UE USSI78 - Outils mathématiques pour l'informatique
Cours 2 - Élements d'arithmétique

Alain Faye

Cnam

2025-2026

Plan du cours

1. Eléments de logique
2. Relations et ordres
3. Éléments d'arithmétique
   - Division euclidienne
   - Nombres premiers
   - PGCD et PPCM
4. Calcul matriciel et analyse
5. Suites et séries

Plan

Plan

Plan

Plan

Éléments d'arithmétique

Division euclidienne

- $\mathbb{N}$ désigne l'ensemble des **entiers naturels**, $\mathbb{Z}$ l'ensemble des **entiers relatifs**, et $\mathbb{N}^*$ l'ensemble des entiers strictement positifs.
- L'**arithmétique** est l'étude de ces ensembles.
- En plus de l'addition, la soustraction et la multiplication, on peut faire une quatrième opération sur les entiers, fondamentale en arithmétique : la **division euclidienne** :

Théorème

Soient a et b des entiers. Si $b \neq 0$, il existe deux entiers q et r vérifiant :

$$a = bq + r \qquad \textit{et} \qquad 0 \leq r < |b|$$

Ils sont les seuls à vérifier ces deux conditions.

- Le calcul de q et r s'appelle la **division euclidienne** de a par b, le nombre q s'appelle le **quotient** de la division et r le **reste**.

Exemple

la division euclidienne de 150 par 11 donne le quotient 13 et le reste 7. La division euclidienne de -80 par 7 donne le quotient -12 et le reste 4.

- Soient a et b deux entiers. On dit que b **divise** a, ou encore que a est un **multiple** de b, ou que b est un **facteur** de a et on écrit $b|a$, s'il existe un entier q tel que $a = bq$.
- En particulier un entier b non nul divise l'entier a si et seulement si le reste de la division euclidienne de a par b est nul.
- Le nombre 0 est son seul multiple.

Théorème

La relation de divisibilité $b \mid a$ est une relation d'ordre sur $\mathbb{N}^*$.

- L'ensemble $\mathbb{N}^*$ est muni de deux relations d'ordre :
  - la relation habituelle, $\leq$,
  - et la relation de divisibilité $|$.
- Comme $b \leq a$ entraîne $(b + c) \leq (a + c)$ nous dirons que la première est **additive** ;
- Nous dirons que la seconde est **multiplicative** car $b|a$ entraîne $bc \mid ac$.
- Ces deux relations ne sont pas indépendantes : si $b \mid a$, alors $b \leq a$. (La réciproque est bien sûr fausse).
- *Exercice* : tracer le diagramme de Hasse de $\mathbb{N}_6^*$ ordonné par la relation additive et par la relation multiplicative.

Théorème

Si $c \mid a$ *et* $c \mid b$ *alors tout nombre de la forme* $ua + vb$ *avec* u *et* v *dans* $\mathbb{Z}$ *est divisible par* c*. En particulier* c *divise* $a + b$ *et* $a - b$*.*

Plan

- Un élément de $\mathbb{N}^*$, strictement supérieur à 1, qui n'a pour diviseurs dans $\mathbb{N}^*$ que 1 et lui-même, s'appelle un **nombre premier**.
- En d'autres termes, un nombre premier est un élément minimal dans l'ensemble $\mathbb{N}^*$ privé de 1, ordonné par la relation de divisibilité.
- Sur le diagramme de Hasse de $\mathbb{N}^*$ les nombres premiers sont les éléments qui se trouvent immédiatement après 1.

Exemple

Les 25 nombres premiers inférieurs à 100 sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

- Un entier qui n'est pas un nombre premier est un nombre **composé**.

Théorème

Si n est un entier strictement supérieur à 1, son plus petit diviseur strictement supérieur à 1 est un nombre premier.

- La liste des diviseurs d'un nombre n, ordonnée par la relation $\leq$, commence par 1 et finit par n.
- Le deuxième élément de cette liste est toujours un nombre premier.
- ***Exercice*** : Dresser les listes ordonnées des diviseurs de 1, 5, 18, 100. Remarquez (puis expliquez) une certaine forme de symétrie sur ces exemples.

Théorème

Dans la liste ordonnée des diviseurs de n le produit de deux diviseurs placés symétriquement par rapport au milieu de la liste est égal à n.

Théorème

Un entier $n \geq 4$ qui n'est divisible par aucun entier compris entre 2 et $\sqrt{n}$ est premier.

$\rightarrow$ crible d'Eratosthène : algo. pour trouver les nombres premiers $\leq n$.

Théorème

Tout élément de $\mathbb{N}^*$ supérieur ou égal à 2 est soit un nombre premier, soit un produit de nombre premiers.

Éléments d'arithmétique

Nombres premiers

- Ce dernier théorème signifie qu'en multipliant ensemble les puissances des nombres premiers on obtient tous les nombres entiers supérieurs ou égaux à 2.
- Nous verrons plus loin qu'à condition de ne pas tenir compte de l'ordre des facteurs, il existe une seule façon d'écrire un entier comme produit de nombres premiers.
- Les nombres premiers sont des atomes et les entiers sont des molécules : toutes les molécules sont fabriquées avec ces atomes et une molécule donnée a une composition parfaitement définie. Le calcul des nombres premiers dont le produit est égal à n est appelé la **décomposition en facteurs premiers** de n, et le résultat de ce calcul la **factorisation** de n.

Méthode pour décomposer un nombre en facteurs premiers

1. Déterminer le plus petit diviseur de n autre que 1 ; c'est le plus petit facteur de n.
2. Diviser n par ce facteur premier, ce qui donne m pour quotient.
3. Si $m > 1$ recommencer à partir du 1. en remplaçant n par m.

- ***Exercice*** : décomposer 2200 en facteurs premiers.

Méthode pour décomposer un nombre en facteurs premiers

1. Déterminer le plus petit diviseur de n autre que 1 ; c'est le plus petit facteur de n.
2. Diviser n par ce facteur premier, ce qui donne m pour quotient.
3. Si $m > 1$ recommencer à partir du 1. en remplaçant n par m.

- ***Exercice*** : décomposer 2200 en facteurs premiers. (Résultat : $2200 = 2^3.5^2.11$)
- Cette méthode s'applique sans difficulté aux entiers pas très grands.
- Par contre, quand un entier est "grand", la recherche de son plus petit facteur premier n'est pas une chose facile.
- C'est cette difficulté qui est utilisée comme rempart dans certaines méthodes de cryptographie.

Théorème

Il existe une infinité de nombres premiers

- Soient $p_1,\ p_2,\dots,p_k$ des nombres premiers et n leur produit.
- Aucun des p_i ne peut diviser $(n+1)$ car un nombre qui divise à la fois n et $(n+1)$, divise leur différence qui vaut 1 (or le seul diviseur de 1 est 1 lui-même).
- Par conséquent, les diviseurs premiers de $(n+1)$ sont tous différents des p_i et la factorisation de ce nombre fournit de nouveaux nombres premiers.
- Nous avons donc un procédé qui permet de rajouter à tout ensemble fini de nombres premiers des nombres premiers qui n'y étaient pas, ce qui fait que l'ensemble des nombres premiers ne peut pas être fini.

Exemple

Voyons quels nombres premiers sont obtenus quand on suit cette méthode. Au départ, 2 est le seul nombre premier connu. À chaque étape, on factorise $M = p_1 p_2 \ldots p_k + 1$*, et on ajoute ses facteurs premiers à l'ensemble des nombres premiers précédemment connus. Puis on recommence avec la nouvelle liste de nombres premiers.*

Plan

- Soient a et b deux éléments de $\mathbb{N}^*$. Les éléments de $\mathbb{N}^*$ qui divisent à la fois a et b sont tous compris entre 1 et le plus petit des deux nombres a et b. Ils forment donc un ensemble fini.
- Comme cet ensemble n'est pas vide, puisqu'il contient 1, il possède un plus grand élément pour la relation $\leq$. Nous l'appelerons le **plus grand commun diviseur** de a et b, en abrégé **PGCD** de a et b, et nous le noterons $a \wedge b$
- Quand deux nombres entiers ont leur PGCD égal à 1 on dit qu'ils sont **premiers entre eux**.
- On décide aussi que le PGCD de deux éléments non nuls de $\mathbb{Z}$ est le PGCD de leurs valeurs absolues et que $a \wedge 0 = 0$

Exemple

Calculer $36 \wedge 90$ *en utilisant uniquement la définition.*

(Au passage, remarquons que l'ensemble des diviseurs communs à 36 et 90 coïncide avec l'ensemble des diviseurs de 18, leur PGCD. C'est un fait général, nous y reviendrons).

Propriétés du PGCD

- $a \wedge b = b \wedge a$
- $a \wedge 1 = 1$
- $a \wedge a = a$
- $a \wedge b = b \iff b \mid a$
- si p est premier, $a \wedge p = \begin{cases} p & \text{quand} \quad p \mid a \\ 1 & \text{quand} \quad p \nmid a \end{cases}$
- si p et q sont premiers, $p \wedge q = \begin{cases} p & \text{quand} \quad p = q \\ 1 & \text{quand} \quad p \neq q \end{cases}$

Méthode pratique pour calculer $a \wedge b$ par l'algorithme d'Euclide

1. Ranger a et b de façon que $a \geq b$ et poser $r_{-1} = a$ et $r_0 = b$.
2. Faire les divisions euclidiennes jusqu'au moment où l'on trouve un reste nul :

$$\begin{array}{lcll}
r_{-1} & = & r_0 q_1 & + \; r_1 \\
r_0 & = & r_1 q_2 & + \; r_2 \\
r_1 & = & r_2 q_3 & + \; r_3 \\
 & & \vdots & \\
r_k & = & r_{k+1} q_{k+2} & + \; r_{k+2} \\
 & & \vdots & \\
r_{n-2} & = & r_{n-1} q_n & + \; \mathrm{r_n} \\
r_{n-1} & = & r_n q_{n+1} & + \; 0
\end{array}$$

3. Le dernier reste non nul, $\mathrm{r_n}$, est le PGCD de a et b et r_n divise chacun des r_k.

PGCD

Algorithme d'Euclide – Remarques

- D'abord, le calcul s'arrête toujours car $r_0 > r_1 > r_2 > r_3 > \ldots \geq 0$ et on finit forcément par rencontrer un reste nul.
- Soit c un diviseur commun à a et b. D'après un précédent théorème, il divise $r_{-1} - r_0 q_1$, c'est-à-dire r_1.
- De même, il divise $r_0 - r_1 q_2$ qui n'est autre que r_2.
- En descendant les équations, on montre que c divise tous les restes jusqu'à r_n. Et donc $c \leq r_n$.
- En sens inverse, la dernière équation montre que r_n divise r_{n-1}. L'avant dernière équation montre qu'il divise r_{n-2} et de proche en proche, en remontant les équations, on montre que r_n divise a et b.
- On montre ainsi que r_n est un diviseur commun à a et b et que tout diviseur commun à a et b divise r_n. Par conséquent r_n est le PGCD de a et b.

Exemple

Calculer le PGCD de 791 et 336 par l'algorithme d'Euclide.

Exemple

Calculer le PGCD de 791 et 336 par l'algorithme d'Euclide.

$791 = 2 \times 336 + 119$
$336 = 2 \times 119 + 98$
$119 = 1 \times 98 + 21$
$98 = 4 \times 21 + 14$
$21 = 1 \times 14 + 7$
$14 = 2 \times 7 + 0$
(Résultat : $791 \wedge 336 = 7$)

PGCD

Algorithme d'Euclide – Exemple (suite)

Exemple

En remontant l'algorithme d'Euclide, mettre le PGCD de 791 et 336 sous la forme $u \times 791 + v \times 336$ *avec* u, v *entiers.*

PGCD

Algorithme d'Euclide – Exemple (suite)

Exemple

En remontant l'algorithme d'Euclide, mettre le PGCD de 791 et 336 sous la forme $u \times 791 + v \times 336$ *avec* u, v *entiers.*

$791 = 2 \times 336 + 119$
$336 = 2 \times 119 + 98$
$119 = 1 \times 98 + 21$
$98 = 4 \times 21 + 14$
$21 = 1 \times 14 + 7$
$14 = 2 \times 7 + 0$
On remonte l'algorithme : $7 = 21 - 1 \times 14$
$7 = 21 - 1 \times (98 - 4 \times 21) = -98 + 5 \times 21$
$7 = -98 + 5 \times (119 - 1 \times 98) = 5 \times 119 - 6 \times 98$
$7 = 5 \times 119 - 6 \times (336 - 2 \times 119) = -6 \times 336 + 17 \times 119$
$7 = -6 \times 336 + 17 \times (791 - 2 \times 336) = 17 \times 791 - 40 \times 336$
Ainsi, on voit que tout diviseur de 791 et 336 divise leur PGCD.

Théorème

Les diviseurs communs à deux nombres sont tous les diviseurs de leur PGCD.

(Autrement dit, pour la relation d'ordre multiplicative, l'ensemble des minorants communs à a et b possède un plus grand élément : $a \wedge b$

PGCD

Propriétés (2)

Théorème

Soient a, b et c trois éléments de $\mathbb{N}^*$.

1. *La multiplication est distributive par rapport au PGCD :*

$$c(a \wedge b) = ca \wedge cb$$

2. *Si c est un diviseur commun à a et b alors :*

$$\left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = \frac{a \wedge b}{c}$$

3. *Si c est un diviseur commun à a et b, pour que $c = a \wedge b$, il faut et il suffit que $\left(\frac{a}{c}\right) \wedge \left(\frac{b}{c}\right) = 1$*

PPCM

- Soient $a_1, a_2, ..., a_n$ des éléments de $\mathbb{N}^*$.
- L'ensemble de leurs **multiples communs** n'est pas vide puisqu'il contient leur produit $a_1 \times a_2 \times ... \times a_n$.
- Il a donc un plus petit élément, qu'on appelle le **plus petit commun multiple** de $a_1, a_2, ..., a_n$, et qu'on note $a_1 \vee a_2 \vee ... \vee a_n$ ou encore $PPCM(a_1, a_2, ..., a_n)$.

Théorème

Le PGCD et le PPCM de deux nombres sont liés par : $ab = (a \vee b)(a \wedge b)$

- On peut donc calculer le PPCM de deux nombres à partir de leur PGCD.

Plan

Plan