Arithmétique

Terminale S - Spé

N.Daval

Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple (q, r) tel que $a = bq + r$ avec $0 \leq r < b$

Vocabulaire : a est le dividende ; b le diviseur ; q le quotient et r le reste

Divisibilité dans $\mathbb{Z}$

a divise b

$\iff$ b multiple de a

$\iff$ il existe $k \in \mathbb{Z}$ tel que $b = ka$

- Notation : a/b
- Réflexivité : a/a
- Transitivité : $\left\{ \begin{array}{l} a/b \\ b/c \end{array} \right. \implies a/c$
- Linéarité : $\left\{ \begin{array}{l} a/b \\ a/c \end{array} \right. \implies a/bu + cv$
- Lien avec les congruences : $a/b \iff b \equiv 0(a)$
- Lien avec le PGCD : $a/b \iff PGCD(a, b) = a$

Congruence dans $\mathbb{Z}$

a et b ont même reste dans la division euclidienne par n

$\iff$ a est congru à b modulo n

$\iff$ $a - b$ est multiple de n

- Notation : $a \equiv b\,(n)$
- Réflexivité : $a \equiv a\,(n)$
- Symétrie : $a \equiv b\,(n) \implies b \equiv a\,(n)$
- Transitivité : $\left\{ \begin{array}{l} a \equiv b\,(n) \\ b \equiv c\,(n) \end{array} \right. \implies a \equiv c\,(n)$
- Addition : $\left\{ \begin{array}{l} a \equiv b\,(n) \\ a' \equiv b'\,(n) \end{array} \right. \implies a + a' \equiv b + b'\,(n)$
- Multiplication : $\left\{ \begin{array}{l} a \equiv b\,(n) \\ a' \equiv b'\,(n) \end{array} \right. \implies aa' \equiv bb'\,(n)$
- Puissance : $a \equiv b\,(n) \implies a^k \equiv b^k\,(n)$

Nombres premiers

Un entier p supérieur ou égal à 2 est premier si et seulement si il admet exactement deux diviseurs : 1 et lui-même

Théorème fondamental de l'arithmétique : tout entier naturel supérieur ou égal à 2 se décompose de manière unique à l'ordre des facteurs près en produit de facteurs premiers : on note $p = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$

Critère d'arrêt : si n n'admet pas de diviseur premier p tel que $2 \leq p \leq \sqrt{n}$ alors n est premier

PGCD, PPCM

L'ensemble des diviseurs communs à a et b admet un plus grand élément noté PGCD(a, b)

L'ensemble des multiples communs à a et b admet un plus petit élément noté PPCM(a, b)

- Si $\left\{ \begin{array}{l} a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \\ b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} \end{array} \right.$ alors $\left\{ \begin{array}{l} \text{PGCD}(a, b) = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} \\ \text{PPCM}(a, b) = p_1^{M_1} p_2^{M_2} \dots p_n^{M_n} \end{array} \right.$ où $m_i = \min(\alpha_i, \beta_i)$ et $M_i = \max(\alpha_i, \beta_i)$
- PGCD$(ka, kb) = k$PGCD(a, b)
- Si $a = bq + r$, alors PGCD$(a, b) =$ PGCD(b, r)
- Le PGCD de deux nombres non nuls est le dernier reste non nul de la suite des divisions de l'algorithme d'Euclide

Théorème de Bézout

- PGCD$(a, b) = 1$

  $\iff$ a et b sont premiers entre eux

  $\iff$ il existe deux entiers u et v tels que $au + bv = 1$
- Identité de Bézout : PGCD$(a, b) = d$

  $\implies$ il existe deux entiers u et v tels que $au + bv = d$
- Corollaire de Bézout : l'équation $ax + by = c$ admet des solutions entiers $\iff$ c est multiple de PGCD(a, b)

Théorème de Gauss

$\left\{ \begin{array}{l} a/bc \\ \text{PGCD}(a, b) = 1 \end{array} \right. \implies a/c$

Corollaires :

- $\left\{ \begin{array}{l} a/c \text{ et } b/c \\ \text{PGCD}(a, b) = 1 \end{array} \right. \implies ab/c$
- $\left\{ \begin{array}{l} p \text{ premier} \\ p/ab \end{array} \right. \implies p/a \text{ ou } p/b$

Matrices et suites

Terminale S - Spé

N. Daval

Vocabulaire des matrices

matrice $m \times n$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

matrice ligne

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

matrice colonne

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$$

matrice diagonale

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}$$

matrice unité

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

$A = (a_{ij})$: matrice de coefficients a_{ij} (ligne i, colonne j) $\quad$ $m = n$: matrice carrée d'ordre n $\quad$ matrice unité : I_n ou I

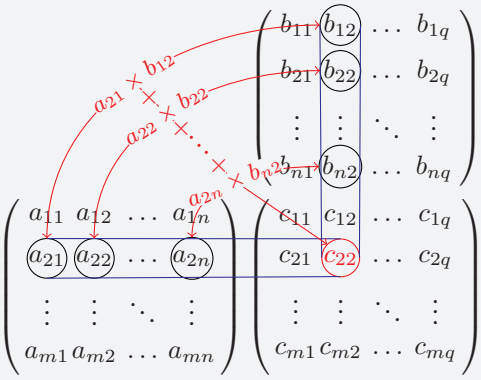
Opérations avec des matrices

$A = (a_{ij})$ est une matrice de dimension $m \times n$

$B = (b_{ij})$ est une matrice de dimension $p \times q$

Pour tout $1 \leq i \leq m$ et $1 \leq j \leq n$:

- $A = B \iff m = p$; $n = q$ et $a_{ij} = b_{ij}$
- $C = A + B$ avec $m = p$ et $n = q$: $c_{ij} = a_{ij} + b_{ij}$
- $C = kA$: $c_{ij} = ka_{ij}$
- $C = A \times B$: $c_{ij} =$ ligne $i_{|A} \times$ colonne $j_{|B}$
- $A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ fois}}$ si $n \neq 0$ et $A^0 = I$



$$(kA)B = k(AB)$$
$$ABC = (AB)C = A(BC)$$
$$A(B + C) = AB + BC$$
$$(A + B)C = AC + BC$$
$$AI = IA = A$$

⚠ en général : $AB \neq BA$

Inverse d'une matrice

- A matrice carrée inversible $\iff$ il existe B tel que $AB = BA = I$
  Notation : $B = A^{-1}$
- $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ inversible $\iff$ $\det(A) = ad - bc \neq 0$

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Résolution d'un système linéaire

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \qquad\qquad\quad = \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{cases} \iff \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{X} = \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}}_{B}$$

- Écriture : $AX = B$
- Condition de solution (unique) : A inversible
- Solution : $X = A^{-1}B$

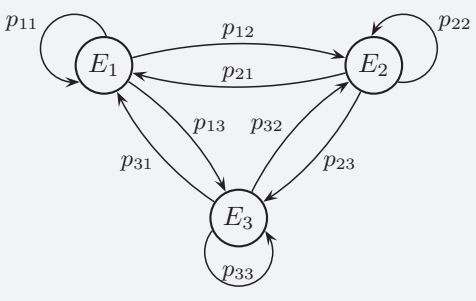
Marche aléatoire

Un système qui a n états possibles $E_1, E_2, \ldots E_n$ qui évolue de l'un à l'autre par étapes successives aléatoires suit une marche aléatoire à n états

On note P_n la matrice ligne associée à la marche aléatoire à l'instant n

$P_n = (P(X_n = E_1)\ P(X_n = E_2)\ \ldots\ P(X_n = E_n))$

graphe probabiliste



matrice de transition

$$T = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix}$$

avec : $0 \leq p_{ij} \leq 1$ et

$p_{11} + p_{12} + p_{13} = 1$

$p_{21} + p_{22} + p_{23} = 1$

$p_{31} + p_{32} + p_{33} = 1$

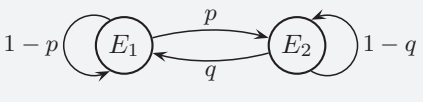
- $P_{n+1} = P_n \times T$ et $P_n = P_0 \times T^n$
- Un état probabiliste P est stable $\iff$ $P \times T = P$

Suites $U_{n+1} = AU_n$

Une suite de matrices converge $\iff$ toutes les suites formant les éléments de cette matrice converge

- Si $U_{n+1} = AU_n$ alors $U_n = A^nU_0$

Cas particulier de deux états



$$T = \begin{pmatrix} 1 - p & p \\ q & 1 - q \end{pmatrix}$$

Si $(p; q) \neq (0; 0)$ et $(p; q) \neq (1; 1)$ alors P_n converge