

Chapitre 15

Divisibilité et congruence sur $\mathbb{Z}$. PGCD & PPCM

Résumé -

Nous plongeons ici dans une des parties mathématiques les plus ancestrales : la théorie des nombres (entiers) ou arithmétique. Beaucoup de résultats présentés ici datent (au moins) d'Euclide (3-ième siècle avant notre ère) : la notion de divisibilité, associée à la division euclidienne.

Etonnamment, le meilleur point de vue sur la question est assez récent : il date des *Disquisitiones arithmeticae* de GAUSS, publié à l'aube du XIX siècle. Ce point de vue insiste sur les congruences (modulo n) comme des nouvelles égalités.

Nous nous concentrons ensuite, dans ce chapitre sur la notion de PGCD de deux (ou plusieurs nombres) et l'algorithme d'Euclide pour l'obtenir. Un théorème clé, ignoré des mathématiciens grecs, est la décomposition de (Bachet-)Bézout. C'est le théorème clé de ce chapitre.

On termine par l'étude du PPCM (sorte de complément symétrique du PGCD)

Youtube (parodies?) :

- Canal Universitaire - Arithmétique dans $\mathbb{Z}$ - <https://www.canal-u.tv/chaines/canal-universitaire/arithmetique-dans-z/chapitre-arithmetique-partie-1-division-euclidienne-et>
- Optimal sup-spé - Arithmétique modulaire - <https://www.youtube.com/watch?v=jZoOGB9WUms>

Sommaire

1. Problèmes	294
2. Divisibilité dans $\mathbb{Z}$	295
2.1. Intégrité de $\mathbb{Z}$ et régularité	295
2.2. Diviseurs, multiples	295
2.3. Division euclidienne de a par b	296
2.4. Arithmétique modulaire	298
3. Plus Grand Commun Diviseur de deux nombres	300
3.1. PGCD de deux nombres. Définition « naturelle »	300
3.2. Algorithme d'Euclide	300
3.3. Couple de Bézout	302
3.4. Deux caractérisations essentielles du PGCD	304
4. Entiers premiers entre eux. Factorisation	306
4.1. Définition et critère de Bézout	306
4.2. Lemme de Gauss et décomposition en facteurs relativement premiers	306
5. Généralisation à plusieurs entiers	308
5.1. PGCD d'un nombre fini d'entiers relatifs	308
5.2. Deux caractérisation du PGCD($a_1, a_2, \dots, a_k$)	309

5.3.	Entiers premiers entre eux dans leur ensemble . . .	310
6.	Plus Petit Commun Multiple	311
6.1.	Construction	311
6.2.	Relation PPCM et PGCD	313
7.	Bilan	313

1. Problèmes

? **Problème 70 - Pairs, impairs et ...**

L'addition de deux nombres pairs ou de deux nombres impairs donnent **toujours** un nombre pair.
L'addition d'un nombre pair et d'un nombre impair deux toujours un nombre impair.
Une multiplication donne un nombre impair si et seulement si les deux nombres multipliés sont impairs.
Comment démontrer ces résultats? Existe-t-il un résultat équivalent pour des multiples de 3, 4, 5, n ?
A propos de multiples, on sait que les nombres divisibles par 9 (et 3) sont exactement ceux dont la somme des chiffres est divisible par 9 (respectivement par 3). Est-ce vrai? Pourquoi? Existe-t-il d'autres règles équivalentes?

? **Problème 71 - Table de multiplication modulo n**

Lorsqu'on trace les tables des multiplications modulo 5 ou modulo 6, on trouve les deux tableaux suivants :

$\times_{[5]}$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\times_{[6]}$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

on voit que sur certaines lignes, on retrouve tous les nombres possibles et pas sur d'autres. Pourquoi?
Existe-t-il des tableaux où sur toutes les lignes on retrouve tous les nombres (comme celui de la multiplication modulo 5)?

? **Problème 72 - Représentation sous un treilli**

La divisibilité est l'exemple typique d'une relation d'ordre non totale.
Le treillis est le bon outil pour visualiser les relations d'ordre non totales.
Est-il possible de convertir tous les théorèmes qui suivent en un schéma visuel basé sur des treillis?

? **Problème 73 - Division euclidienne et PGCD**

Si la division de a par b donne combien de fois on peut placer b dans a (quotient) et la place qui reste (reste), on peut continuer l'algorithme en plaçant ensuite r dans b ...
On crée ainsi l'algorithme d'Euclide. Est-ce que cela (se) termine?

- Qu'est-ce qu'on obtient au bout du compte

? Problème 74 - Monde fictif

Dans un monde où il n'y aurait que des pièces de 3 euros et 5 euros, quel montant pourrions-nous payer? (Sachant que le vendeur pourrait nous rendre la monnaie).

Et s'il y a des pièces de 6 et 9 euros?

Et des pièces de 6, 10 et 15 euros?

2. Divisibilité dans $\mathbb{Z}$

2.1. Intégrité de $\mathbb{Z}$ et régularité

Proposition - Intégrité de l'anneau $\mathbb{Z}$

$\mathbb{Z}$ est un anneau intègre.

Formellement :

$$\forall a, b \in \mathbb{Z}, \quad a \times b = 0 \implies a = 0 \text{ ou } b = 0$$

Démonstration

Comme pour tout anneau intègre :

Proposition - Régularité

Les éléments non nuls de $\mathbb{Z}$ sont réguliers. Formellement :

$$\forall a \in \mathbb{Z}, a \neq 0, \quad \forall b, c \in \mathbb{Z}, a \times b = a \times c \implies b = c$$

Démonstration

Pour aller plus loin - Anneaux, Corps...

Nous reviendrons sur ces propriétés formalisées lorsque nous étudierons les anneaux (euclidiens).

On a vu dans le cours sur les groupes, que l'inversibilité entraîne la régularité. On voit ici que la réciproque est fausse.

Il existe donc des anneaux intègres qui ne sont pas des corps

Remarque - A quoi sert cette propriété?

Ce résultat assure l'unicité de la décomposition, si a divise d , il n'y a qu'une décomposition possible de d sous la forme $a \times b$.

Par ailleurs, on remarque aussi, qu'à ce stade, n'avons pas besoin de plonger dans $\mathbb{Q}$ l'inégalité $a \times b = a \times c$ en faisant une division par a . Cela est rassurant.

2.2. Diviseurs, multiples

Définition - Diviseur, multiple

Soit $(a, b) \in \mathbb{Z}^2$. On dit que b divise a s'il existe $k \in \mathbb{Z}$ tel que $a = kb$ et on note $b|a$.

On dit aussi que b est un diviseur de a , ou que a est un multiple de b .

On note $b\mathbb{Z} = \{b \times k; k \in \mathbb{Z}\}$ l'ensemble des multiples de b .

 Savoir faire - Montrer que b divise a

(Sous-entendu en arithmétique entière) Le plus important n'est pas de montrer l'existence de k tel que b divise a , mais bien montrer qu'il s'agit d'un nombre entier.

Définition - Ensemble des diviseurs

On notera par la suite $\mathcal{D}(a)$ l'ensemble des diviseurs de a . Pour $a \neq 0$, cet ensemble ne contient qu'un nombre fini d'éléments puisque

$$d|a \Rightarrow |d| \leq |a|.$$

 Application - Majoration du cardinal **Remarque - Le cas de 0 et 1**

- 1 et -1 divisent tous les entiers mais ne sont divisibles que par 1 et -1 .
- 0 est un multiple de tous les entiers mais n'est diviseur que de lui-même.

Définition - Nombres associés

Soit $(a, b) \in \mathbb{Z}^2$. on dit que a et b sont associés si $a|b$ et $b|a$. On a la caractérisation suivante :

$$(a|b \text{ et } b|a) \Leftrightarrow |a| = |b| \Leftrightarrow a = \epsilon b \text{ avec } \epsilon \in \{-1, 1\} = \mathbb{Z}^{\times}$$

Proposition - Division de combinaison linéaire

Soit $(a, b) \in \mathbb{Z}^2$. Pour $(u, v) \in \mathbb{Z}^2$, $n \in \mathbb{Z}$, $n \neq 0$ on a :

$$(d|a \text{ et } d|b) \Rightarrow d|au + bv$$

$$an|bn \Leftrightarrow a|b$$

DémonstrationExercice

Montrer que la relation « divise » est une relation d'ordre

2.3. Division euclidienne de a par b **Théorie** **Heuristique - La division euclidienne : des soustractions!**

A cause de l'algorithme de la division présentée au XIV-ième par Fibonacci, très efficace, on a tendance à considérer la division euclidienne comme une vraie division de a par b , qui s'arrête avant d'écrire les chiffres derrière la virgule.

Mais il est souvent beaucoup plus efficace de considérer l'algorithme d'Euclide comme une succession de soustraction de a par b (ou d'addition de b à a si $a < 0$).

L'algorithme suivant le précise.

Théorème - Division euclidienne

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \text{ et } 0 \leq r < b.$$

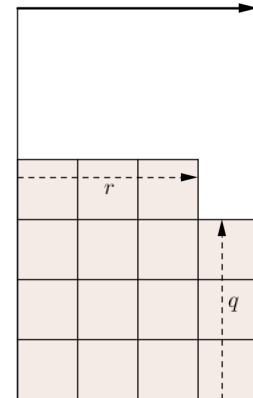
q et r sont appelés respectivement quotient et reste de la division euclidienne de a par b .

Dans ce cours, nous noterons comme en Python : $a // b$ pour désigner q et $a \% b$ pour désigner r .

Démonstration

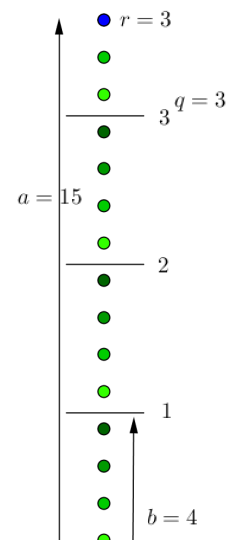
✳ **Représentation - Première représentation de la division euclidienne**

sur l'exemple de 15 divisé par 4 :



✳ **Représentation - Deuxième représentation de la division euclidienne**

sur l'exemple de 15 divisé par 4 :

**Proposition - Critère de divisibilité et division euclidienne**

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$.

$b|a$ si et seulement si le reste de la division euclidienne de a par b vaut 0.

Démonstration**Algorithme**

Cette démonstration n'est pas explicite. On préférera le programme suivant :

📁 **Informatique - Division euclidienne**

```

1 def div_eucl(a,b):
2     """division euclidienne de a par b"""
3     #Principe : on soustrait b autant que nécessaire a a
4     d,k=a,0
5     if a<0 :
6         c,eps=-b,-1 # si a<0, il faudra additionner b
7     else :
8         c,eps=b,1
9     while d>=b or d<0:
10         d=d-c
11         k=k+eps #k = nbre de soustractions = quotient
12     return (k,d)

```

 Application - Déroulement de $\text{div_eucl}(12, 5)$ et $\text{div_eucl}(-12, 5)$

 Informatique - Récursivité

Une autre possibilité est d'exploiter la récursivité :

```

1  def div_eucl_rec(a,b):
2      """calcul de la division euclidienne de a par b, par récursivité"""
3      if a<b and a>-1:
4          return (0,a)
5      elif a>b :
6          m,n=div_eucl_rec(a-b,b)
7          return (m+1,n)
8      else :
9          m,n=div_eucl_rec(a+b,b)
10         return (m-1,n)

```

 Pour aller plus loin - Démontrer qu'un programme fait bien ce qu'il faut...

Pour démontrer qu'un programme fait bien ce qu'il faut, on a besoin :

- d'un variant de boucle.
Il nous assure la terminaison du programme.
Ici on prend d
- d'un invariant de boucle.
Connaissant sa valeur initiale et finale, on obtient le résultat final donné par l'algorithme. On compare avec le résultat attendu.
Ici, on considère $kb+d=a$

2.4. Arithmétique modulaire

Relation d'équivalence

Définition - a congru à b modulo n

Soient $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.

On dit que a est congru à b modulo n si n divise $a - b$ ($\Leftrightarrow a - b \in n\mathbb{Z}$),
c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

On note $a \equiv b[n]$.

Pour tout $n \in \mathbb{N}^*$, la relation de congruence modulo n est une relation d'équivalence (nous l'avons déjà vu).

 Remarque - $\mathbb{U}_n$

Le groupe des racines n -ième de l'unité (avec la multiplication) est bien un lieu où les congruences modulo n sont naturelles.

En effet, si on note $\xi_r = \exp(\frac{2ri\pi}{n})$, on a $\xi_r = \xi_{r'}$ ssi $r \equiv r'[n]$.

Puis, si on considère $\xi_r \times \xi_s$, on trouve $\xi_{r+s} = \xi_{(r+s)\%n}$.

La proposition suivante donne un système de représentant naturel (et donc le nombre de classe d'équivalence)

Proposition - Reste

Soit $n \in \mathbb{N}^*$. Pour tout $a, b \in \mathbb{Z}$

$$a \equiv b[n] \Leftrightarrow a \% n = b \% n.$$

Ainsi, $[0, n-1]$ est un système de représentant de $\frac{\mathbb{Z}}{\equiv \cdot [n]}$, ensemble possédant donc n éléments

Démonstration

Arithmétique modulaire

Proposition - Opérations : arithmétique modulaire

Soit $n \in \mathbb{N}$. La congruence modulo n est compatible avec l'addition et la multiplication :

Pour a, a', b, b' entiers relatifs on a

$$\begin{cases} a \equiv a' [n] \\ b \equiv b' [n] \end{cases} \implies \begin{cases} a + b \equiv a' + b' [n] \\ a \times b \equiv a' \times b' [n] \end{cases}$$

Démonstration

Truc & Astuce pour le calcul - Réduction modulo n

La réduction modulo n réduit les calculs : les nombres ne dépassent pas la valeur n .

En revanche, on perd des informations ou bien parfois, on supprime les informations inutiles (à quoi sert de connaître exactement un nombre, alors que seul son dernier chiffre est demandé?)

Remarque - Vérifier un calcul

Dans l'art de calculer, nous avons vu l'importance d'avoir des clés de vérification de calcul.

Ainsi d'après la formule précédente, si $a \equiv a' [n]$, alors $a^k \equiv a'^k [n]$,

et par linéarité, pour tout polynôme $P : P(a) \equiv P(a') [n]$.

Par exemple, montrer qu'une racine entière x d'un polynôme $P = a_0 + a_1 X + \dots + a_d X^d \in \mathbb{Z}[X]$ vérifie : $x | a_0$.

Il suffit d'écrire : $P(x) = 0 = a_0 + a_1 x + \dots + a_d x^d \equiv a_0 [x]$.

Exercice

Avons-nous l'équivalence $a \equiv b [n] \iff ca \equiv cb [n]$?

Quelle est l'implication. Donner un contre-exemple de l'implication réciproque. Une condition pour l'équivalence ?

Remarque - Réduction modulo p , $p \in \mathcal{P}$

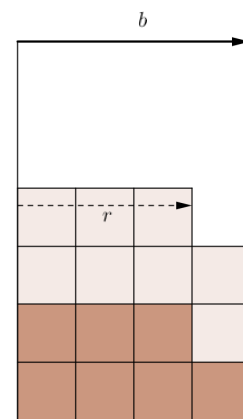
Si p est premier, donc premier avec tous les nombres, pour tout $a \in \mathbb{Z}$, $a \wedge p = 1$, donc d'après le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tels que $ua + vp = 1$, donc modulo p : $au \equiv 1 [p]$.

Ainsi, a est inversible. Donc $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps (tous les éléments sont inversibles, donc régulier).

***Représentation - Voir les congruences modulo n**

Si on prend l'habitude de regarder les congruences modulo n dans un damier (comme lors de la première représentation).

Alors $a \equiv b [n]$ ssi le dernier carré de a et de b est dans la même colonne. Ici $15 \equiv 7 [4]$.



3. Plus Grand Commun Diviseur de deux nombres

3.1. PGCD de deux nombres. Définition « naturelle »

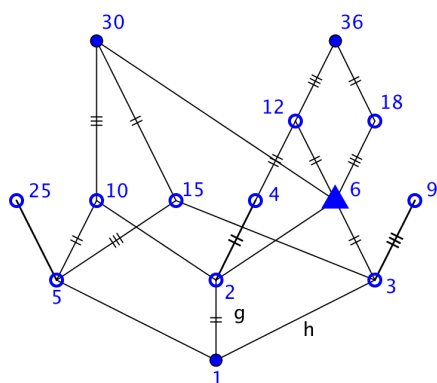
Il s'agit du plus grand pour la relation d'ordre classique : $\leq$.

🔍 Analyse - Construction du PGCD

🔍 Pour aller plus loin - Treillis des diviseurs

Il est possible de représenter sous forme de treillis les diviseurs de 30 et 36 et chercher le PGCD.

C'est le plus grand pour $a \leq b$, mais aussi $a|b$



Définition - PGCD de a et b

Soient a et b deux entiers relatifs non nuls.

On appelle PGCD (Plus Grand Commun Diviseur) de a et b , le nombre

$$\text{PGCD}(a, b) = \max(\mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathbb{N}).$$

On le note également $a \wedge b$.

On a clairement $b \wedge a = a \wedge b = |a| \wedge |b|$.

Par convention on pose pour $a \in \mathbb{Z}$, $a \wedge 0 = |a|$ (y compris si $a = 0$).

🔍 Exemple - $a = 36, b = 30$

🛑 Remarque - Divisibilité des nombres de $\mathcal{D}(30) \cap \mathcal{D}(36)$

6, le PGCD(36, 30) est divisible par tous les éléments de $\mathcal{D}(30) \cap \mathcal{D}(36)$.

Et c'est le seul (avec son associé : -6)!

🛑 Remarque - Algorithme des facteurs premiers

Plus jeunes, les étudiants exploitaient l'algorithme de la décomposition en facteurs premiers.

Il s'agit de faire deux listes : celles des facteurs premiers de chacun des deux nombres. Puis on multiplie tous ceux qui sont en commun (avec leur multiplicité) pour obtenir le PGCD.

Tant que nous ne savons pas ce qu'est un nombre premier, cet algorithme attendra...

3.2. Algorithme d'Euclide

Algorithme des divisions successives pour obtenir le PGCD

Lemme - Stabilité par division euclidienne

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

Si $a = bq + r$, alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r) \cap \mathcal{D}(b)$ et donc $a \wedge b = b \wedge r$.

Démonstration

✎ Heuristique - Algorithme pour obtenir le PGCD de deux nombres

La proposition qui donne un algorithme qui exploite une suite de division euclidienne pour trouver le $PGCD(a, b)$.

Il permet également d'obtenir les coefficients de Bézout des nombres a et b .

On notera qu'il s'applique à deux nombres a et b vérifiant : $0 < b < a$. Toute recherche de $PGCD(a, b)$ se ramène à ce cas là, en effet :

- Si $b = 0$ alors $PGCD(a, b) = |a|$
- Si $b \neq 0$, notons alors que $PGCD(a, b) = PGCD(|a|, |b|) = PGCD(|b|, |a|)$,
on peut donc supposer que les deux nombres sont positifs et que le premier est le plus grand.

Proposition - Algorithme d'Euclide

Soient $a, b \in \mathbb{N}^*$. Supposons que $0 < b < a$. L'algorithme d'Euclide consiste en une succession de division euclidienne :

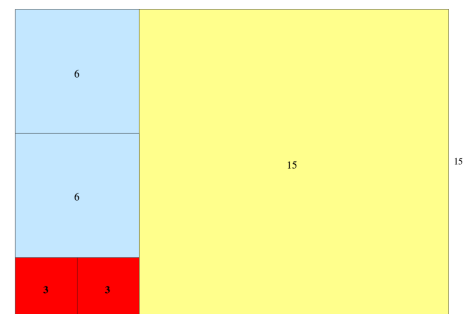
- On commence par poser $r_0 = a$ et $r_1 = b$;
- ensuite, k désignant un entier naturel non nul (étape de l'algorithme),
tant que $r_{k+1} \neq 0$,
on note r_{k+2} le reste de la division euclidienne de r_k par r_{k+1}
(on a donc $r_{k+2} < r_{k+1}$).

Il existe $N \in \mathbb{N}^*$ tel que $r_N = 0$,

r_{N-1} est alors le dernier reste non nul de la suite (r_k) , et : $a \wedge b = r_{N-1}$

✳ Représentation - Illustration de l'algorithme d'Euclide (Wikipedia)

pour $a = 21$ et $b = 15$. On complète les trous par des carrés horizontalement ↔ verticalement :



Ici le PGCD vaut 3

Démonstration

🔧 Application - $PGCD(1542, 58) = 2$

La division euclidienne s'exploite en pratique, c'est-à-dire avec un calcul réel, à savoir-faire (on fait plutôt des divisions que des soustractions). Ou bien

 Savoir faire - Exploiter la division euclidienne (théorie)

Si $f : \mathbb{Z}^2 \rightarrow E$ (E quelconque) tel que $f(a, b) = f(b, a \% b)$, alors $f(a, b) = f(a \wedge b, 0)$.

 Truc & Astuce pour le calcul - Trouver son erreur dans un algorithme d'Euclide

Une fois l'algorithme terminé, il est important de vérifier que le dernier reste non nul est bien un diviseur de a et de b .

Si ce n'est pas le cas, il faut revenir à la ligne de calcul où le reste obtenu n'est pas divisible par le PGCD-candidat.

 Informatique - Division euclidienne

On peut écrire l'algorithme d'Euclide sous Python. Remarquons que dans le programme ainsi écrit, on tient compte des cas $b = 0$ et a ou b négatif.

```

1 def alg_eucl(a,b):
2     """pgcd(a,b) par algorithme d'Euclide"""
3     if b==0:
4         return(a)
5     a1,a2=max(abs(a),abs(b)),min(abs(a),abs(b))
6     ra,rb=a1,a2
7     while rb!=0:
8         rc=div_eucl(ra,rb)[1]
9         ra,rb=rb,rc
10    return(ra)
```

 Pour aller plus loin - Fractions continues

L'algorithme d'Euclide a une autre application importante : la décomposition en fractions continues. C'est clairement le cas concernant les fractions comme le montre l'exemple :

$$\frac{1542}{58} = 26 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}}}$$

Mais c'est aussi le cas concernant les nombres irrationnels

3.3. Couple de Bézout**Exploitation plus fine de l'algorithme d'Euclide**

 **Analyse - Exploitation plus approfondie encore de l'algorithme d'Euclide**

Théorème - Coefficients de Bézout

Soit $(a, b) \in \mathbb{Z}^2$. Il existe des entiers u et v tels que $au + bv = a \wedge b$.

Un tel couple (u, v) est appelé un couple de coefficients de Bézout de a et b .

Savoir faire - Pas unicité du couple de Bézout. Les obtenir tous

Il n'y a pas unicité du couple (u, v) :

si (u_0, v_0) est un couple de Bézout, en divisant par $\delta = a \wedge b$:

$$ua + bv = u_0a + v_0b \Rightarrow \frac{a}{\delta}(u - u_0) = \frac{b}{\delta}(v_0 - v) \quad \Rightarrow \quad \frac{a}{\delta} \mid (v - v_0) \dots$$

lemme de Gauss

Alors pour tout $n \in \mathbb{Z}$, $(u_0 + n\frac{b}{\delta}, v_0 - n\frac{a}{\delta})$ en est aussi un.

Informatique - Division euclidienne

En étendant la division euclidienne (elle garde en mémoire les calculs des quotients), on peut obtenir les coefficients de Bézout

```

1 def Bezout(a, b):
2     """pgcd(a,b)+coefficient de Bezout"""
3     if b==0:
4         return (a)
5     a1, a2=max(abs(a), abs(b)), min(abs(a), abs(b))
6     u, uu=1, 0
7     v, vv=0, 1
8     ra, rb=a1, a2
9     while rb!=0:
10        q, rc=div_eucl(ra, rb)
11        ra, rb=rb, rc
12        u, uu=uu, u-q*uu
13        v, vv=vv, v-q*vv
14    return (ra, u, v)
```

Truc & Astuce pour le calcul - Obtenir un couple de Bézout

En pratique, il y a deux stratégies.

- Celle plutôt vue en terminale, assez naturelle et peut-être bien ancrée en vous. On trouve (u, v) en EN REMONTANT l'algorithme d'Euclide.
(à la main, il vaut mieux partir des valeurs numériques, elles n'arrivent qu'en fin d'algorithme).

Par exemple pour 1542 et 58 on a (en remontant les division euclidienne) :

$$\begin{aligned} 2 &= 10 - 2 \times 4 = 10 - 2(24 - 2 \times 10) = -2 \times 24 + 5 \times 10 = -2 \times 24 + 5 \times (34 - 24) \\ &= 5 \times 34 - 7 \times 24 = 5 \times 34 - 7 \times (58 - 34) = -7 \times 58 + 12 \times 34 \\ &= -7 \times 58 + 12 \times (1542 - 26 \times 58) = 12 \times 1542 - 319 \times 58 \end{aligned}$$

Donc $1542u + 58v = 2$, avec (par exemple) : $u = 12$ et $v = -319$.

- Celle qui découle ici, avec un tableau à remplir directement :

On rappelle qu'à chaque étape $k \in \mathbb{N}^*$: $r_{k+1} = q_k r_k + r_{k-1}$ et (u_k) et (v_k)

Histoire - Bézout

Etienne Bézout (1730-1783) est un mathématicien français. Il généralisa l'identité de Bachet, c'est pourquoi elle lui est couramment attachée.

**Histoire - Bachet de Méziriac ou Bézout**

Le théorème de Bézout est en fait obtenu pour la première fois par Gaspard Bachet de Méziriac (1581-1638). C'est un mathématicien, poète et traducteur français. Il a en particulier traduit *l'arithmetica* de Diophante (là où Fermat a écrit l'énoncé de son grand théorème), et est l'auteur de *Problèmes plaisants et délectables qui se font par les nombres*.



vérifient la même relation de récurrence $x_{k+1} = -q_k x_k + x_{k-1}$.

k	r_k	q_k	u_k	v_k	$1\,542 \times u_k + 58 \times v_k = r_k$
0	1 542		1	0	1 542
1	58	26	0	1	58
2	34	1	1	-26	34
3	24	1	-1	27	24
4	10	2	2	-53	10
5	4	2	-5	133	4
6	2	0	12	-319	2

Algorithme d'Euclide, arithmétique modulaire et carrelage

🔍 Analyse - Relation de Bézout modulaire

Exercice

Donner une représentation théorique de la recherche du PGCD de a et de b , par algorithme d'Euclide dans un carrelage.

On pourra appliquer la méthode pour donner le PGCD et les coefficients de Bézout pour les couples (13, 7) et (12, 6)

3.4. Deux caractérisations essentielles du PGCD

Caractérisation par divisibilité

En fait la définition de plus grand diviseur commun peut s'entendre d'une seconde façon : plus grand pour la relation d'ordre de divisibilité.

🛑 Remarque - Relation binaire

La relation binaire "est un diviseur de", définie par $a \mathcal{R} b \Leftrightarrow a|b$, est une relation d'ordre partiel sur $\mathbb{N}$.

Pour cette relation d'ordre $\mathcal{D}(a) \cap \mathcal{D}(b)$ admet un plus grand élément qui est $a \wedge b$.

Proposition - Caractérisation essentielle du PGCD

Soit $(a, b) \in \mathbb{Z}^2$.

Alors $a \wedge b$ est le seul entier naturel dont les diviseurs sont exactement les diviseurs communs à a et b :

$$\mathcal{D}(a \wedge b) = \mathcal{D}(a) \cap \mathcal{D}(b)$$

autre façon de l'écrire :

$$\forall d \in \mathbb{Z}, (d|a \text{ et } d|b) \Leftrightarrow d|a \wedge b$$

🛑 Remarque - Force de cette propriété

Dans l'équivalence trouvée (ou la double inclusion d'ensemble),

une équivalence est triviale : $d|a \wedge b \Rightarrow d|a$ et $d|b$.

L'usage fréquent que l'on fera donc de cette proposition est : $d|a$ et $d|b \Rightarrow d|a \wedge b$.

Démonstration

 Savoir faire - Trouver un PGCD. Exploiter un PGCD.

On note $\delta = a \wedge b$.

Pour trouver le PGCD de a et b :

on démontre que si $m|a$ et $m|b$, alors nécessairement $m|\delta$.

Puis on cherche m le plus grand possible.

(si $m = 1$, a et b sont premiers entre eux).

Pour exploiter le PGCD de a et b :

on exploite le fait que si $m|\delta$, alors $m|a$ et $m|b$.

Et on travaille sur cette co-divisibilité.

 Application - $\lambda a \wedge \lambda b = \lambda(a \wedge b)$ **Caractérisation par combinaison linéaire****Proposition - Combinaison linéaire**

Soient $a, b \in \mathbb{Z}$.

On note $a\mathbb{Z} + b\mathbb{Z}$ l'ensemble $\{au + bv, (u, v) \in \mathbb{Z}\}$ des combinaisons linéaires de a et b .

Alors

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Démonstration

 Pour aller plus loin - Construction classique

La tradition mathématique utilise donc une autre stratégie pour **définir** le PGCD de a et b :

1. on s'intéresse à l'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{ua + vb, u, v \in \mathbb{Z}\}$
2. on **démontre** qu'il existe $\delta \in \mathbb{N}^*$ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$

On appelle alors δ le PGCD de a, b

✂ **Savoir faire - Combinaisons linéaires (entières)**

Dès que l'on a des combinaisons linéaires d'entiers (on appelle cela un réseau d'entiers), il faut penser que la maille élémentaire est donnée par le PGCD des nombres. C'est par exemple, le cas du problème « monde fictif »

4. Entiers premiers entre eux. Factorisation

4.1. Définition et critère de Bézout

Définition - Couple d'entiers premiers entre eux

a et b sont dits premiers entre eux si $a \wedge b = 1$.

On note que pour le théorème suivant, nous avons bien une équivalence :

Théorème - Théorème (ou identité) de Bézout

Soient a et b deux entiers relatifs non nuls. Alors

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2 \text{ tel que } au + bv = 1$$

 Histoire - Disquisitiones Arithmeticae

En 1801, Gauss âgé de 24 ans publie les *Disquisitiones Arithmeticae* (recherches arithmétiques) et révolutionne totalement le genre. Pour la première fois, on pense les nombres à l'aide de l'arithmétique modulaire (congruence - voir fin de chapitre)!



Démonstration

Comme il est plus simple de travailler avec des nombres premiers entre eux, on exploite souvent le savoir-faire suivant :

✂ **Savoir faire - Réduction à des entiers premiers entre eux (1)**

Soient $a, b \in \mathbb{Z}$. On note $\delta = a \wedge b$.

Alors, $a = \delta a'$ et $b = \delta b'$, avec $a' \wedge b' = 1$.

Puis on travaille avec les a' et b'

4.2. Lemme de Gauss et décomposition en facteurs relativement premiers

Enoncé

Théorème - Lemme de Gauss

Soient $a, b, c \in \mathbb{Z}$. Alors

$$(a \wedge b = 1 \text{ et } a|bc) \implies a|c.$$

Démonstration

Facteur relativement premier

Proposition - Facteur relativement premier

Soient $a, b, c \in \mathbb{Z}$. Alors

$$(a \wedge b = 1 \text{ et } a \wedge c = 1) \implies a \wedge bc = 1 \text{ (réciproque vraie)}$$

$$(a \wedge b = 1, a|c, b|c) \implies ab|c$$

Démonstration**Exercice**

On note $\mathcal{P}_a$, l'ensemble des nombres premiers avec a et $a\mathbb{Z}$, les multiples de a .
Ré-écrire les théorèmes de GAUSS avec ces ensembles.

Plusieurs facteurs (relativement premiers)**Corollaire - Facteurs premiers**

Soient $a, c, b_1, \dots, b_n$ des entiers relatifs.

$$(\forall i \in \llbracket 1, n \rrbracket, a \wedge b_i = 1) \implies a \wedge \prod_{i=1}^n b_i = 1$$

$$(\forall (i, j) \in \llbracket 1, n \rrbracket^2, i \neq j \Rightarrow b_i \wedge b_j = 1 \text{ et } \forall i \in \llbracket 1, n \rrbracket, b_i|c) \implies \prod_{i=1}^n b_i | c$$

Démonstration**Corollaire - Forme irréductible d'un rationnel**

Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{p}{q}$ et tel que p et q soient premiers entre eux.

Cette écriture est appelée la forme irréductible de r .

Les autres écritures fractionnaires sont de la forme $r = \frac{\lambda p}{\lambda q}$ avec $\lambda \in \mathbb{Z}^*$.

Démonstration

5. Généralisation à plusieurs entiers

5.1. PGCD d'un nombre fini d'entiers relatifs

Heuristique - Définition

Au lieu de construire le PGCD de k nombres en prenant :

$$\delta = \max(\mathcal{D}(a_1) \cap \mathcal{D}(a_2) \cdots \mathcal{D}(a_k) \cap \mathbb{N})$$

nous allons prendre pour définition, une méthode récursive.

On notera ensuite l'extension de la caractéristique vue par la suite :

$$d|a \text{ et } d|b \implies d|\delta$$

Dans ce cas le terme « plus grand » ne doit pas être pris pour la relation d'ordre $n \leq n$, mais pour la relation d'ordre $n|m$.



Pour aller plus loin - Lien PGCD et $\inf$

$\inf E$ est le plus grand des minorants de E .

- $\forall x \in E, \inf E \leq x$
- $\forall m$ tel que $\forall x \in E, m \leq x$, alors $m \leq \inf E$.

PGCD(E) est le plus grand des diviseurs de E .

- $\forall x \in E, \text{PGCD}(E) | x$
- $\forall m$ tel que $\forall x \in E, m | x$, alors $m | \text{PGCD}(E)$.

Ce n'est pas la méthode la plus naturelle (compte-tenu du nom PGCD), mais la plus pratique pour les démonstrations...

Définition - Définition par récurrence

Soient $k \in \mathbb{N}^*$, $k \geq 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$. Alors, on définit récursivement :

$$\bigwedge_{i=1}^k a_i := \left(\bigwedge_{i=1}^{k-1} a_i \right) \wedge a_k$$

L'identité de Bézout se généralise également :

Proposition - Décomposition de Bézout

Soient $k \in \mathbb{N}^*$, $k \geq 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$.

$$\exists (u_1, \dots, u_k) \in \mathbb{Z}^k \quad \Bigg| \quad \bigwedge_{i=1}^k a_i = \sum_{i=1}^k u_i a_i.$$

Démonstration

Proposition - Avec l'ensemble des diviseurs

Pour tout $j \in \mathbb{N}_k$, $\bigwedge_{i=1}^k a_i$ est un diviseur de a_j .

Mieux : $\bigwedge_{i=1}^k a_i = \max(\mathcal{D}(a_1) \cap \mathcal{D}(a_2) \cdots \mathcal{D}(a_k) \cap \mathbb{N})$,
au choix pour max : au sens de la relation d'ordre $|$ ou $\leq$.

On a $\mathcal{D}(\bigwedge_{i=1}^k a_i) = \bigcap_{j=1}^k \mathcal{D}(a_j)$.

Démonstration**5.2. Deux caractérisation du $PGCD(a_1, a_2, \dots, a_k)$**

Réécriture de la propriété précédente :

Proposition - Critère caractéristique du $PGCD(a_1, a_2, \dots, a_k)$

Soient $k \in \mathbb{N}^*$, $k \geq 2$, et $(a_1, a_2, \dots, a_k) \in \mathbb{Z}^k$.

$(\bigwedge_{i=1}^k a_i)$ est l'unique entier naturel d dont les diviseurs sont exactement les diviseurs communs à tous les a_i , c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, \quad (\forall i \in \llbracket 1, k \rrbracket, n|a_i) \iff n|d.$$

Démonstration

Cela donne bien une caractérisation

✂ Savoir faire - Démontrer/utiliser le PGCD de $(a_1, a_2, \dots, a_k)$

Tout diviseur du PGCD, divise chaque a_i .

Tout diviseur de tous les a_i est un diviseur de leur PGCD.

Et le PGCD est le plus grand de tous les diviseurs au sens de la relation d'ordre de la division (c'est une borne inférieure).

Proposition - Linéarité absolue

Le PGCD de $(xa_1, xa_2, \dots, xa_k)$ est $x \mid \times \bigwedge_{i=1}^k a_i$

Démonstration**Proposition - Sous-groupe $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_k\mathbb{Z}$**

Soient $a_1, a_2, \dots, a_k \in \mathbb{N}$.

Alors $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_k\mathbb{Z}$ est exactement le sous-groupe de $(\mathbb{Z}, +)$: $(\bigwedge_{i=1}^k a_i)\mathbb{Z}$.

Autrement écrit, le groupe engendré par $\{a_1, a_2, \dots, a_k\}$ est le groupe $(\bigwedge_{i=1}^k a_i)\mathbb{Z}$.

$$\langle a_1, a_2, \dots, a_k \rangle_{\mathbb{Z}} = \left(\bigwedge_{i=1}^k a_i \right) \mathbb{Z}$$

Démonstration**5.3. Entiers premiers entre eux dans leur ensemble****Définition - Entiers premiers entre eux dans leur ensemble**

Les entiers $a_1, \dots, a_k$ sont dits premiers entre eux dans leur ensemble si leur PGCD vaut 1.

⚠ Attention - Ne pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux »

Il ne faut pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».
 Par exemple $a = \quad, b = \quad, c = \quad$
 sont
 ne sont pas

Tous les savoir-faire donnés précédemment sur les PGCD se généralisent à plusieurs nombres. Nous ne les ré-écrivons pas mais il faudra savoir y penser. Voici un exemple

🔧 Savoir faire - Réduction à des entiers premiers entre eux (2)

Soient $a_1, a_2, \dots, a_k \in \mathbb{Z}$. On note $\delta = \bigwedge_{i=1}^k a_i$.
 Alors pour tout $i \in \llbracket 1, k \rrbracket$, $a_i = \delta a'_i$, avec $(a'_1, a'_2, \dots, a'_k)$ premiers entre eux dans leur ensemble.
 Puis on travaille avec les a'_i

Proposition - Théorème (identité) de Bézout

Soient $a_1, \dots, a_k$ des entiers relatifs. Alors

$$\bigwedge_{i=1}^k a_i = 1 \iff \exists (u_1, \dots, u_k) \in \mathbb{Z}^k \mid \sum_{i=1}^k u_i a_i = 1$$

Démonstration

Selon que l'on cherche à montrer que des nombres sont premiers entre eux, ou utiliser cette connaissance, on exploite ce l'identité de Bézout de l'une ou l'autre de ces façons :

🔧 Savoir faire - Exploiter l'identité de Bézout

Pour montrer que $(a_1, \dots, a_n)$ sont premiers entre eux, ils arrivent, qu'on montre :

$$\exists u_1, u_2, \dots, u_n \in \mathbb{Z} \text{ tels que } \sum_{i=1}^n u_i a_i = 1$$

Quand, on sait que $(a_1, \dots, a_n)$ sont premiers entre eux, on génère alors

$$u_1, u_2, \dots, u_n \in \mathbb{Z} \text{ tels que } \sum_{i=1}^n u_i a_i = 1 \text{ et on exploite ces } (u_i).$$

6. Plus Petit Commun Multiple

6.1. Construction

On considère une borne supérieure...

🔍 Analyse - Construction du PPCM

Définition - PPCM de a et de b

Soient a et b deux entiers relatifs non nuls.

On appelle *PPCM* (Plus Petit Commun Multiple) de a et b , le nombre

$$\text{PPCM}(a, b) = \min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*)$$

On le note également $a \vee b$.

On a clairement $b \vee a = a \vee b = |a| \vee |b|$.

Les deux caractéristiques du PGCD se fusionne en une seule, concernant le PPCM :

Proposition - Caractérisation essentielle du PPCM

Soit $(a, b) \in \mathbb{Z}^2$. Alors $a \vee b$ est le seul entier naturel dont les multiples sont exactement les multiples communs à a et b

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

c'est-à-dire tel que

$$\forall m \in \mathbb{Z}, (a|m \text{ et } b|m) \iff a \vee b|m$$

Démonstration**🔧 Savoir faire - Trouver un PPCM. Exploiter un PPCM.**

On note $\mu = a \vee b$.

Pour trouver le PPCM ,

on démontre que si $a|m$ et $b|m$, alors nécessairement $\mu|m$.

Puis on cherche le m le plus petit possible.

Pour exploiter le PPCM,

on exploite le fait que si $\mu|m$, alors $a|m$ et $b|m$.

Et on travaille sur cette co-divisibilité.

Proposition - Linéarité

Soient $a, b, \lambda \in \mathbb{Z}$, alors $\lambda a \vee \lambda b = |\lambda|(a \vee b)$.

Démonstration

6.2. Relation PPCM et PGCD

Proposition - Relation PPCM et PGCDSoient $a, b \in \mathbb{Z}$.

- si $a \wedge b = 1$ alors $|ab| = (a \vee b)$.
- dans le cas général, $|ab| = (a \wedge b) \times (a \vee b)$.

Démonstration

 Remarque - Généralisation à un nombre fini d'entiers

On peut également généraliser la notion de PPCM à un nombre fini d'entiers relatifs. Il existe un unique entier naturel m dont les multiples sont exactement les multiples communs à tous les a_i , c'est-à-dire tel que

$$\forall n \in \mathbb{Z}, (\forall i \in \llbracket 1, k \rrbracket, a_i | n) \iff m | n.$$

On l'appelle PPPCM de $a_1, a_2, \dots, a_k$ et on le note $a_1 \vee a_2 \vee \dots \vee a_k$ ou $\bigvee_{i=1}^k a_i$.

7. Bilan

Synthèse

- ↪ Les nombres entiers relatifs sont les premiers objets reconnus comme mathématiques rencontrés. Ils sont donc comme à la base du sentiment mathématique de tout apprenti mathématicien.
- ↪ Comme un jeu, leur manipulation est ludique. On travaille uniquement avec addition et soustraction, puis multiplication ou division euclidienne (soustractions répétées). Pour deux (voire n) nombres quelconques, le commun est le PGCD. C'est comme la plus grosse molécule constitutive de chacun de ces nombres; avec ces deux nombres, il n'est pas possible de dégager des nombres plus fins que cette molécule. De là, de nombreux lemmes, théorèmes découlent dont les essentielles : théorème de Bézout et lemme de Gauss. On peut également réfléchir en terme de PPCM.

$\rightsquigarrow$ Reprenant une idée fondamentale simple et simplifiante de GAUSS, nous pouvons étudier les nombres entiers réduits modulo n . La plupart des propriétés arithmétiques se prolongent bien lors de cette réduction : addition et multiplication (pas très bien pour la division, car tous les nombres ne sont pas nécessairement inversibles...).

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Montrer que b divise a
- Truc & Astuce pour le calcul - Réduction modulo n
- Savoir-faire - Exploiter la division euclidienne (théorie)
- Truc & Astuce pour le calcul - Trouver une erreur dans un algorithme d'Euclide
- Savoir-faire - Pas d'unicité du couple de Bézout. Les obtenir tous
- Truc & Astuce pour le calcul - Obtenir un couple de Bézout
- Savoir-faire - Trouver un PGCD. Exploiter un PGCD.
- Savoir-faire - Combinaisons linéaires (entières)
- Savoir-faire - Réduction à des entiers premiers entre eux (1)
- Savoir-faire - Démontrer/utiliser le PGCD de $(a_1, a_2, \dots, a_k)$
- Savoir-faire - Réduction à des entiers premiers entre eux (2)
- Savoir-faire - Exploiter l'identité de Bézout
- Savoir-faire - Trouver un PPCM. Exploiter un PPCM.

Notations

Notations	Définitions	Propriétés	Remarques
$\mathcal{D}(a)$	Ensemble des diviseurs de a		
$a\mathbb{Z}$	Ensemble des multiples de a		
$a // b, a \% b$	Quotient et reste (resp.) de la division euclidienne de a par b	$a = (a // b) \times b + (a \% b)$ avec $a \% b \in [0, b - 1]$	Notations Python. Non officielle.
$a \equiv b[n]$	$n (b - a) \iff \exists k \in \mathbb{Z} \text{ tel que } a = b + nk$	Relation de congruence modulo n (relation d'équivalence)	$\forall a \in \mathbb{Z}, n \in \mathbb{N}, a \equiv (a \% n) [n]$
$a \wedge b$	PGCD de a et b (généralisable)	$a \wedge b = \max(\mathcal{D}(a) \cap \mathcal{D}(b))$ $d a \text{ et } d b \text{ ssi } d a \wedge b$	$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$
$a \vee b$	PPCM de a et b (généralisable)	$a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z})$ $a m \text{ et } b m \text{ ssi } a \vee b m$	$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$
$\mathcal{P}_a$	Ensemble des nombres premiers avec a	$b \in \mathcal{P}_a \iff a \wedge b = 1$	Equivalent à $a \in \mathcal{P}_b$ (symétrie)

Retour sur les problèmes

70. Oui, on peut tout faire. Sinon, on rajoute le nombre dans les premiers.
71. C'est les congruences.
72. Par exemple, les nombres premiers sont les nombres au premier étage du treillis des diviseurs.
Le PGCD de deux nombres a et b est celui situé le plus haut dans les racines communes de a et de b .
Le PPCM de deux nombres a et b est celui situé le plus bas dans les décédants communs de a et de b ...
73. Oui cela termine (suite d'entiers naturels, strictement décroissantes).
On obtient en dernier reste non nul, le PGCD.
74. Avec 3 et 5 euros, on peut obtenir tous les nombres entiers d'euros.
Avec 6 et 9 euros, on peut obtenir tous les multiples de 3 euros.
Avec 6, 10 et 15 euros, on peut obtenir tous les nombres entiers d'euros $(6 + 10 - 15)$.