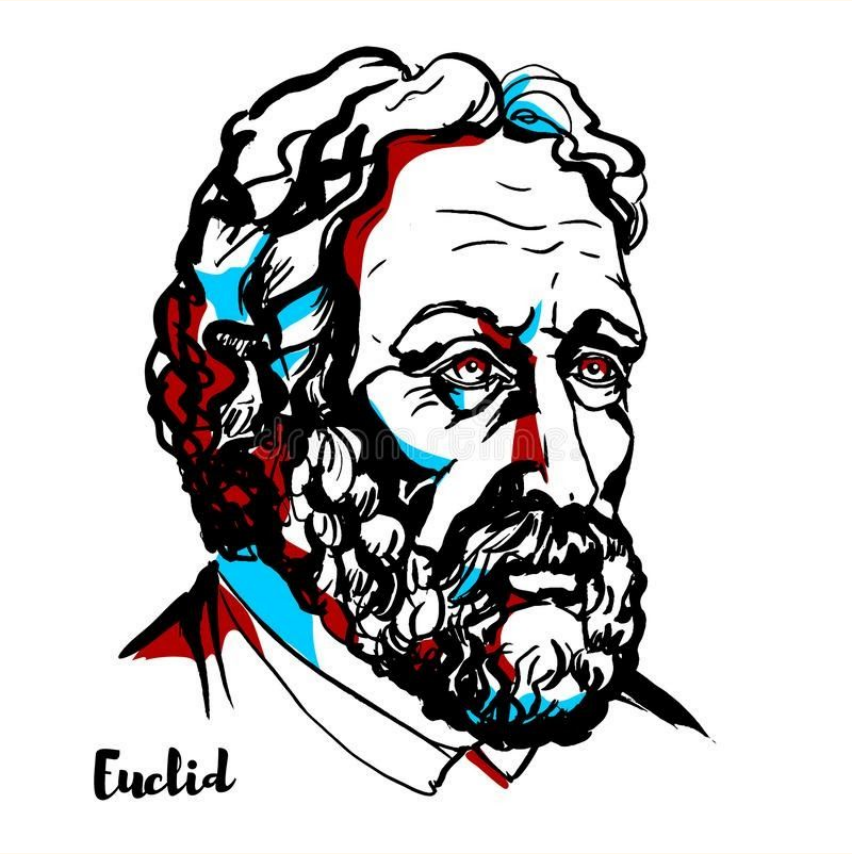
dPromotion Mirzakhani 2020-2021
LYCÉE EDGAR MORIN

PGCD et applications



OBJECTIFS

1. Déterminer le PGCD de deux nombres entiers
2. Connaître et utiliser les théorèmes de Gauss et de Bézout
3. Résoudre une congruence $ax \equiv b[n]$
4. Déterminer l'inverse de a $[n]$ quand a et n sont premiers entre eux

PLAN DU COURS

I. PGCD
II. Nombres premiers entre eux
III. Théorème de Gauss et applications
IV. Utilisation de la calculatrice et algorithmes en Python

INTRODUCTION

Dans ce cours, nous verrons comment est défini, calculé et utilisé le $PGCD$ de deux entiers naturels, une divisibilité au cœur de systèmes mathématiques allant du chiffrement à l'élaboration de calendriers.

I. PGCD

Le $PGCD$ est une notion déjà vue en primaire, et est très intuitive. Dans cette partie, nous verrons une manière plus mathématique de le déterminer, ainsi que les conséquences que porte cette méthode.

1. Définitions et propriétés

Définition :

Soient a et b deux entiers relatifs non simultanément nuls.

L'ensemble des diviseurs communs à a et b est une partie non vide de $\mathbb{Z}$ (cette partie contient 1) et majoré (par le maximum entre $|a|$ et $|b|$). Cet ensemble admet un plus grand élément appelé **Plus Grand Diviseur Commun de a et b noté $PGCD(a\ ;\ b)$.**

Propriétés :

Soient a et b deux entiers relatifs non simultanément nuls.

On a $PGCD(a\ ;\ b) = PGCD(|a|\ ;|b|)$ et, pour tout couple $(a\ ;\ b) \in \mathbb{N}^2$ avec $a \neq 0$:

- $PGCD(a\ ;\ b) \geq 1$; $PGCD(0\ ;\ a) = a$; $PGCD(1\ ;\ a) = 1$
- a divise b si, et seulement si, $PGCD(a\ ;\ b) = a$
- $PGCD(a\ ;\ b) = PGCD(a - b\ ;\ b)$ $\rightarrow$ Méthode de la soustraction

Exemple :

$PGCD(229\ ;\ 225) = PGCD(229 - 225\ ;\ 225) = PGCD(4\ ;\ 225) = 1$ car 1 est le seul diviseur positif commun à 4 et 225.

Remarques :

- On a $PGCD(a\ ;\ 0) = |a|$ et, par convention, $PGCD(0\ ;\ 0) = 0$.
- Un nombre entier et son opposé ont les mêmes diviseurs. On se restreint donc au cas des entiers naturels.

2. Algorithme d'Euclide et conséquences

Propriété :

Ici, a et b sont deux entiers naturels non nuls avec $a > b$.

On note q et r le quotient et le reste de la division euclidienne de a par b.

Avec ces notations, $PGCD(a\ ;\ b) = PGCD(b\ ;\ r)$.

Démonstration :

Soit d, un diviseur commun à a et b. Par définition, $a = bq + r$ donc $r = a - bq$.

- r est une combinaison linéaire de a et de b et d divise à la fois a et b, donc $d \mid r$.

  d est un diviseur commun à b et r.

- Mais aussi, a est une combinaison linéaire de b et r, donc tout diviseur commun à b et r divise a.

Ainsi, l'ensemble des diviseurs communs à a et b est confondu avec l'ensemble des diviseurs communs à b et r. Ils ont donc le même plus grand élément d'où :

$$PGCD(a\ ;\ b) = PGCD(b\ ;\ r).$$

Remarque :

Par logique pour montrer l'égalité de deux $PGCD$, on montre que les ensembles dont ils sont les plus grands éléments sont les mêmes. La propriété d'unicité du plus grand élément permet de conclure.

L'algorithme d'Euclide :

On définit par récurrence la suite des entiers $r_0, r_1, ..., r_n$ tels que :

- r_0 est le reste de la division euclidienne de a par b
- si $r_0 \neq 0$, r_1 est le reste de la division de b par r_0
- pour tout $k \in \{1, ..., n-1$, si $r_k \neq 0$ alors r_{k+1} est le reste de la division euclidienne par r_{k-1} et r_k

Alors, cette suite d'entiers est nulle à partir d'un certain rang et la dernière valeur non nulle prise par cette suite est le $PGCD$ de a et b.

Histoire des mathématiques - Euclide Euclide est un savant grec qui enseignait les mathématiques à Alexandrie, en Égypte, où il avait fondé la plus célèbre école de l'Antiquité, l' "école d'Alexandrie". Le roi Ptolémée I[er] lui propose une récompense. Euclide la refuse car il pense qu'un savant doit enseigner sans viser un cadeau.	

L'une des conséquences de l'algorithme d'Euclide porte sur l'homogénéité du PGCD :

Définition :

Soit a et b deux entiers relatifs non nuls

Pour tout entier naturel k non nul, $PGCD(ka; kb) = kPGCD(a; b)$

Exemple :

$PGCD(60\ ;90) = PGCD(30 \times 2; 30 \times 3) = 30 \times PGCD(2\ ;3) = 30$ car $PGCD(2\ ;3) = 1$

II. Nombres premiers entre eux

Les nombres premiers sont des nombres aux caractéristiques mathématiques particulières, et sont notamment utilisés dans le chiffrement RSA, utilisés universellement dans les communications via Internet. Dans cette partie, nous verrons la notion de “nombres premiers entre eux” et comment les déterminer, ainsi que leurs conséquences pour la résolution d'équations diophantiennes.

Surnommé le “père de l’algèbre”, Diophante d’Alexandrie, mathématicien de langue grecque, a vécu à alexandrie et est connu pour son étude des équations à variables sur les nombres rationnels positifs, qui a donné son nom aux équations diophantiennes.	

1. Définitions et propriétés

Définitions :

Soient a et b deux entiers relatifs non nuls.

On dit que a **et** b **sont premiers entre eux** lorsque leurs seuls diviseurs communs sont 1 et −1. Autrement dit, a et b sont premiers entre eux lorsque $PGCD(a\,;\,b) = 1$.

Exemple:

4 et 9 sont-ils premiers entre eux ?

$div(4) = \{1; 2; 4\}$

$div(9) = \{1; 3; 9\}$

Les nombres 4 et 9 partagent le nombre 1 comme unique diviseur commun et donc sont premiers entre eux.

On écrit alors $PGCD(4\,;9) = 1$

Définition :

Soient a un entier relatif et b un entier naturel non nul.

La fraction $\frac{a}{b}$ est irréductible si les entiers a et b sont premiers entre eux.

Exemple :

La fraction $\frac{7}{11}$ est irréductible car 7 et 11 sont premiers entre eux.

Propriétés:

Soient a et b deux entiers relatifs non nuls. Soient $d = PGCD(a\ ;\ b)$ et a', b' les entiers tels que $a = da'$ et $b = db'$. Alors a' et b' sont premiers entre eux. Réciproquement, s'il existe $d \in \mathbb{N}$ et a', b' des entiers premiers entre eux tels que $a = da'$ et $b = db'$, alors d est le $PGCD$ de a et b et le $PGCD(a'; b') = 1$.

Démonstration :

Soient $d' = PGCD(a'\ ;\ b')$ et k_1 et k_2 les entiers tels que $a' = d'k_1$ et $b' = d'k_2$. On doit montrer que $d = 1$. En effet, $a = dd'k_1$ et $b = dd'k_2$, donc dd' est un diviseur commun à a et b. Comme $d = PGCD(a\ ;\ b)$, on a nécessairement $dd' \leq d$ donc, puisque $d > 0,\ d' = 1$. Réciproquement, $PGCD(a\ ;\ b) = PGCD(da'\ ;\ db') = d\,PGCD = (a'\ ;\ b') = d$ car a' et b' sont premiers entre eux.

Exemple :

36 = 12 × 3 et 60 = 12 × 5.

Puisque 3 et 5 sont premiers entre eux, alors $PGCD(60\ ;\ 36) = 12$

2. Théorème de Bézout

Le théorème de Bézout nous sert à déterminer que 2 nombres sont premiers entre eux en usant de leur PGCD.

Définition :

Soit a et b deux entiers relatifs non nuls.

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

Exemple :

D'après le théorème de Bézout, 30 et 17 sont premiers entre eux car on peut écrire $4 \times 30 + (-7) \times 17 = 120 - 119 = 1$

Remarque :

Le théorème de Bézout, bien que très intéressant, ne nous permet pas définir des valeurs de u et de v. Pour obtenir ces coefficients, on peut notamment se servir de l'algorithme d'Euclide.

3. Application aux équations diophantiennes

Propriété :

Soient a, b et c trois entiers relatifs non nuls

L'équation $ax + by = c$, où les inconnues x et y sont des entiers relatifs non nuls, admet des solutions si et seulement si c est un multiple du $PGCD$ de a et de b

Exemple :

Comme $PGCD(2\ ;\ 3) = 1$ alors l'équation $2x + 3y = 1$ admet au moins un couple d'entiers solutions.

Remarques :

- Une telle équation dont les inconnues sont des nombres entiers s'appelle une équation Diophantienne
- Si $c = PGCD(a\ ;\ b)$, le théorème de Bézout généralisé donne l'existence d'un couple $(x\ ;\ y) \in \mathbb{Z}^2$ solution de l'équation $ax + by = c$

III. Théorème de Gauss et applications

1. Théorème de Gauss

Théorème :

L'énoncé du théorème de Gauss est le suivant :

Soient $a,\ b$ et c trois entiers relatifs non nuls.
Si $a|bc$, et que a et b sont premiers entre eux, alors $a|c$.

Remarque :

Le fait que a et b soient premiers entre eux est essentiel. En effet, par exemple, 4 divisera le produit de 2 et 6, soit 12, néanmoins, 4 ne divisera ni 2, ni 6.

Démonstration :

Supposons que a divise bc et que a et b sont premiers entre eux.
Alors $PGCD(a\ ;\ b) = 1$ donc d'après le théorème de Bézout, il existe $(u\ ;\ v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. On a donc $auc + bvc = c$. Or $a|bc$ par hypothèse et $a|auc$ donc $a|(auc + bvc)$.

Ainsi, $a|c$.

Exemple :

Soit 7 diviseur de 583 = 11 × 53. Comme 7 est premier avec 11, le théorème de Gauss permet de démontrer que 7 divise 53

3. Corollaire du théorème de Gauss

Le théorème de Gauss amène ce corollaire :

Corollaire :

Soient a, b, et c trois entiers relatifs non nuls.
Si b et c sont premiers entre eux et divisent tous deux a, alors $bc|a$.

Remarque :

De même, il est tout aussi primordial que b et c soient premiers entre eux.

Démonstration :

Soient b et c deux diviseurs de a premiers entre eux et b' et c' les entie $bb' = a$ et $cc' = a$. Alors $bb' = cc'$, donc $b|cc'$. Comme b et c sont premiers entre eux, alors, d'après le théorème de Gauss, b divise c'. Soit alors m l'entier tel que $c' = bm$.
On a donc $a = cc' = cbm$.

D'où bc divise a.

Exemple :

Soit $n \in \mathbb{N}$

$$n(n^2 - 1) = n(n-1)(n+1) = (n-1)n(n+1)$$

est le produit de 3 entiers consécutifs, donc $n(n^2 - 1)$ est divisible par 2 et par 3.

Comme 2 et 3 sont premiers entre eux, alors le corollaire de Gauss énoncé ci-dessus affirme que $n(n^2 - 1)$ est divisible par 6.

IV. Utilisation de la calculatrice et algorithmes en Python

Cette partie présentera la méthode de calcul du PGCD sur la calculatrice Numworks.
Si, toutefois, vous ne l'avez pas, vous pouvez utiliser ce simulateur.

Calcul du PGCD de deux entiers a la calculatrice *Numworks* :

Dans l'application **`Calculs`** :

- Appuyer sur la touche : 

- Dans la liste, sélectionner **`Arithmétique`**, et appuyer sur la touche 

:
- Chercher la commande **`gcd(p,q)`**, et appuyer sur la touche 

:

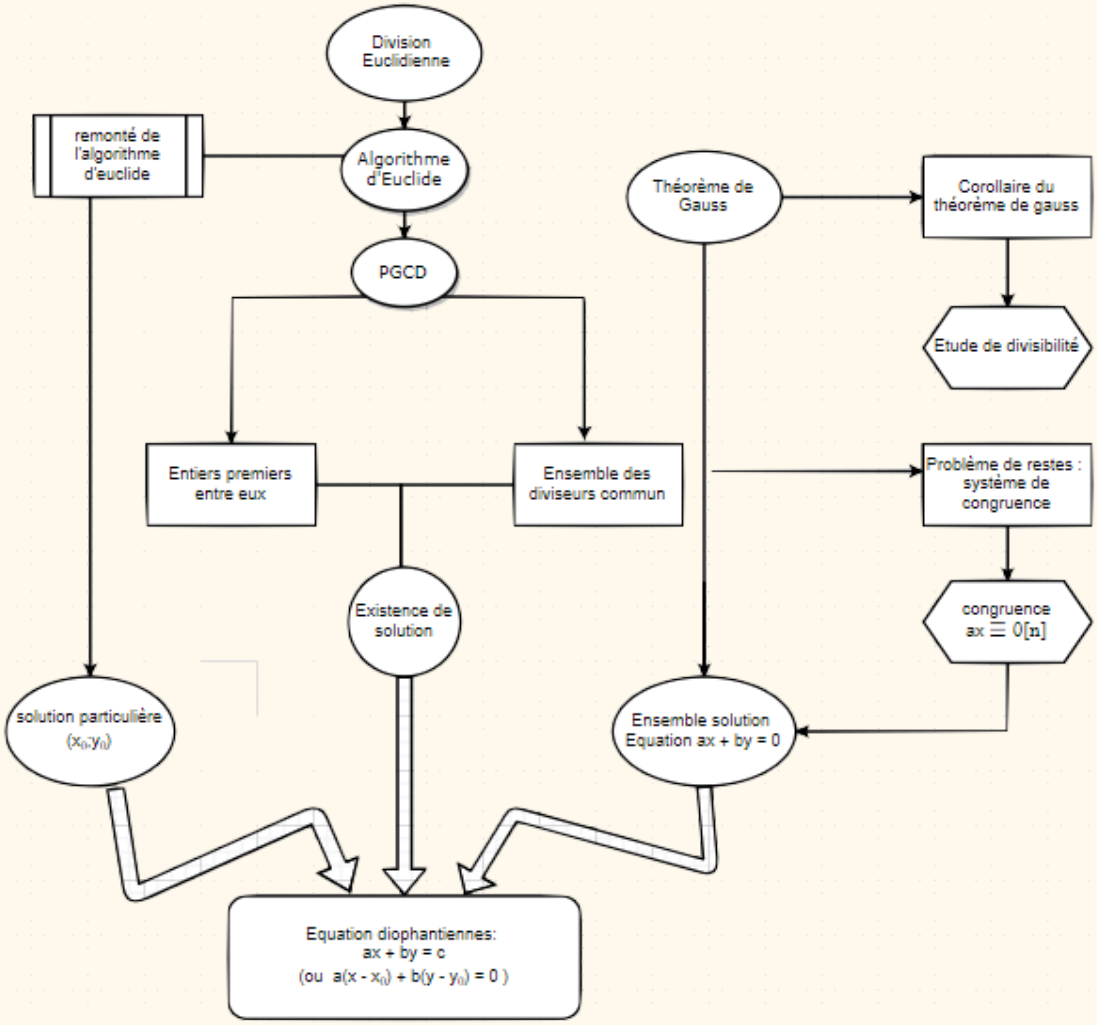
Selon le même processus, on peut également obtenir le PPCM de deux entiers à l'aide de la commande **`lcm(p,q)`**.

Calcul du PGCD de deux entiers avec un algorithme Python :

Un algorithme possible utilisant Python pour déterminer le PGCD de deux entiers est le suivant :

```
1   def pgcd(a,b):
2       if b==0:
3           return a
4       else:
5           r=a%b
6           return pgcd(b,r)
```

CARTE MENTALE



SOURCES

- *Mathématiques Expertes Terminale*, lelivrescolaire.fr, 2020
- *Mathématiques Expertes Terminale*, Eric Barbazo, Collection Barbazo, Hachette Education, 2020
- Chaîne YouTube *m@ths-et-tiques* (Yvan Monka)

LIENS VIDÉOS

- j’aicomprismath - PGCD : comprendre la définition • cours • arithmétique • Terminale S spé maths
- Yvan Monka-Déterminer le PGCD de deux nombres (Recherche diviseurs) - Terminale - Maths expertes
- Yvan Monka-Déterminer le PGCD de deux nombres (Algorithme d'Euclide) - Terminale - Maths expertes
- j’aicomprismath - algorithme d'Euclide • comprendre et savoir l'appliquer pour calculer un PGCD • arithmétique

Rédaction du chapitre et des évaluations

La rédaction doit se faire sur les pages précédentes du Google docs.

Rappel : **ne pas changer les couleurs, les polices et les tailles de police**.
Vous devez rendre le document le plus harmonieux possible.

Avant et pendant la rédaction :

- Consulter le programme et également les ressources proposées par le professeur sur lequel la rédaction doit s'appuyer.
- Attention aux fautes d'orthographe!
- Il faut **respecter le planning** de rendu des travaux, sans quoi, le programme de l'année ne risque pas d'être vu dans sa totalité.
- Penser à mettre des utilisations à la calculatrice (*NumWorks* de préférence) et des algorithmes en Python
- Penser à des exemples détaillés, des exercices, des méthodes, des séries d'exercices pour s'entraîner, et des liens sur des vidéos Youtube réexpliquant les notions abordées.
- Il est important de citer vos sources (livres, sites internet, chaînes YouTube, etc.)

Pendant et après la rédaction :

- Il est primordial d'effectuer une relecture globale et collective des contenus.
- Penser à mettre tous les liens vidéos en hypertexte.
- Me prévenir dès la fin de la rédaction :)

Dates importantes :

- Ce cours doit être terminé avant le **15/01/2021**.
- La carte mentale doit être terminée avant le **15/01/2021**.
- La devoir maison (et son corrigé) doit être terminé avant le **18/01/2021**.
- La devoir sur table (et son corrigé) doit être terminé avant le **18/01/2021**.
- L'interrogation (et son corrigé) doit être terminée avant le **15/01/2021**.

Contacts

Pour toute question sur les contenus, sur les gabarits ou les *consignes éditoriales*, envoyer un mail à :

onenagros@coquillagesetpoincare.fr

Bonne rédaction !