Chapitre 14

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.
Etonnament, 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 Universaitaire - Arithmétique dans Z - https ://www.canal-u.tv/chaines/canal-unisciel/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 288
2. Divisibilité dans $\mathbb{Z}$. Avec un nombre a 289
2.1. Intégrité de $\mathbb{Z}$ et régularité 289
2.2. Diviseurs, multiples de a 289
2.3. Division euclidienne de n par a. 291
2.4. Arithmétique modulaire 292
3. Plus Grand Commun Diviseur de deux nombres. Avec deux nombres $a, b \in \mathbb{Z}$. 294
3.1. $a\mathbb{Z} + b\mathbb{Z}$ 294
3.2. $PGCD$ des deux nombres a et b. Définition « naturelle » 295
3.3. Algorithmes 297
4. Entiers premiers entre eux. Factorisation 300
4.1. Définition et critère de Bézout 300
4.2. Lemme de Gauss et décomposition en facteurs relativement premiers 301
5. Généralisation à plusieurs entiers 302
5.1. $PGCD$ d'un nombre fini d'entiers relatifs 302
5.2. Deux caractérisation du $PGCD(a_1, a_2, \dots a_k)$ 303

5.3. Entiers premiers entre eux dans leur ensemble . . . 305
6. Plus Petit Commun Multiple 305
6.1. Construction 305
6.2. Relation PPCM et PGCD 307
7. Bilan 307

1. Problèmes

? Problème 67 - 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 68 - 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 ou sur toutes les lignes on retrouve tous les nombres (comme celui de la multiplication modulo 5) ?

? Problème 69 - 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 70 - 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 71 - 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 $\mathbb{Z}$. Avec un nombre a

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

Proposition - Intégrité de l'anneau $\mathbb{Z}$
$\mathbb{Z}$ est un anneau intègre.
Formellement :

$$\forall\, n, m \in \mathbb{Z}, \qquad n \times m = 0 \Longrightarrow n = 0 \text{ ou } m = 0$$

Démonstration

Comme pour tout anneau intègre :

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

$$\forall\, a \in \mathbb{Z},\, a \neq 0, \qquad \forall\, k, h \in \mathbb{Z},\, a \times k = a \times h \Longrightarrow k = h$$

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 entraine 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 n, il n'y a qu'une décomposition possible de n sous la forme $a \times k$.
Par ailleurs, on remarque aussi, qu'à ce stade, n'avons pas besoin de plonger dans $\mathbb{Q}$ l'inégalité $a \times n = a \times m$ en faisant une division par a. Cela est rassurant.

2.2. Diviseurs, multiples de a

Définition - Diviseur, multiple
Soit $(a,n) \in \mathbb{Z}^2$. On dit que a divise n s'il existe $k \in \mathbb{Z}$ tel que $n = ak$ et on note $a|n$.
On dit aussi que a est un diviseur de n, ou que n est un multiple de a.
On note $a\mathbb{Z} = \{a \times k;\ k \in \mathbb{Z}\}$ l'ensemble des multiples de a.
Encore, n est un multiple de a ssi $n \in a\mathbb{Z}$.

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

Définition - Ensemble des diviseurs
On notera par la suite $\mathscr{D}(n)$ l'ensemble des diviseurs de n. Pour $n \neq 0$, cet ensemble ne contient qu'un nombre fini d'éléments
puisque $a \in \mathscr{D}(n) \Rightarrow a|n \Rightarrow |a| \leqslant |n|$.,
Donc $\mathscr{D}(n) \subset [\![-n, n]\!]$.

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 :

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

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 :

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

$$an|bn \Longleftrightarrow a|b$$

Démonstration

Remarque - Réciproque ?
Trouver à quelle(s) condition(s) (sur d*, sur* (u,v)*) :* $d|au+bv \Longrightarrow d|a$ *et* $d|b$ *nous occupera principalement en partie 3 ici*
Exercice
Montrer que la relation « divise » est une relation d'ordre sur $\mathbb{N}$

2.3. Division euclidienne de n par a.

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.

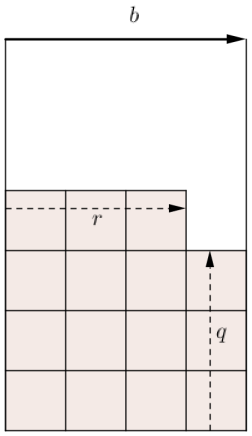
Théorème - Division euclidienne
Soient $n \in \mathbb{Z}$, $a \in \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$n = aq + r \text{ et } 0 \leqslant r < a.$$

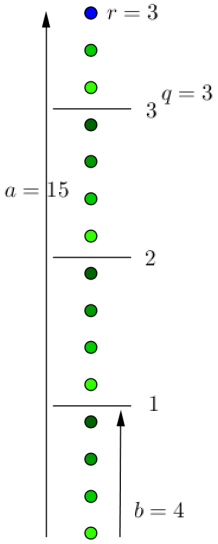
q et r sont appelés respectivement quotient et reste de la division euclidienne de n par a.
Dans ce cours, nous noterons comme en Python : $n//a$ pour désigner q et $n\%a$ pour désigner r.

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 *:*



Savoir faire - Critère de divisibilité par la division euclidienne

Soient $n \in \mathbb{Z}$, $a \in \mathbb{N}^*$.
$a|n$ si et seulement si le reste de la division euclidienne de n par a vaut 0.
(Si $a<0$, on considère $-a$)

Démonstration

Algorithme

Cette démonstration n'est pas explicite. On préfèrera le programme suivant :
Informatique - Division euclidienne

```python
def div_eucl(n,a):
    """division euclidienne de n par a"""
    #Principe : on soustrait b autant que necessaire a a
    d,k=n,0
    if n<0 :
        c,eps=-a,-1 # si n<0, il faudra additionner a
    else :
        c,eps=a,1
    while d>=a or d<0:
        d=d-c
        k=k+eps #k = nbre de soustractions = quotient
    return(k,d)
```

Application - Déroulement de `div_eucl(12,5)` et `div_eucl(-12,5)`

Informatique - Récursivité

Une autre possibilité est d'exploiter la récursivité :

```python
def div_eucl_rec(n,a):
    """calcul de la division euclidienne de a par b, par recursivite"""
    if n<a and n>-1:
        return(0,n)
    elif n>a :
        m,p=div_eucl_rec(n-a,a)
        return(m+1,p)
    else :
        m,p=div_eucl_rec(n+a,a)
        return(m-1,p)
```

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 - n congru à m modulo a
Soient $a \in \mathbb{N}^*$, $n, m \in \mathbb{Z}$.
On dit que n est congru à m modulo a si a divise $n-m$ ($\iff n-m \in a\mathbb{Z}$),
c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $n = m + ak$.
On note $n \equiv m[a]$.

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

Remarque - $\mathbb{U}_n$

Le groupe des racines n-ieme 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 $a \in \mathbb{N}^*$. Pour tout $n, m \in \mathbb{Z}$

$$n \equiv m[a] \iff n\%a = m\%a.$$

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

Démonstration

Arithmétique modulaire

Proposition - Opérations : arithmétique modulaire
Soit $a \in \mathbb{N}^*$. La congruence modulo a est compatible avec l'addition et la multiplication :
Pour n, n', m, m' entiers relatifs on a

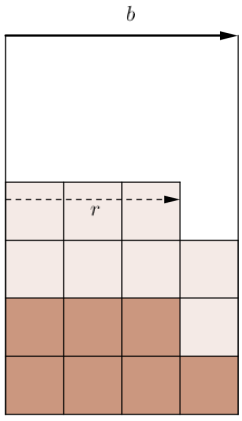
$$\begin{cases} n \equiv n'[a] \\ m \equiv m'[a] \end{cases} \implies \begin{cases} n+m \equiv n'+m'[a] \\ n \times m \equiv n' \times m'[a] \end{cases}$$

Démonstration

Truc & Astuce pour le calcul - Réduction modulo a
La réduction modulo a réduit les calculs : les nombres ne dépassent pas la valeur a.
En revanche, on perd des informations ou bien parfois, on supprime les informations inutiles (ex : à quoi sert de connaître exactement un nombre, alors que seul son dernier chiffre est demandé ? On regarde modulo 10.)

Remarque - Vérifier un calcul
Dans l'art de calculer, nous voyons l'importance d'avoir des clés de vérification de calcul.
Ainsi d'après la formule précédente, si $n \equiv n'[a]$, alors $n^k \equiv n'^k[a]$,
et par linéarité, pour tout polynôme P : $P(n) \equiv P(n')[a]$.
Par exemple, montrer qu'une racine entière x d'un polynôme $P = a_0 + a_1 X + \cdots + a_d X^d \in \mathbb{Z}[X]$ vérifie : $x | a_0$.
Il suffit d'écrire : $P(x) = 0 = a_0 + a_1 x + \cdots + a_d x^d \equiv a_0[x]$.

Représentation - Voir les congruences modulo a
Si on prend l'habitude de regarder les congruences modulo a dans un damier (comme lors de la première représentation).
Alors $n \equiv m[a]$ ssi le dernier carré de n et de m est dans la même colonne. Ici $15 \equiv 7[4]$.



Exercice

Avons-nous l'équivalence $n \equiv m[a] \iff kn \equiv km[a]$?
Quelle est l'implication. Donner un contre-exemple de l'implication réciproque. Une condition pour l'équivalence ?

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

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.

Heuristique - Bilan : des groupes affines parallèles...

A ce stade, on s'intéresse à UN nombre entier (naturel et non nul) a.
On décompose alors $\mathbb{Z} = + \bigcup_{r \in [\![0,a-1]\!]} \overline{r}$, avec $\overline{r} = \{n \in \mathbb{Z}; n\%a = r\} = \{n \in \mathbb{Z}; n \equiv r[a]\}$.
Tous les ensembles $\overline{r}$ sont comparables (translation des uns par rapport aux autres), seul l'ensemble $\overline{0} = a\mathbb{Z}$ est un groupe.
D'une certaine façon, les autres sont des groupes affines.

3. Plus Grand Commun Diviseur de deux nombres. Avec deux nombres $a, b \in \mathbb{Z}$.

3.1. $a\mathbb{Z} + b\mathbb{Z}$

Dans la partie précédente, un seul nombre a était donné. On regardait ses multiples et les restes.
Considérons maintenant deux nombres a et b et les additions de tous leurs multiples.

Proposition - Groupe $a\mathbb{Z} + b\mathbb{Z}$
On note, pour tout $a, b \in \mathbb{Z}$,

$$a\mathbb{Z} + b\mathbb{Z} := \{au + bv, (u, v) \in \mathbb{Z}^2\}$$

$a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Démonstration

Analyse - Rappel sur les sous-groupes de $\mathbb{Z}$

Corollaire - $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, alors il existe $d \in \mathbb{N}^*$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Démonstration

Remarque - Mais qui est d ?
C'est la question...

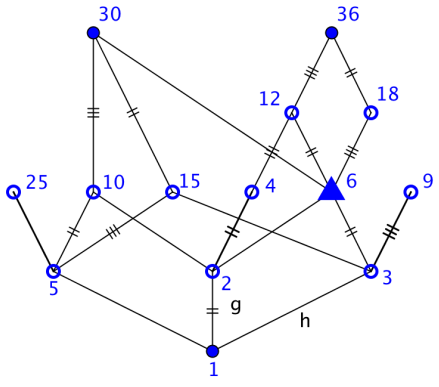
3.2. $PGCD$ des deux nombres a et b. Définition « naturelle »

Il s'agit du plus grand pour la relation d'ordre classique : $\leqslant$.
Analyse - Construction du $PGCD$

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
$$PGCD(a,b) = \max\left(\mathscr{D}(a) \cap \mathscr{D}(b) \cap \mathbb{N}\right).$$
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 - $a = 36$, $b = 30$

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 $a \leqslant b$, mais aussi $a|b$



Remarque - Divisibilité des nombres de $\mathscr{D}(30) \cap \mathscr{D}(36)$
6, *le* $PGCD(36,30)$ *est divisible par tous les éléments de* $\mathscr{D}(30) \cap \mathscr{D}(36)$.
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...

Proposition - $a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z}$. Couple de Bézout
Soit $(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}$. Alors $a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z}$. Et donc il existe $(u,v)\in\mathbb{Z}^2$ tel que $a\wedge b=au+bv$.

Démonstration

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 »

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 :

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

Remarque - Force de cette propriété
Dans l'équivalence trouvée (ou la double inclusion d'ensemble),
une équivalence est triviale : $d|a\wedge b\Longrightarrow d|a$ *et* $d|b$.
L'usage fréquent que l'on fera donc de cette proposition est : $d|a$ *et* $d|b\Longrightarrow d|a\wedge b$.

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 - $\lambda a \wedge \lambda b = \lambda(a \wedge b)$

3.3. Algorithmes

Algorithme des divisions successives pour obtenir le $PGCD$ (Algorithme d'Euclide)

Lemme - Stabilité par division euclidienne
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$.
Si $a = bq + r$, alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(r) \cap \mathscr{D}(b)$ et donc $a \wedge b = b \wedge r$.

Démonstration

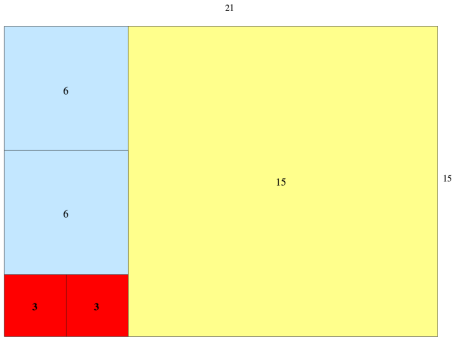
Heuristique - Algorithme pour obtenir le $PGCD$ de deux nombres

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.

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

Proposition - Algorithme d'Euclide

Soient $a, b \in \mathbb{N}^*$. Supposons que $0 < b < a$. L'algorithme d'Euclide consiste en un 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 : $a \wedge b = r_{N-1}$

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 $f : \mathbb{Z}^2 \to E$ (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.

```
def alg_eucl(a,b):
    """pgcd(a,b) par algorithme d'Euclide"""
    if b==0:
        return(a)
    a1,a2=max(abs(a),abs(b)),min(abs(a),abs(b))
    ra,rb=a1,a2
    while rb!=0:
        rc=div_eucl(ra,rb)[1]
        ra,rb=rb,rc
    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 :

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

Mais c'est aussi le cas concernant les nombres irrationnels

Exploitation plus fine de l'algorithme d'Euclide (Couple de Bézout)

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 Bezout, en divisant par $\delta = a \wedge b$:

$$ua + bv = u_0 a + v_0 b \Rightarrow \frac{a}{\delta}(u - u_0) = \frac{b}{\delta}(v_0 - v) \underbrace{\Rightarrow}_{\text{lemme de Gauss}} \frac{a}{\delta} | (v - v_0) \dots$$

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

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



Informatique - Division euclidienne

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

```
def Bezout(a,b):
    """pgcd(a,b)+coefficient de Bezout"""
    if b==0:
        return(a)
    a1,a2=max(abs(a),abs(b)),min(abs(a),abs(b))
    u,uu=1,0
    v,vv=0,1
    ra,rb=a1,a2
    while rb!=0:
        q,rc=div_eucl(ra,rb)
        ra,rb=rb,rc
        u,uu=uu,u-q*uu
        v,vv=vv,v-q*vv
    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 $k\in\mathbb{N}^*$: $r_{k+1}=q_kr_k+q_{k-1}$ et (u_k) et (v_k) vérifient la même relation de récurrence $x_{k+1}=-q_kx_k+x_{k-1}$.

k	r_k	q_k	u_k	v_k	$1542\times u_k+58\times v_k=r_k$
0	1542		1	0	1542
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

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

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

Démonstration

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)!



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

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

Démonstration

Facteur relativement premier

Proposition - Facteur relativement premier
Soient $a, b, c \in \mathbb{Z}$. Alors

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

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

Démonstration

Exercice

On note $\mathscr{P}_a$, 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.

$$(\forall i \in [\![1,n]\!], a \wedge b_i = 1) \Longrightarrow a \wedge \prod_{i=1}^{n} b_i = 1$$

$$(\forall (i,j) \in [\![1,n]\!]^2, i \neq j \Rightarrow b_i \wedge b_j = 1 \text{ et } \forall i \in [\![1,n]\!], b_i | c) \Longrightarrow \prod_{i=1}^{n} b_i \Big| c$$

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 $r = \dfrac{p}{q}$ 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 $r = \dfrac{\lambda p}{\lambda q}$ 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 :

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

nous allons prendre pour définition, la version du générateur du sous-groupe. Dans ce cas le terme « plus grand » ne doit pas être pris pour la relation d'ordre $n \leqslant n$, 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.
- $\forall\, x \in E, \inf E \leqslant x$
- $\forall\, m$ *tel que* $\forall\, x \in E,\ m \leqslant x$, *alors* $m \leqslant \inf E$.

$PGCD(E)$ *est le plus grand des diviseurs de* E.
- $\forall\, x \in E, PGCD(E) \mid x$
- $\forall\, m$ *tel que* $\forall\, x \in E,\ m|x$, *alors* $m|PGCD(E)$.

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

Définition - PGCD de $a_1, a_2, \dots a_n$
Soit $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n \setminus \{(0,0,\dots,0)\}$.
Il existe un unique entier $d \in \mathbb{N}^*$ tel que $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$, on le note $a_1 \wedge a_2 \wedge \cdots \wedge a_n$ ou encore $\bigwedge_{i=1}^{n} a_i$.

Démonstration

Proposition - Récurrence
Soient $n \in \mathbb{N}^*$, $n \geqslant 2$, et $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n \setminus \{(0, \cdots, 0)\}$. Alors, on a :

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

Démonstration

L'identité de Bézout se généralise également :

Proposition - Décomposition de Bézout
Soient $n \in \mathbb{N}^*$, $n \geqslant 2$, et $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n \setminus \{(0, \cdots, 0)\}$.

$$\exists (u_1, \dots, u_n) \in \mathbb{Z}^n \quad ; \quad \bigwedge_{i=1}^{n} a_i = \sum_{i=1}^{n} u_i a_i$$

Démonstration

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

Proposition - Avec l'ensemble des diviseurs
Soient $n \in \mathbb{N}^*$, $n \geqslant 2$, et $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n \setminus \{(0, \cdots, 0)\}$ Pour tout $j \in \mathbb{N}_n$, $\bigwedge_{i=1}^{n} a_i$ est un diviseur de a_j.
Mieux : $\bigwedge_{i=1}^{n} a_i = \max\left(\mathscr{D}(a_1) \cap \mathscr{D}(a_2) \cdots \mathscr{D}(a_k) \cap \mathbb{N}\right)$,
au choix pour max : au sens de la relation d'ordre | ou $\leqslant$.
On a $\mathscr{D}(\bigwedge_{i=1}^{n} a_i) = \bigcap_{j=1}^{n} \mathscr{D}(a_j)$.

Démonstration

Réécriture de la propriété précédente :

Proposition - Critère caractéristique du $PGCD(a_1, a_2, \dots a_k)$
Soient $n \in \mathbb{N}^*$, $n \geqslant 2$, et $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n \setminus \{(0, \cdots, 0)\}$.
$\left(\bigwedge_{i=1}^{n} a_i\right)$ 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

$$\forall m \in \mathbb{Z}, \qquad (\forall i \in [\![1, n]\!],\ m | a_i) \iff m | d.$$

Démonstration

Cela donne bien une caractérisation

Savoir faire - Démonter/utiliser le PGCD de $(a_1, a_2, \dots a_n)$
Tout diviseur du PGCD, divise chaque a_i.
Toute 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 $(xa_1, xa_2, \dots xa_n)$ est $|x| \times \bigwedge_{i=1}^{n} a_i$

Démonstration

5.3. Entiers premiers entre eux dans leur ensemble

Définition - Entiers premiers entre eux dans leur ensemble
Les entiers $a_1, \dots, a_n$ 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 $a =$, $b =$, $c =$
sont
ne sont pas

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

Savoir faire - Réduction à des entiers premiers entre eux (2)
Soient $a_1, a_2, \dots a_n \in \mathbb{Z}$. On note $\delta = \bigwedge_{i=1}^{n} a_i$.
Alors pour tout $i \in [\![1, n]\!]$, $a_i = \delta a_i'$, avec $(a_1', a_2', \dots, a_n')$ premiers entre eux dans leur ensemble.
Puis on travaille avec les a_i'.

Proposition - Théorème (identité) de Bézout
Soient $a_1, \dots, a_n$ des entiers relatifs. Alors

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

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 :

$\exists\, u_1, u_2, \dots u_n \in \mathbb{Z}$ 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 $u_1, u_2, \dots u_n \in \mathbb{Z}$ tels que $\sum_{i=1}^{n} u_i a_i = 1$ 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.
Alors $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Il existe donc $\mu \in \mathbb{Z}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$. On appelle $PPCM$ (Plus Petit Commun Multiple) de a et b, ce nombre μ. On le notera plutôt $a \vee b$.
On a clairement $b \vee a = a \vee b = |a| \vee |b|$.

Démonstration

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 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 $PGCD$
Soient $a, b \in \mathbb{Z}$.
— 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 μ dont les multiples sont exactement les multiples communs à tous les a_i, c'est-à-dire tel que

$$\forall m \in \mathbb{Z}, (\forall i \in [\![1, n]\!],\ a_i | m) \iff \mu | m.$$

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

On a $\bigcap_{i=1}^{n} (a_i \mathbb{Z}) = \left(\bigvee_{i=1}^{k} a_i \right) \mathbb{Z}$

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.

⇝ 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 a divise n

— Savoir-faire - Critère de divisibilité par la division euclidienne
— Truc & Astuce pour le calcul - Réduction modulo n
— Savoir-faire - Combinaisons linéaires (entières)
— Savoir-faire - Trouver un PGCD. Exploiter un PGCD.
— 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 - 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*
$\mathscr{D}(a)$	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.
$a \equiv b[n]$	$n\|(b-a) \iff \exists\, k \in \mathbb{Z}$ 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)	$a \wedge b = \max(\mathscr{D}(a) \cap \mathscr{D}(b))$ $d\|a$ et $d\|b$ 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)	$a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z})$ $a\|m$ et $b\|m$ ssi $a \vee b\|m$	$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$
$\mathscr{P}_a$	Ensemble des nombres premiers avec a	$b \in \mathscr{P}_a \iff a \wedge b = 1$	Equivalent à $a \in \mathscr{P}_b$ (symétrie)

Retour sur les problèmes

67. Oui, on peut tout faire. Sinon, on rajoute le nombre dans les premiers.
68. C'est les congruences.
69. 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 commus de a et de b…
70. Oui cela termine (suite d'entiers naturels, strictement décroissantes). On obtient en dernier reste non nul, le PGCD.
71. 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 $(6 + 10 - 15)$.