire de a et b à coefficients entiers.
Il existe donc deux entiers relatifs u et v tels que $au+bv=d$.

2e cas : b est non nul et divise a

Il existe donc un entier k tel que $a=kb$.
On sait que dans ce cas $d=b$.

On peut écrire $a-kb=0$ d'où $a-kb+b=b$ soit $a+(1-k)b=b$ ce qui donne donc $a+(1-k)b=d$.
On a bien exprimé d comme combinaison linéaire à coefficients entiers de a et b.

3e cas : b est nul

Dans ce cas, a est non nul et $d=a$.
On peut écrire $1\times a+0\times b=a$.

● Vocabulaire

On dit qu'un couple (u,v) d'entiers relatifs tel que $au+bv=d$ est un « couple de Bezout » pour les entiers a et b.

3°) Conséquence

● Identité de Bezout pour des entiers relatifs premiers entre eux

***a* et *b* sont deux entiers relatifs.**

Si *a* et *b* sont premiers entre eux, alors il existe des entiers relatifs *u* et *v* tels que $au+bv=1$.

On applique l'identité de Bezout dans le cas où $d=1$.

En rassemblant cette identité de Bezout avec la propriété rappelée dans **II. 5°)**, on obtient le théorème suivant qui est fondamental. Il s'agit d'une condition nécessaire et suffisante pour que deux entiers relatifs soient premiers entre eux.

● Théorème de Bezout

***a* et *b* sont deux entiers relatifs.**

a et b sont premiers entre eux si et seulement si il existe des entiers relatifs u et v tels que $au+bv=1$.

● Vocabulaire

Lorsque a et b sont deux entiers relatifs premiers entre eux, une égalité du type $au+bv=1$ où u et v sont deux entiers est appelée « égalité de Bezout » et le couple $(u\,;v)$ est appelé un « couple de Bezout » associé au couple $(a\,;b)$.
On dit aussi que u et v sont des coefficients de Bezout.

4°) Remarques

• Lorsque a et b sont deux entiers dont le PGCD est égal à d, l'identité de Bezout affirme l'existence d'un couple $(u\,;v)\in\mathbb{Z}^2$ tel que $au+bv=d$.

Il n'existe pas de formule permettant d'obtenir des expressions d'un tel couple en fonction de a et b.

En revanche, lorsque l'on connaît les valeurs numériques de a et b, il existe plusieurs méthodes pour trouver un tel couple.

• Lorsque a et b ont des valeurs simples, on peut chercher directement un tel couple [on essaie différents couples].

• Sinon, on peut aussi utiliser la méthode de la fonction affine.

• On peut aussi utiliser l'algorithme d'Euclide.

• Enfin, il existe même un algorithme facile à programmer permettant d'obtenir un tel couple.

L'étude du 1°) pour le lemme fondamental permet d'obtenir un tel couple en descendant l'algorithme d'Euclide. C'est ce que nous verrons dans l'exemple numérique du 5°).

On peut obtenir un tel couple dans des cas simples comme celui donné dans l'exemple qui suit.
$a=4$ et $b=3$ sont premiers entre eux : $4\times1+3\times(-1)=1$.

Dans les cas plus compliqués, on utilise l'algorithme d'Euclide. C'est l'objet du paragraphe suivant.

• Il n'y a pas unicité du couple $(u\,;v)$ dans le théorème.
Par exemple, pour $a=4$ et $b=3$, le couple $(-2\,;3)$ fonctionne également.
Nous verrons dans la suite, comment à partir d'un couple de Bezout, obtenir tous les autres.

• Attention, l'existence d'une relation du type $au+bv=d$ ne permet pas d'affirmer que d est le PGCD de a et b.
Exemple : $\forall n\in\mathbb{N}\quad 2(3n+5)-3(2n+1)=7$
Cette égalité ne permet pas d'affirmer que le PGCD de $3n+5$ et de $2n+1$ est égal à 7 pour tout entier naturel n.

5°) Obtention d'un couple de Bezout avec l'algorithme d'Euclide (détermination d'un couple de Bezout « à la main »)

Exemple : $a=47$ et $b=35$

L'algorithme d'Euclide appliqué au couple $(a\,;b)$ s'écrit $\begin{cases}47=35\times1+12\\35=12\times2+11\\12=11\times1+1\\11=11\times1\end{cases}$.

On peut en déduire que $\text{PGCD}(a\,;b)=1$.

On va chercher un couple de Bezout grâce à cet algorithme.

• **1ère méthode :** On « remonte » l'algorithme d'Euclide.

$1=12-11$

Or $11=35-12\times2$

Donc $1=12-(35-12\times2)=3\times12-35$.

Or $12=47-35$.

Donc $1=3\times(47-35)-35$.

Finalement, on obtient : $1=3\times47-4\times35$ que l'on peut écrire sous la forme $3\times47-4\times35=1$.

Ainsi le couple $(3\,;-4)$ est un couple de Bezout.

► Voici la présentation classique :

$1=12-11$

$1=12-(35-12\times2)$

$1=3\times12-35$

$1=3\times(47-35)-35$

$1=3\times47-4\times35$

• **2e méthode :** On « descend » l'algorithme d'Euclide.

$\begin{cases}a=b+12\\b=12\times2+11\\12=11\times1+1\\11=11\times1\end{cases}$

$12=a-b$

$b=(a-b)\times2+11$ qui donne $11=3b-2a$.

$a-b=3b-2a+1$, ce qui donne $3a-4b=1$.

► Voici une présentation pratique sous forme de tableau :

$47 = 35\times 1+12$

$35 = 12\times 2+11$

$12 = 11\times 1+1$

$11 = 11\times 1+0$

On utilise les quotients.

		$a=47$	$b=35$		
47	L_1	1	0		
35	L_2	0	1		
12	L_3	1	-1	$L_3 \leftarrow L_1 - 1\times L_2$	$47 = 35\times 1+12$
11	L_4	-2	3	$L_4 \leftarrow L_2 - 2\times L_3$	$35 = 12\times 2+11$
1	L_5	3	-4	$L_5 \leftarrow L_3 - 1\times L_4$	$12 = 11\times 1+1$
		↑	↑		
		u	v		

On vérifie que à chaque étape les nombres de la colonne de gauche s'écrivent comme combinaisons linéaires de a (c'est-à-dire 47) et de b (c'est-à-dire 35) avec les coefficients u et v des deux colonnes de droite.

$47 = 1\times a+0\times b$
$35 = 0\times a+1\times b$
$12 = 1\times a-1\times b$
$11 = -2\times a+3\times b$
$1 = 3\times a-4\times b$

6°) Obtention d'un couple de Bezout

En pratique, lorsque l'on connaît les valeurs de a et b, on peut obtenir un couple de Bezout « à la main » en effectuant l'algorithme d'Euclide puis en le « descendant » ou en le « remontant ».
On peut aussi utiliser :
- le programme de calculatrice (algorithme et programme correspondant donnés en appendice) ;
- une méthode plus astucieuse en utilisant une fonction affine (voir le paragraphe 6°)) ;
- utiliser des sites Internet (par exemple le site http://www.dcode.fr/identite-bezout).

Programme Python :

```
def bezout(a, b):
    (u0, v0, u1, v1)=(1, 0, 0, 1)
    while b!=0:
          (q, r) = divmod(a, b)
          (a, b) = (b, r)
          (u0, v0, u1, v1) = (u1, v1, u0-q*u1, v0-q*v1)
    return (u0, v0)
```

7°) Autre méthode simple pour déterminer un couple de Bezout

Exemple : Déterminons un couple $(u, v)\in\mathbb{Z}^2$ tel que $141u-34v=1$.

Dans cette égalité, on isole u ou v.

1ère méthode : On isole v.
On obtient $v=\dfrac{141u-1}{34}$.

On « rentre » alors la fonction $f : x\mapsto \dfrac{141x-1}{34}$ dans la calculatrice (dans $\boxed{f(x)}$). On notera qu'il s'agit d'une fonction affine.

On effectue le réglage nécessaire pour obtenir un tableau de valeurs de $f(x)$ pour des valeurs entières de x (pour cela, le « début » de la table doit être un entier relatif et le « pas » doit être égal à 1).

On détermine la première valeur de x pour laquelle $f(x)$ est un entier relatif.
On trouve $f(7)=29$.
Le couple obtenu est $(7\,;29)$.

2e méthode : On isole u.
On obtient $u=\dfrac{34v+1}{141}$.

On « rentre » alors la fonction $g : x\mapsto \dfrac{34x+1}{141}$ dans la calculatrice.
Grâce au tableau de valeurs, on trouve $g(29)=7$.
On retrouve le couple $(7\,;29)$ obtenu avec la 1ère méthode.

8°) Conséquence de l'identité de Bezout [propriété]

● Énoncé

a et b sont des entiers relatifs non tous les deux nuls.
On note d le PGCD de a et b.
Tout multiple de d peut s'exprimer comme combinaison linéaire de a et de b.

• Démonstration

D'après le théorème de Bezout, il existe deux entiers relatifs u et v tels que $au+bv=d$.

Pour tout entier relatif k, on peut donc écrire $kau+kbv=kd$ ou encore $a\times(ku)+b\times(kv)=kd$.

Or u, v, k sont des entiers relatifs donc ku et kv sont aussi des entiers relatifs.

Cette dernière égalité montre que kd s'exprimer comme combinaison linéaire de a et b à coefficients entiers relatifs.

• Exemple

On prend $a=5$ et $b=3$.

a et b sont premiers entre eux ; leur PGCD vaut 1.

D'après la propriété, tout multiple de 1, c'est-à-dire tout entier relatif, peut s'exprimer comme combinaison linéaire à coefficients entiers relatifs de a et b.

En pratique, on part d'une égalité de Bezout entre a et b, par exemple $2\times5-3\times3=1$.

Pour exprimer un entier relatif n quelconque, on multiple les deux membres par n : $2n\times5-3n\times3=n$.

Par exemple, pour $n=100$, $100=200\times5-300\times3$.

9°) Une nouvelle propriété du PGCD pour le produit

• Énoncé

Si un entier est premier avec deux entiers, alors il est premier avec leur produit.

• Démonstration

1ère démonstration :

Soit a, b, c trois entiers tels que a soit premier avec b et avec c.

Démontrons que a est premier avec bc.

D'après le théorème de Bezout,
• il existe des entiers relatifs u et v tels que $au+bv=1$;
• il existe des entiers relatifs u' et v' tels que $au'+cv'=1$.

Par produit membre à membre des deux égalités précédentes, on obtient : $(au+bv)(au'+cv')=1$.

En développant, on obtient alors $a^2uu'+aucv'+bvau'+bvcv'=1$ ce qui donne :

$$\underbrace{a\underbrace{(auu'+ucv'+bvu')}_{U}}_{\in\mathbb{Z}}+\underbrace{bc\underbrace{(vv')}_{V}}_{\in\mathbb{Z}}=1.$$

On obtient une combinaison linéaire de a et bc à coefficients entiers égale à 1.
D'après le théorème de Bezout, a et bc sont donc premiers entre eux.

2e démonstration :

Soit d un diviseur positif commun à a et bc.

On a $d\mid a$ donc $d\mid ab$.

On a $d\mid ab$ et $d\mid bc$.

Par suite, $d\mid \text{PGCD}(ab\,;bc)$.

$\text{PGCD}(ab\,;bc)=b\text{PGCD}(a\,;c)=b\times1=b$ ($\text{PGCD}(a\,;c)=1$ puisque a et c sont premiers entre eux par hypothèse).

On en déduit que $d\mid b$.

On a donc $d\mid a$ et $d\mid b$.

Or a et b sont premiers entre eux par hypothèse, donc $d=1$.

On en conclut que le seul diviseur positif commun à a et bc est 1 et donc que a est premier avec bc.
Généralisation :

Si a est premier avec b_1, b_2, …, b_n, alors a est premier avec $b_1b_2..b_n$.

Cas particulier :

• Exemple d'utilisation

a et b sont deux entiers.
Si a est premier avec b, alors a est premier avec b^2.

Idée de démonstration : On applique la propriété avec $b=c$.

• Corollaire

Si a et b sont deux entiers premiers entre eux, alors pour tout couple $(n\,;\,p)$ d'entiers naturels a^n et b^p sont premiers entre eux.

VIII. Théorème de Gauss

1°) Énoncé

a, b et c sont trois entiers relatifs.
Si a divise le produit bc et a est premier avec b, alors a divise c.

2°) Démonstration

On suppose que :

- $a \mid bc$
- a et b sont premiers entre eux.

Démontrons que $a \mid c$.

1ère méthode :

a et b sont premiers entre eux donc, d'après le théorème de Bezout, il existe deux entiers relatifs u et v tels que $au+bv=1$.
En multipliant les deux membres de cette égalité par c, on obtient l'égalité : $acu+bcv=c$.

Or $a \mid bc$ par hypothèse et $a \mid a$ de manière évidente.
Donc a divise toute combinaison linéaire de a et bc à coefficients entiers relatifs.
On en déduit que $a \mid acu+bcv$ et, par suite, $a \mid c$.

2e méthode : (dans le cas où a, b, c sont non nuls pour pouvoir parler de PGCD)

a est premier avec b donc $\text{PGCD}(a\,;b)=1$.

$$\begin{aligned}\text{PGCD}(ac\,;bc) &= c\times 1\\ &= c\end{aligned}$$

$a \mid bc$

a est un diviseur commun à ac et bc.
Donc a divise le PGCD de ac et de bc d'où $a \mid c$.

3°) Application à un type d'équations diophantiennes

On s'intéresse à des équations du type $ax+by=c$ d'inconnue $(x\,;\,y)\in\mathbb{Z}^2$ où a, b, c sont des entiers relatifs.

Cas particulier où l'un des coefficients a ou b au moins est égal à 1 ou à – 1 :

Exemple :

$x+2y=5$; $3x-y=1$

Dans ces deux cas, on résout très facilement les deux équations.

Cas général où aucun des coefficients a ou b est égal à 1 ou à – 1 :

Exemple :

On considère l'équation diophantienne $7x-11y=3$ (E) d'inconnue $(x\,;\,y)\in\mathbb{Z}^2$.
a) Vérifier que le couple $(13\,;8)$ est une solution particulière de (E).
b) En déduire toutes les solutions de (E).

Résolution :

a) On a : $7\times 13-11\times 8=3$ donc le couple $(13\,;8)$ est une solution particulière de (E).

b)

1ère partie :

$$\begin{aligned}(\text{E}) &\Leftrightarrow 7x-11y=3\\ &\Leftrightarrow 7x-11y=7\times 13-11\times 8\\ &\Leftrightarrow 7(x-13)=11(y-8)\quad (\text{E}')\end{aligned}$$

On note (E') l'égalité de la 3e ligne car on va s'en servir après.
On ne donne pas de notation à l'égalité qui apparaît sur la deuxième ligne.

On a : $(\text{E}) \Leftrightarrow (\text{E}')$.

On en déduit que $11 \mid 7(x-13)$ avec 11 et 7 premiers entre eux.
D'après le théorème de Gauss, il en résulte que $11 \mid x-13$.
Il existe donc $k\in\mathbb{Z}$ tel que $x-13=11k$.
En remplaçant $x-13$ par $11k$ dans l'équation (E'), on obtient : $7\times 11k=11(y-8)$ soit $y-8=7k$.
D'où finalement : $x=13+11k$ et $y=8+7k$.

2e partie :
Pour tout entier relatif k, $(13+11k\,;8+7k)$ est un couple d'entiers relatifs.
On vérifie que $\forall k\in\mathbb{Z}\quad 7\times(13+11k)-11\times(8+7k)=3$.
On en déduit que tout couple $(13+11k\,;8+7k)$ avec $k\in\mathbb{Z}$ est solution de (E).

Conclusion :

L'ensemble des solutions de (E) est $S=\{(13+11k\,;8+7k),k\in\mathbb{Z}\}$.

Commentaires :

(E) admet une infinité de solutions.
On obtient des solutions de (E) en remplaçant k par des valeurs particulières.

On remarque que pour $k=0$, on « retombe » sur la solution particulière, à savoir le couple $(13;8)$.

Remarques :

• Si on prend un autre couple solution particulière, les solutions seront données sous une forme différente mais ce sera toujours le même ensemble de solutions.

• Lorsque la solution particulière n'est pas évidente à trouver, on peut utiliser le programme sur calculatrice de recherche d'un couple de Bezout ou la méthode consistant à utiliser une fonction affine.

• L'adjectif « diophantien » vient de Diophante (III^{e} siècle après Jésus-Christ) qui est l'un des plus grands mathématiciens grecs de l'Antiquité.

• Les couples de Bezout correspondent à un paramétrage.
Ils correspondent à une paramétrisation de la droite d'équation $7x-11y=3$.

Application des équations diophantiennes linéaires à la résolution de problèmes concrets : voir exercices.

Utilisation d'un logiciel de calcul formel tels que dcode (en ligne)

La prise en main du logiciel pour la résolution des équations est extrêmement intuitive.

On commence par taper l'équation.

On précise que :
- les inconnues sont x et y ;
- l'ensemble de résolution est $\mathbb{Z}$ (mathématiquement, pour nous, c'est plutôt $\mathbb{Z}^2$).

Par exemple, le logiciel permet de dire que les solutions de l'équation $2x+3y=8$ sont les couples $(x\,;y)$ avec $x=3k+1$ et $y=2-2k$, k décrivant $\mathbb{Z}$.

k est désigné par c_1.

Étude d'existence de solutions :

Propriété (fondamentale) :

Soit a, b, c trois entiers relatifs.
On s'intéresse à l'équation $ax+by=c$ (E) d'inconnue $(x,y)\in\mathbb{Z}^2$.
On note d le PGCD de a et de b.

1er cas : c est un multiple de d
Dans ce cas, (E) admet une solution (et même une infinité de solutions).

2^{e} cas : c n'est pas multiple de d
Dans ce cas, (E) n'admet pas de solution.

Démonstration :

On raisonne dans les deux sens.
On note d le PGCD de a et de b.

Conséquence : propriété (à connaître par cœur) [condition nécessaire et suffisante pour qu'une équation de la forme $ax+by=c$ admette des solutions]

Soit a, b, c trois entiers relatifs.

L'équation $ax+by=c$ (E) d'inconnue $(x,y)\in\mathbb{Z}^2$ admet (au moins) une solution si et seulement si c est un multiple du PGCD de a et de b.

Démonstration :

On raisonne dans les deux sens.
On note d le PGCD de a et de b.

Sens 1 : On suppose qu'il existe un couple $(x_0,y_0)\in\mathbb{Z}^2$ solution de (E).
On a donc $ax_0+by_0=c$ (1).
On sait que d divise a et que d divise b donc d divise toute combinaison linéaire de a et de b à coefficients entiers relatifs.
Or l'égalité (1) fait apparaître c comme combinaison linéaire de a et de b à coefficients entiers relatifs.
On en déduit que d divise c.

Variante : On peut alors écrire $a=da'$ et $b=db'$. L'égalité peut donc s'écrire $da'x_0+db'y_0=c$ soit $da'x_0+db'y_0=c$.

Sens 2 : On suppose que c est un multiple de d.
On a démontré que c peut s'exprimer comme combinaison linéaire de a et b à coefficients entiers relatifs.
Ainsi, (E) admet une solution.

Exemple : L'équation $5x+15y=7$ n'admet aucune solution dans Z^2.

On peut donc écrire $c = \lambda d$ où λ est un entier relatif.
D'après le théorème de Bezout, on sait qu'il existe un couple $(x_1 ; y_1)$ d'entiers relatifs tels que $ax_1 + by_1 = d$.
En multipliant les deux membres par λ, on obtient l'égalité $\lambda a x_1 + \lambda b y_1 = \lambda d$ ce qui donne $a(\lambda x_1) + b(\lambda y_1) = c$.
Le couple $(\lambda x_1 ; \lambda y_1)$ est donc une solution de (E).

Méthode à retenir pour résoudre une équation du type $ax + by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$ avec *a*, *b*, *c* entiers relatifs.

1) On calcule $\text{PGCD}(a, b)$.
2) S'il est différent de 1, soit on simplifie l'équation, si on ne peut pas, elle n'a pas de solution.
3) S'il est égal à 1 (c'est le cas en particulier après simplification), on cherche une solution particulière.
4) On soustrait l'équation à résoudre avec l'égalité donnée par la solution particulière.
5) On utilise le théorème de Gauss pour trouver les solutions.

4°) Propriété sur produit et nombres premiers entre eux [divisibilité d'un entier par un produit d'entiers premiers entre eux deux]

• Énoncé

a, *p* et *q* sont des entiers relatifs.
On suppose que *p* et *q* sont premiers entre eux.
Si $p \mid a$ et $q \mid a$, alors $pq \mid a$.

• Démonstration

On fait les hypothèses suivantes :

p et *q* sont premiers entre eux.
$p \mid a$
$q \mid a$

$p \mid a$ par hypothèse donc il existe un entier *k* tel que $a = pk$ (1).

$q \mid a$ par hypothèse donc il existe un entier *l* tel que $a = ql$ (2).

(1) et (2) donnent $pk = ql$ (3).

D'après (3), on peut affirmer que $q \mid pk$.

Or *q* est premier avec *p* par hypothèse donc d'après le théorème de Gauss, $q \mid k$.

On en déduit qu'il existe un entier *m* tel que $k = mq$ (4).

On reprend l'égalité (1).
Compte tenu de (4), (1) donne $a = p(mq)$ soit $a = m(pq)$.

On en déduit que $pq \mid a$.

• Remarque sur l'énoncé

On peut formuler l'énoncé sous la forme d'une équivalence.

a, *p* et *q* sont des entiers relatifs.
On suppose que *p* et *q* sont premiers entre eux.
($p \mid a$ et $q \mid a$) $\Leftrightarrow$ $pq \mid a$

C'est sous cette forme qu'il est parfois utilisé.

• Généralisation à des entiers naturels premiers entre eux deux à deux

Si un entier est divisible par des entiers premiers entre eux deux à deux, alors il est divisible par leur produit.

• Exemple d'application important : critère de divisibilité par 6

On applique la propriété avec $p = 2$ et $q = 3$.

On a l'équivalence suivante : $6 \mid a \Leftrightarrow (2 \mid a$ et $3 \mid a)$.

Un entier relatif est divisible par 6 si et seulement si il est divisible par 2 et par 3.

De la même façon, on peut crée des critères de divisibilité par différents nombres : 21, 30 etc.

• L'hypothèse « *p* et *q* premiers entre eux » est indispensable comme le montre le contre-exemple suivant.
2 divise 12 et 6 divise 18 mais 12 $(= 2 \times 6)$ ne divise pas 18.

IX. PPCM de deux entiers relatifs

1°) Introduction

La notion de multiple commun et de PPCM a été rencontrée dès la classe de 5e dans le cours sur les fractions ainsi qu'à l'occasion de problèmes concrets (recherche d'un nombre présent dans deux tables de multiplication différentes).

On est fréquemment amener un dénominateur commun à plusieurs fractions lorsque l'on veut :
- les comparer ;
- les additionner ou les soustraire.

On cherche chaque fois le plus dénominateur commun.

Exemple :

On considère les fractions $\frac{1}{6}$ et $\frac{3}{8}$.

Pour les écrire avec un même dénominateur, on cherche le plus petit « résultat » en commun dans la table de multiplication de 6 et 8, ici : 24 ; 24 est appelé le PPCM de 6 et 8.

On a $\frac{1}{6}=\frac{4}{24}$ et $\frac{3}{8}=\frac{9}{24}$.

On peut alors les comparer, les additionner et les soustraire.

$\frac{1}{6}<\frac{3}{8}$

$\frac{1}{6}+\frac{3}{8}=\frac{4}{24}+\frac{9}{24}=\frac{13}{24}$ (on écrit alors les deux fractions avec le dénominateur avec le dénominateur 24 avant d'effectuer l'addition).

$\frac{1}{6}-\frac{3}{8}=\frac{4}{24}-\frac{9}{24}=-\frac{5}{24}$

Nous reviendrons sur l'application du PPCM aux fractions un peu plus loin dans la suite du cours.

2°) Notations

Pour tout entier relatif *a*, on note :
- $M(a)$ l'ensemble des multiples de *a*. $M(a)$ est donc l'ensemble des entiers relatifs de la forme *ka* avec $k\in\mathbb{Z}$.
- $M^{+}(a)$ l'ensemble des multiples strictement positifs de *a*.

3°) Multiples communs à deux entiers relatifs

Dans tout ce paragraphe, *a* et *b* sont deux entiers relatifs.

- $M(a)\cap M(b)$ est l'ensemble des multiples communs à *a* et *b*.

On notera que $M(a)\cap M(b)$ contient 0 et *ab*.

- $M^{+}(a)\cap M^{+}(b)$ est l'ensemble des multiples strictement positifs communs à *a* et *b*.

On notera que $M^{+}(a)\cap M^{+}(b)$ contient $|ab|$.

Lorsque *a* et *b* sont non nuls, $M^{+}(a)\cap M^{+}(b)$ est donc non vide.

Tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.

3°) Définition

Étant donnés deux entiers relatifs *a* et *b* non nuls, le **plus petit commun multiple** de *a* et *b* est le plus petit élément de $M^{+}(a)\cap M^{+}(b)$.
On le note $\text{PPCM}(a;b)$.

On peut dire que le PPCM de deux entiers relatifs non nuls est le plus petit élément entier naturel strictement positif qui est divisible par chacun des deux entiers.

4°) Exemple

Déterminer $\text{PPCM}(20;6)$ à l'aide de la définition.

$M^{+}(20)=\{20;40;60;80;\ldots\}$
$M^{+}(6)=\{6;12;18;24;30;36;42;48;54;60;\ldots\}$

On en déduit que $\text{PPCM}(20;6)=60$.

60 est le plus petit entier strictement positif divisible par 20 et par 6.
On peut vérifier le résultat à l'aide de la calculatrice comme cela est indiqué au **7°)** de cette partie.

5°) Remarques

- Le plus petit commun multiple positif ou nul de deux entiers naturels non nuls est 0.
- Le plus petit commun multiple strictement positif de deux entiers naturels non nuls est le PPCM.
- Le PPCM de deux entiers naturels non nuls est au moins égal à 1.
- $\forall a\in\mathbb{N}^{*}\quad \text{PPCM}(a;a)=a$
- $\forall a\in\mathbb{N}^{*}\quad \text{PPCM}(a;1)=a$

• Le seul multiple de 0 est 0. Pour tout entier relatif a, on pose donc $\text{PPCM}(a\,;0)=0$.

• On définit de même le PPCM de deux entiers relatifs a et b comme le plus petit multiple strictement positif commun à a et b. On le note encore $\text{PPCM}(a\,;b)$. Déjà dit dans la définition (**noté le 5-3-2020**)

On vérifie alors aisément que $\text{PPCM}(a\,;b)=\text{PPCM}(|a|\,;|b|)$.

• a est un entier relatif et b est un entier naturel.
Si $a \mid b$, alors $\text{PPCM}(a\,;b)=b$.

• Comme pour le PGCD, on peut définir le PPCM de plusieurs entiers non nuls. Nous y reviendrons dans le paragraphe **XII**.
• Si a et b sont deux entiers naturels non nuls, alors $\text{PPCM}(a\,;b)\geqslant \max(a\,;b)$.

6°) Exemples « classiques »

Si on veut paver un carré (dont les côtés mesurent un nombre entier de cm) en juxtaposant des rectangles (tous disposés de la même manière) dont les côtés ont pour longueurs 24 cm et 60 cm et si on demande de chercher quelle est la valeur minimale possible pour la longueur du côté du carré, on cherche le PPCM de 24 et 60 car la mesure de la longueur du côté du carré en cm doit être un multiple à la fois de 24 et 60.

Si on cherche un nombre de taille minimale ayant telle ou telle propriété, on pense plutôt au PPCM.

6°) Obtention du PPCM de deux entiers

Rechercher le PPCM en établissant le début de la liste des multiples de deux entiers peut être fastidieux lorsque ces deux nombres sont grands.

Pour calculer le PPCM de deux entiers, on peut commencer par calculer le PGCD (par exemple avec l'algorithme d'Euclide) puis utiliser la relation liant le PGCD et le PPCM de deux entiers qui sera vue plus loin.

Sinon, on peut utiliser la calculatrice ou un logiciel de calcul formel.
Certaines calculatrices ont déjà une fonction intégrée permettant de calculer le PPCM de deux entiers que l'on rentre ; on peut éventuellement modifier le programme correspondant à l'algorithme d'Euclide afin qu'il affiche le PPCM des deux entiers.

Par exemple, pour la calculatrice TI-82 Stats.fr, il faut aller dans math puis sélectionner NUM et enfin descendre jusqu'à 8 (ou 9 selon le modèle) : ppcm(.
Certains sites Internet permettent aussi d'obtenir le PPCM de deux entiers.
On verra dans le prochain chapitre une méthode utilisant la décomposition en facteurs premiers.

7°) Utilisation de la calculatrice

• Toutes les calculatrices de lycée actuelles ont une commande intégrée permettant de calculer le PPCM de deux entiers naturels que l'on rentre.
En anglais, le PPCM est appelé *lower common divisor* et est *noté lcm*. Cette notation est utilisée par les calculatrices en anglais.

• **Calculatrice TI-83 Plus**

Choisir : math puis sélectionner NUM et enfin descendre jusqu'à 8 : ppcm(ou lcm(.

Syntaxe : ppcm(nombre 1, nombre 2) [calculatrice en français]

lcm(nombre 1, nombre 2) [calculatrice en anglais]

Les deux nombres doivent être positifs ou nuls (et non tous les deux nuls).
Le deux nombres sont séparés par une virgule.

7°) Théorème [multiples communs à deux entiers]

• **Énoncé**

L'ensemble des multiples communs à deux entiers a et b non nuls est l'ensemble des multiples de leur PPCM.

• **Démonstration (cette démonstration est à comprendre mais n'est pas à savoir refaire)**

On suppose que a et b sont non nuls (sinon l'égalité est évidente).
On suppose aussi que a et b sont positifs.

On note $d=\text{PGCD}(a\,;b)$.

On peut alors poser $a=da'$ et $b=db'$ où a' et b' sont des entiers naturels premiers entre eux.

Soit μ un multiple commun à a et b.

On a alors : $\mu=k\times a$ et $\mu=k'\times b$ avec k et k' entiers relatifs non nuls.
Par suite, $ka=k'b$ d'où $kda'=k'db'$ et finalement $ka'=k'b'$ (car $d>0$).
Il en résulte que $a' \mid k'b'$ avec a' et b' premiers entre eux.
D'après le théorème de Gauss, on en déduit que $a' \mid k'$ c'est-à-dire $k'=pa'$ avec p entier relatif non nul.

On a $\mu=k'\times b$ d'où $\mu=pa'b$ et $\mu=pa'db'=p(a'b'd)$.

μ est donc un multiple de $a'b'd$.

Tous les multiples communs à a et b sont des multiples de $a'b'd$.

Or $a'b'd=a'b=ab'$.
$a'b'd$ est donc un multiple commun à a et b.
Par suite, $a'b'd$ est le plus petit multiple commun à a et b.

On a donc bien démontré que l'ensemble des multiples communs à a et b était égal à l'ensemble des multiples de leur PPCM (à savoir $a'b'd$).

Dans cette partie démonstration, on peut dégager le résultat suivant :

$$\text{PPCM}(a\,;b) = da'b'$$

résultat dont nous allons nous servir pour démontrer le théorème suivant.

Autre démonstration :

Plan :

• Démontrons que si un entier est un multiple du PPCM, alors c'est un multiple de *a* et de *b*.

• Démontrons que si un entier est un multiple de *a* et de *b*, alors c'est un multiple du PPCM.

On note *m* le PPCM de *a* et de *b*.

Comme *m* est un multiple commun à *a* et *b*, tous ses multiples sont aussi dans $M(a) \cap M(b)$ donc $M(m) \subset M(a) \cap M(b)$.

Réciproquement, soit $\mu \in M(a) \cap M(b)$.
Effectuons la division euclidienne de μ par *m*.
Il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que $\mu = qm + r$ avec $r < m$ d'où $r = qm - \mu$.
Alors *r* est un multiple commun à *a* et *b* car μ et *m* le sont.
C'est ici que la minimalité intervient : $r \in M(a) \cap M(b)$, $0 \leqslant r < m$ et *m* est le plus petit élément de $M(a) \cap M(b) \cap \mathbb{N}^*$.
Par suite $r = 0$.
Donc $\mu = qm \in M(m)$ ce qui montre que $M(a) \cap M(b) \subset M(m)$.

8°) Théorème [relation entre PGCD et PPCM]

• Énoncé

a et *b* sont des entiers naturels non nuls.
$\text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) = a \times b$

• Démonstration

On note $d = \text{PGCD}(a\,;b)$.

On peut alors poser $a = da'$ et $b = db'$ où a' et b' sont des entiers naturels premiers entre eux.

$$\begin{aligned} a \times b &= da' \times db' \\ &= d \times a'b'd \\ &= d \times \text{PPCM}(a\,;b) \quad \text{(on a en effet dégagé dans la démonstration du 6°), l'égalité } \text{PPCM}(a\,;b) = da'b') \\ &= \text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) \end{aligned}$$

• Corollaire

a et *b* sont des entiers naturels non nuls.

Si *a* et *b* sont premiers entre eux, alors $\text{PPCM}(a\,;b) = a \times b$.

On peut aussi retenir ce corollaire sous la formulation suivante :

« Si deux entiers naturels non nuls sont premiers entre eux, alors leur PPCM est égal à leur produit ».

9°) Propriété

• Énoncé

a et *b* sont des entiers relatifs non nuls.
k est un entier naturel non nul.
$\text{PPCM}(ka\,;kb) = k\text{PPCM}(a\,;b)$

Cette propriété est le pendant de la propriété similaire sur le PGCD de deux entiers.

• Démonstration

On commence par supposer que *a* et *b* sont strictement positifs.

On sait d'après la relation liant le PGCD et le PPCM de deux entiers que :
$\text{PGCD}(ka\,;kb) \times \text{PPCM}(ka\,;kb) = ka \times kb$.

Or on a vu que : $\text{PGCD}(ka\,;kb) = k\text{PGCD}(a\,;b)$.
Par suite, $k\text{PGCD}(a\,;b) \times \text{PPCM}(ka\,;kb) = ka \times kb$.
Donc $\text{PGCD}(a\,;b) \times \text{PPCM}(ka\,;kb) = ka \times b$.
D'où $\text{PPCM}(ka\,;kb) = k \times \dfrac{ab}{\text{PGCD}(a\,;b)}$.
Or $\text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) = a \times b$.

On en déduit que $\text{PPCM}(ka\,;kb) = k\text{PPCM}(a\,;b)$.

Dans le cas où *a* et *b* sont de signe quelconques, on se ramène au cas précédent en considérant $|a|$ et $|b|$.

• Conséquence (démonstration évidente)

a et *b* sont deux entiers relatifs non nuls.
k est un diviseur positif commun à *a* et *b*.
Alors $\text{PPCM}\left(\dfrac{a}{k}\,;\dfrac{b}{k}\right) = \dfrac{1}{k}\text{PPCM}(a\,;b)$.

Cette propriété est le pendant de la propriété similaire sur le PGCD de deux entiers.

10°) Utilisation du PPCM pour les fractions

Le PPCM permet de mettre au même dénominateur deux fractions ce qui peut être utile pour :

- comparer des fractions de dénominateurs différents ;

- calculer des sommes ou des différences de fractions de dénominateurs différents.
Il faut noter que l'on utilise le PPCM d'une famille finie d'entiers dès lors que l'on calcule une somme algébrique de fractions (exemple : $\frac{7}{12}-\frac{3}{8}+\frac{5}{6}$).

11°) Utilisation du PPCM pour la résolution de problèmes concrets

• Lorsqu'on a deux grandeurs A et B qui sont chacune multiple entier de U par exemple, on dit que ces grandeurs sont **commensurables** (elles peuvent être mesurées ensemble, elles ont une unité de mesure commune), et **incommensurables** sinon.

• Le PPCM permet d'étudier :
- des problèmes d'engrenages (par exemple braquets d'un vélo, rapports de transmission d'une boîte de vitesses, horloge) ;
- de conjonction de phénomènes périodiques (par exemple éclipses ou alignements de planètes).

• Exemples concrets :
On observe deux phénomènes périodiques dont les périodes A et B sont commensurables.
Le calcul de PPCM permet de connaître la durée qui sépare deux conjonctions du phénomène.
La durée séparant deux apparitions simultanées des deux phénomènes est un multiple commun des deux périodes. La durée qui sépare deux apparitions simultanées consécutives est le PPCM de A et B.

Par exemple, si le parlement est élu tous les 5 ans et le président de la République tous les 7 ans, alors tous les $35=\text{PPCM}(5;7)$ ans les deux élections ont lieu la même année.
Dans la nature, certaines espèces ont des cycles de reproduction dont les périodes sont adaptées à ceux de leur prédateur naturel, de façon à ce que les nouvelles générations de chacune des deux espèces n'apparaissent que rarement en même temps.

12°) Algorithme naïf de recherche du PPCM

Les variables a et b saisies en entrée sont des entiers naturels (relatifs) non nuls.

La négation de ($a \mid m$ et $b \mid m$) est ($a \nmid m$ ou $b \nmid m$).

Entrées :
Saisir a et b

Initialisation :
m prend la valeur 1 [ou $\max(a,b)$ si on veut gagner du temps]

Traitement :
Tantque $a \nmid m$ ou $b \nmid m$ **Faire**
  m prend la valeur $m+1$
FinTantque

Sortie :
Afficher m

La valeur de m affichée en sortie est le PPCM de a et de b.

Programme Python :

On définit une fonction ppcm.

```
def ppcm(a,b):
    m=1
    while m%a!=0 or m%b!=0:
          m=m+1
    return m
```

Autre idée intéressante (Julie Fiadino maths experts le mercredi 3-2-2021) :

```
def ppcm(a,b):
    m=a
    while m%b!=0:
          m=m+a
    return m
```

X. Fractions irréductibles

1°) Définition

a et b sont deux entiers relatifs avec $b \neq 0$.
La fraction $\frac{a}{b}$ est dite **irréductible** lorsque a et b sont premiers entre eux.

2°) Exemple et contre-exemple

• $\text{PGCD}(12\,;5)=1$ donc la fraction $\frac{12}{5}$ est irréductible.

• $\text{PGCD}(22\,;4)=2$ donc la fraction $\frac{22}{4}$ n'est pas irréductible.

3°) Lien entre fraction irréductible et PGCD

• Propriété

a et b sont deux entiers relatifs avec $b\neq 0$.
La fraction $\frac{a}{b}$ est égale à une fraction irréductible $\frac{a'}{b'}$.

• Démonstration (évidente)

On introduit $d=\text{PGCD}(a\,;b)$.

• Méthode pour rendre irréductible une fraction

- On calcule le PGCD du numérateur et du dénominateur (par exemple avec l'algorithme d'Euclide).
- On divise le numérateur et le dénominateur par ce PGCD.

4°) Exemple

Écrire sous forme irréductible la fraction $\frac{630}{924}$.

On a : $\text{PGCD}(630\,;924)=42$ donc $\frac{630}{924}=\frac{630:42}{924:42}=\frac{15}{22}$.

La forme irréductible de la fraction $\frac{630}{924}$ est $\frac{15}{22}$.

3°) Application : démonstration de l'irrationalité de $\sqrt{2}$

Nous allons démontrer que $\sqrt{2}$ est un nombre irrationnel.

Nous allons effectuer un raisonnement par l'absurde.

Supposons que $\sqrt{2}$ soit rationnel.

$\sqrt{2}$ peut donc s'écrire sous la forme d'une fraction irréductible $\frac{a}{b}$ où a et b sont deux entiers naturels premiers entre eux.

On a donc $\sqrt{2}=\frac{a}{b}\quad(1)$.

(1) donne alors $2=\frac{a^2}{b^2}$ soit $a^2=2b^2\quad(2)$.

(2) permet de dire que a^2 est pair.
Par conséquent, a est pair.
On peut donc écrire $a=2k$ avec $k\in\mathbb{N}$.
En remplaçant a par $2k$ dans (2), on obtient : $(2k)^2=2b^2$.
D'où $b^2=2k^2$.
Cette dernière égalité permet de dire que b^2 est pair.
Par conséquent, b est pair, ce qui est absurde puisque l'on a supposé que a et b sont premiers entre eux.

XI. PGCD et PPCM de plusieurs entiers

1°) Définition

Comme nous l'avons dit précédemment, les définitions du PGCD et du PPCM s'étendent au cas de plusieurs entiers.
La notion de PPCM est présente naturellement lors de l'addition ou la soustraction de plusieurs fractions.

Dans la suite, nous allons nous intéresser au cas de trois entiers relatifs non nuls.

• Le PGCD de trois entiers relatifs a, b, c non nuls est le plus grand diviseur commun à ces trois entiers. On le note $\text{PGCD}(a\,;b\,;c)$.

• Le PPCM de trois entiers relatifs a, b, c non nuls est le plus petit multiple commun strictement positif à ces trois entiers. On le note $\text{PPCM}(a\,;b\,;c)$.

On définit de même le PGCD et le PPCM d'une famille a_1, a_2, … a_n d'entiers relatifs non nuls.

2°) Propriété d'associativité

• Énoncé :

On reprend les notations précédentes.
On a : $\text{PGCD}(a\,;b\,;c)=\text{PGCD}\big(\text{PGCD}(a\,;b)\,;c\big)$.

On peut dire qu'il s'agit d'une sorte de propriété d'associativité du PGCD.

• Démonstration (à étudier) :

On écrit des égalités d'ensembles (il s'agit d'un raisonnement d'un type particulier, non encore pratiqué au lycée).

$$\boldsymbol{D}(a)\cap\boldsymbol{D}(b)\cap\boldsymbol{D}(c)=\left(\boldsymbol{D}(a)\cap\boldsymbol{D}(b)\right)\cap\boldsymbol{D}(c)$$

$$=\boldsymbol{D}\left(\text{PGCD}(a;b)\right)\cap\boldsymbol{D}(c)$$

$$=\boldsymbol{D}\left(\text{PGCD}\left(\text{PGCD}(a;b);c\right)\right)$$

On a : $\boldsymbol{D}(a)\cap\boldsymbol{D}(b)\cap\boldsymbol{D}(c)=\boldsymbol{D}\left(\text{PGCD}\left(\text{PGCD}(a;b);c\right)\right)$.

Par conséquent, on a : $\max\left(\boldsymbol{D}(a)\cap\boldsymbol{D}(b)\cap\boldsymbol{D}(c)\right)=\max\boldsymbol{D}\left(\text{PGCD}\left(\text{PGCD}(a;b);c\right)\right)$.

D'où $\text{PGCD}(a;b;c)=\text{PGCD}\left(\text{PGCD}(a;b);c\right)$.

Le type de raisonnement pour démontrer l'égalité d'ensembles est différent de celui qui a été rencontré dans la démonstration du lemme d'Euclide.

● Utilisation :

Il n'existe pas d'algorithme qui permette de déterminer le PGCD de trois entiers.
Dans le cas de plusieurs nombres, on cherche le PGCD des deux premiers puis le PGCD du nombre ainsi obtenu et du troisième etc.

Déterminer $\text{PGCD}(1755;1053;2210)$.

On procède par groupement (propriété d'associativité du PGCD) afin de se ramener au PGCD de deux entiers.

On a : $\text{PGCD}(1755;1053)=351$. Or $\text{PGCD}(351;2210)=13$. Donc $\text{PGCD}(1755;1053;2210)=13$.

La calculatrice ne permet pas de déterminer directement le PGCD de plusieurs entiers ; la propriété est alors intéressante pour se ramener au PGCD de plusieurs entiers.

● Une autre propriété :

a, b, c, d sont des entiers relatifs non nuls.

On a : $\text{PGCD}(a,b,c,d)=\text{PGCD}\left(\text{PGCD}(a,b),\text{PGCD}(c,d)\right)$.

● Programme Python permettant de trouver le PGCD de plusieurs nombres en utilisant la récursivité :

```
def mpgcd(nb):
    if len(nb)==2:
        return pgcd(nb[0], nb[1])
    else:
        return pgcd(nb.pop(0), mpgcd(nb))
```

La fonction pop() est quelque peu similaire à la fonction remove() et permet de retirer un élément d'une liste à une position donnée et de renvoyer cette élément. Ici on retire donc l'élément à la position 0 de la liste et on calcule le pgcd avec cet élément et le reste des éléments de la liste.

Enfin, une fonction pgcd a bien été préalablement créée.

● Cas du PPCM :

On a des propriétés analogues pour le PPCM de plusieurs entiers.

3°) Propriété de factorisation

On peut généraliser à plusieurs entiers les propriétés qui ont été étudiées pour deux entiers.

Soit $a_1, a_2, \ldots a_n$ des entiers relatifs non nuls.
Soit k un entier naturel non nul.

$\text{PGCD}(ka_1, ka_2, ..., ka_n)=k\text{PGCD}(a_1, a_2, ..., a_n)$
$\text{PPCM}(ka_1, ka_2, ..., ka_n)=k\text{PPCM}(a_1, a_2, ..., a_n)$

4°) Nombres premiers entre eux dans leur ensemble

● Définition :

La définition d'entiers premiers entre eux s'étend au cas de plusieurs nombres.

On dit que des entiers relatifs sont *premiers entre eux dans leur ensemble* pour exprimer que leurs seuls diviseurs communs sont 1 et – 1.

Pour une famille finie d'entiers relatifs non tous nuls cela équivaut à dire que leur PGCD est égal à 1.

Exemple :

Les entiers 6, 15, 20 sont premiers dans leur ensemble (mais pas premiers entre eux deux à deux).

● Propriété :

Si une famille d'entiers relatifs comporte deux entiers relatifs premiers entre eux, alors cette famille est constituée d'entiers premiers entre eux dans leur ensemble.

La réciproque est fausse.

La démonstration de cette propriété est très facile.

● Propriété :

Soit $a_1, a_2, \ldots a_n$ des entiers relatifs non nuls.
On note d leur PGCD.
On note $a_1', a_2', \ldots a_n'$ les entiers relatifs tels que $a_1=da_1'$, $a_2=da_2'$, … $a_n=da_n'$.
Les entiers $a_1', a_2', \ldots a_n'$ sont premiers entre eux dans leur ensemble.

XIII. Inverse modulaire

Dans ce paragraphe, nous revenons à la notion d'inverse modulo n déjà étudiée dans le chapitre des congruences.

1°) Définition [inverse modulo n]

Soit n un entier naturel supérieur ou égal à 2 et a un entier relatif.
On appelle inverse de a modulo n tout entier b, sous réserve d'existence, tel que $ab \equiv 1 \pmod{n}$.

La notion d'inverse est ici relative à la multiplication (inverse pour la multiplication).

2°) Vocabulaire

Il est important de retenir le vocabulaire suivant

Lorsque l'on a l'égalité de la forme $ab \equiv 1 \pmod{n}$ où a et b sont deux entiers, on peut dire que :
b est un inverse de a modulo n ;
a est un inverse de b modulo n ;
a et b sont inverses l'un de l'autre modulo n.

3°) Exemples

① n est un entier naturel quelconque supérieur ou égal à 2.
1 admet un inverse modulo n : lui-même.
De même, – 1 admet un inverse modulo n : lui-même.

② n est un entier naturel quelconque supérieur ou égal à 2.
0 n'admet pas d'inverse modulo n.

③ On prend $n = 9$ et $a = 4$.

7 est un inverse de 4 modulo 9 car $4 \times 7 \equiv 1 \pmod{5}$.

4°) Questions

Comment savoir si un entier admet un inverse modulo n ?
Quel est le lien entre deux inverses modulo n éventuels d'un même nombre ?
Existe-t-il une méthode générale permettant de trouver l'inverse d'un nombre modulo n ?

5°) Propriété [relation entre deux inverses]

On reprend les notations de la définition.

Supposons que a admettent deux inverses b et c modulo n.
Alors $b \equiv c \pmod{n}$.

La démonstration a déjà été faite dans le chapitre sur les congruences.

6°) Propriété [existence d'un inverse]

On reprend les notations de la définition.

a possède un inverse modulo n si et seulement si a et n sont premiers entre eux.

Démonstration :

Sens direct

a possède un inverse modulo n.

Soit b un tel inverse.

On a $ab \equiv 1 \pmod{n}$.
Il existe donc un entier k tel que $ab = 1 + kn \quad (1)$.
(1) donne donc $ab - kn = 1 \quad (1')$.
$(1')$ montre que 1 peut s'écrire comme une combinaison linéaire de a et de n à coefficients entiers relatifs.
On en déduit que a et n sont premiers entre eux.

Sens réciproque

On suppose que a et n sont premiers entre eux.
D'après le théorème de Bézout, il existe deux entiers u et v tels que $au + bv = 1 \quad (2)$.

(2) implique $au \equiv 1 \pmod{n}$.
Donc u est un inverse de a modulo n.

On pourrait faire une démonstration directe par équivalences.
La démonstration proposée ici permet cependant de mieux comprendre.

La démonstration fournit une méthode pour trouver un inverse à partir de l'identité de Bezout.

7°) Recherche d'un inverse par identité de Bezout

Le sens réciproque nous permet de trouver un inverse grâce à une relation de Bézout.

● Exemple :

Démontrer que 9 admet un inverse modulo 25 et déterminer un tel inverse.

On veut démontrer que 9 et 25 sont premiers entre eux.
On utilise une relation de Bézout.

On a $25\times 4-9\times 11=1$ (relation facile à trouver par simple calcul mental) donc $-9\times 11\equiv 1 \pmod{25}$.

Donc – 11 est un inverse de 9 modulo 25.

On a $-11\equiv 14 \pmod{25}$ donc 14 est aussi un inverse de 9 modulo 25.

● Dans le cas général, pour trouver une égalité de Bezout, on peut utiliser l'algorithme d'Euclide puis le « remonter » ou utilise les quotients dans un tableau.

Le Plus Grand Diviseur Commun était généralement nommé dans les livres en latin *maximus communis divisor*.
Cataneo utilisa en 1546 *il maggior commune ripiego* en italien.
Greatest common measure est trouvé en anglais en 1570 à Billingsley, *Elem. Geom. : « Il est demandé à ces trois magnitudes de trouver la plus grande mesure commune » (OED2).*
Cataldi en 1606 écrivit *massima comune misura* en italien.
Highest common divisor est trouvé en 1830 dans le Traité sur l'Algèbre de George Peacock.
Highest common factor est trouvé en 1843 dans La Penny Cyclopedia de la Société pour la diffusion du savoir utile.
Greatest common divisor est trouvé en anglais en 1811 dans Une enquête élémentaire sur la Théorie des Nombres [James A. Landau].
Olaus Henrici (1840-1918), déclara dans un discours présidentiel à la Société Mathématiques de Londres en 1883 : « Il y a des processus, comme la découverte du P.G.C.D, que la plupart des garçons n'auront jamais l'opportunité d'utiliser, excepté peut-être dans les salles d'examens. »

Le Plus Petit Commun Multiple. *Common denominator* apparaît en anglais en 1594 dans les *Exercices* de Blundevil : « Multiplie les dénominateurs l'un dans l'autre, et le produit résultant devrait être un dénominateur commun aux deux fractions » (OED2).
Common divisor a été utilisé en 1674 par Samuel Jeake dans Arithmétique, publié en 1696 : « Commensurable, called also Symmetral, is when the given Numbers have a Common Divisor ». (OED2)
Least common multiple est trouvé en 1823 dans l'œuvre de J.Mitchell, Dict.Math et Phys. Sci. : « To find the least common Multiple of several numbers » « Pour trouver le dernier multiple commun de plusieurs nombres ».
Least Common Denominator est trouvé en 1844 dans l'Introduction à l'arithmétique nationale, sur le système inductif de Benjamin Greenleaf : « RULE. – Reduce the fractions, if necessary, to the least common denominator. Then find the greatest common divisor of the numerators, which, written over the least common denominator, will give the greatest common divisor required » "REGLE.- Réduisez les fractions, si nécessaire, jusqu'au dernier dénominateur commun. Trouvez par la suite le plus grand diviseur commun, qui, écrit sur le dernier diviseur commun, donnera le plus grand diviseur commun demandé. » [Bibliothèque Digitale de l'Université du Michigan]
Lowest Common Denominator apparaît en 1854 dans Arithmétique, oral et écrit, appliqué pratiquement par des questions suggestives de Thomas H. Palmer : « Suggestive questions. – Are all the underlined factors to be found in the denominators of the fractions marked a and b ? Should they be omitted, then, in finding the lowest common denominator? What is the product of the factors that are not underlined? Has this product every factor contained in all the given denominators? Will it form their common denominator, then? Does it contain no more factors than they do? Will it form, then, their lowest common denominator?" « Questions suggestives. – Est-ce que tous les facteurs soulignés peuvent être trouvés dans les dénominateurs des fractions *a* et *b* ? Devraient-ils être omis, alors, en trouvant le plus petit diviseur commun ? Quel est le produit des facteurs qui ne sont pas soulignés ? Est-ce que ce produit a tous les facteurs contenus dans les dénominateurs donnés ? Formera-t-il alors le dénominateur commun ? Ne contient-il pas plus de facteurs qu'eux ? Formera-t-il alors le plus petit diviseur commun ? » [Bibliothèque Digitale de l'Université du Michigan]
Least Common Dividend apparaît en 1857 dans Le Dictionnaire Mathématique et l'Encyclopédie des Sciences Mathématiques.
Lowest Common Multiple apparaît en 1873 dans Test examples in algebra, especially adapted for use in connection with Olney's School, or University algebra d'Edward Olney. [Bibliothèque Digitale de l'Université du Michigan]

GREATEST COMMON DIVISOR in Latin books was usually written as *maximus communis divisor*.

Cataneo in 1546 used *il maggior commune ripiego* in Italian.

Greatest common measure is found in English in 1570 in Billingsley, *Elem. Geom.*: "It is required of these three magnitudes to finde out the greatest common measure" (OED2).

Cataldi in 1606 wrote *massima comune misura* in Italian.

Highest common divisor is found in 1830 in *A Treatise on Algebra* by George Peacock. [Google print search]

Highest common factor is found in 1843 in *The Penny Cyclopædia of the Society for the Diffusion of Useful Knowledge.* [Google print search]

Greatest common divisor is found in English in 1811 in *An Elementary Investigation in the Theory of Numbers* [James A. Landau].

Olaus Henrici (1840-1918), in a Presidential address to the London Mathematical Society in 1883, said, "Then there are processes, like the finding of the G. C. M., which most boys never have any opportunity of using, except perhaps in the examination room."

LEAST COMMON MULTIPLE. *Common denominator* appears in English in 1594 in *Exercises* by Blundevil : "Multiply the Denominators the one into the other, and the Product thereof shall bee a common Denominator to both fractions" (OED2).

Common divisor was used in 1674 by Samuel Jeake in *Arithmetick*, published in 1696 : "Commensurable, called also Symmetral, is when the given Numbers have a Common Divisor" (OED2).

Least common multiple is found in 1823 in J. Mitchell, *Dict. Math. & Phys. Sci.*: "To find the least common Multiple of several Numbers" (OED2).

Least common denominator is found in 1844 in *Introduction to The national arithmetic, on the inductive system* by Benjamin Greenleaf: "RULE. - Reduce the fractions, if necessary, to the least common denominator. Then find the greatest common divisor of the numerators, which, written over the least common denominator, will give the greatest common divisor required" [University of Michigan Digital Library].

Lowest common denominator appears in 1854 in *Arithmetic, oral and written, practically applied by means of suggestive questions* by Thomas H. Palmer: "*Suggestive Questions*. - Are all the underlined factors to be found in the denominators of the fractions marked *a* and *b* ? Should they be omitted, then, in finding the *lowest* common denominator? What is the product of the factors that are not underlined? (80·3·5.) Has this product every factor contained in all the given denominators? Will it form their *common* denominator, then? Does it contain no more factors than they do ? Will it form, then, their *lowest* common denominator?" [University of Michigan Digital Library].

Least common dividend appears in 1857 in *Mathematical Dictionary and Cyclopedia of Mathematical Science*.

Lowest common multiple appears in 1873 in *Test examples in algebra, especially adapted for use in connection with Olney's School, or University algebra* by Edward Olney [University of Michigan Digital Library].

Notations standards sans doute définies en anglais par Hardy & Wright.
Le site de définitions est le : http://jeff560.tripod.com/g.html

Fin du cours sur le PGCD et le PPCM

On peut généraliser les notions du PGCD et du PPCM au cas de plusieurs nombres.
Si on prend 3 nombres, on appelle PGCD de ces 3 nombres le diviseur commun de ces 3 nombres. De même pour le PPCM.

Propriété
$\mathrm{PGCD}(a;b;c) = \mathrm{PGCD}(\mathrm{PGCD}(a;b);c)$

Soit n un entier naturel supérieur ou égal à 2 fixé.

Définition :

On appelle *inverse modulaire* d'un entier relatif a pour la multiplication modulo n un entier relatif b tel que $ab \equiv 1 \pmod{n}$.

Il n'y a pas de notation particulière.

Exemple :

On prend $n = 5$.
3 est un inverse de 2 modulo 5 car $3 \times 2 \equiv 1 \pmod{5}$.

Questions :
Un entier relatif b admet-il toujours un inverse modulo n ?
Comment le trouver ?
Comment s'en servir ?

La définition est donc équivalente à :

Propriété :

Supposons que a admettent deux inverses b et c modulo n.
Alors $b \equiv c \pmod{n}$.

En effet,

$b \equiv 1 \times b \pmod{n}$

$b \equiv ac \times b \pmod{n}$

$b \equiv c \times (ab) \pmod{n}$

$b \equiv c \times 1 \pmod{n}$

$b \equiv c \pmod{n}$

Propriété :

a possède un inverse modulo *n* si et seulement si *a* et *n* sont premiers entre eux.

a possède un inverse modulo *n* si et seulement si il existe deux entiers *b* et *k* tels que $ab = 1 + kn$

si et seulement si il existe deux entiers *b* et *k* tels que $ab - kn = 1$

si et seulement si *a* et *n* sont premiers entre eux

La démonstration fournit une méthode pour trouver un inverse à partir de l'identité de Bezout.

Équivalence fondamentale :

Soit *a* un entier relatif.
On suppose que *a* et *n* sont premiers entre eux.
On note *b* un inverse de *a* modulo *n*.

$ax \equiv y \pmod{n} \Leftrightarrow x \equiv by \pmod{n}$