

MATH-F307 - Mathématiques Discrètes
Laurent LA FUENTE
Notes de cours

André MADEIRA CORTES
Nikita MARCHANT

Table des matières

1	Théorie des Graphes	3
1.1	Définitions	3
1.2	Chemins dans les graphes	4
1.3	Arbres	5
1.3.1	Définitions	5
1.3.2	Arbres couvrants et arbres à poids	6
1.4	Isomorphisme	6
1.5	Graphes hamiltoniens	7
1.6	Graphes Eulériens	10
1.7	Application : le problème du voyageur de commerce (TSP)	11
1.7.1	Énoncé du problème	11
1.7.2	Arbres couvrant minimum	12
1.8	Ordres partiels	13
2	Arithmétique Modulaire	17
2.1	Les entiers et la division euclidienne	17
2.1.1	L'algorithme d'Euclide	18
2.2	Groupes, anneaux et entiers modulo n	19
2.2.1	Définitions	19
2.2.2	Groupes quotients	20
2.2.3	Isomorphismes de groupe	21
2.2.4	Les anneaux	21
2.2.5	Relation de congruence	21
2.3	Cryptologie : Le système RSA	23
2.3.1	Fonctionnement des clés de chiffrement RSA	23
3	Suite	25

1 Théorie des Graphes

1.1 Définitions

Définition 1

Un graphe Γ est un triplet (V, E, γ) où V est un ensemble fini dont les éléments sont appelés sommets, E est un ensemble fini dont les éléments sont appelés arêtes, γ est une fonction $\gamma : E \rightarrow \text{Paires}(V)$. On notera le plus souvent $\Gamma = (V, E)$ en omettant la fonction γ .

Soit $\gamma(e) = \{x, y\}$ pour $e \in E, x, y \in V$:

1. On dit que x et y sont adjacents.
2. On dit que e est incidente à x et y .

Définition 2

Soit $\Gamma = (V, E, \gamma)$ un graphe.

1. $\gamma(e) = \{x, x\}$ pour $e \in E, x \in V$ est appelé un lacet.
2. Si au moins 2 arêtes sont incidentes à 2 mêmes sommets, on les appelle arêtes multiples.
3. Un graphe est simple s'il n'a ni lacet, ni arêtes multiples. Dans ce cas, on omet la fonction γ , on note $\Gamma = (V, E)$ et E est identifié un sous-ensemble de $\text{Paires}(V)$.

Définition 3

Soit $\Gamma = (V, E)$ un graphe. Le degré d'un sommet $v \in V$ est le nombre d'arêtes incidentes à v , les lacets comptant pour 2 arêtes. On note le degré de v par $\deg(v)$.

Exemple

Dans la figure suivante, nous avons 2 sommets de degré 4 et 6 sommets de degré 1.

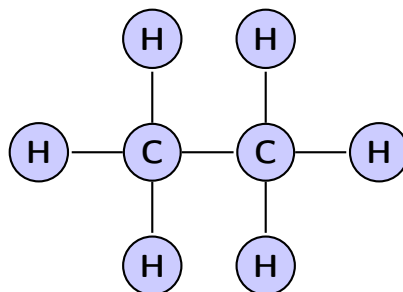


FIGURE 1 – Exemple degrés des sommets dans la molécule C_2H_6 .

Théorème 1

Soit $\Gamma = (V, E)$, alors

$$\sum_{i=1}^{\#V} \deg(v_i) = 2\#E$$

Démonstration

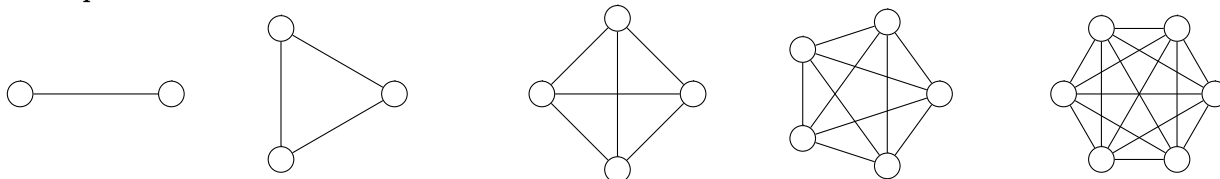
Chaque arête contribue 2 fois dans la somme des degrés.

Corollaire

La somme des degrés des sommets d'un graphe est paire.

Définition 4

Le graphe complet K_n est le graphe simple à n sommets pour lequel chaque paire de sommets est une arête.

Exemple**Définition 5**

Un graphe $\Gamma' = (U, F)$ est un sous-graphe de $\Gamma = (V, E)$ si $U \subseteq V$ et $F \subseteq E$. On notera $\Gamma' \leq \Gamma$.

Exemple

$K_m \leq K_n$ si $m \leq n$.

Exercice

Montrer que K_m possède $q = \frac{1}{2}n(n-1)$ arêtes.

1.2 Chemins dans les graphes**Définition 6**

Soit $\Gamma = (V, E)$ et $v, w \in V$. Un chemin de v à w de longueur n est une séquence alternée de $(n+1)$ sommets v_0, v_1, \dots, v_n et de n arêtes e_1, e_2, \dots, e_n de la forme

$$(v_0, e_1, v_1, e_2, \dots, e_n, v_n)$$

dans laquelle chaque e_i est incident à v_{i-1} et v_i pour $1 \leq i \leq n$ et $e_i \neq e_j, \forall i \neq j \in 1, \dots, n$

Un chemin est simple si aucun sommet ne se répète sauf peut-être v_0 et v_n .

Dans un graphe simple on notera juste la suite des sommets lorsque l'on décrit un chemin.

Définition 7

Un graphe $\Gamma = (V, E)$ est connexe si $\forall x, y \in V : \exists$ un chemin de x à y .

La composante connexe de Γ contenant x est le sous-graphe Γ' de Γ dont les sommets et les arêtes sont contenus dans un chemin de Γ démarrant en x .

Définition 8

Soit $\Gamma = (V, E)$ et $v \in V$.

Un cycle est un chemin de v à v .

Un cycle simple est un cycle de v à v dans lequel aucun sommet n'est répété (mis à part le départ et l'arrivée).

1.3 Arbres

1.3.1 Définitions

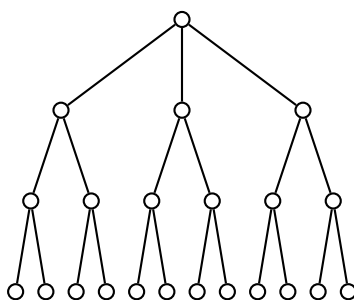
Définition 9

Un arbre est un graphe simple connexe qui ne contient aucun cycle.

Définition 10

Dans un arbre, les sommets de degré 1 sont appelés les feuilles.

Exemple



Proposition 1

Si T est un arbre avec $p \geq 2$ sommets, alors T contient au moins 2 feuilles.

Démonstration

T a p sommets. Tous les chemins sont de longueur inférieure ou égale à p . Considérons un chemin v_0, v_1, \dots, v_r pour $v_i \in V$, $i = 0, \dots, r$ de longueur maximale. Alors, v_0 et v_r sont de degré 1.

Théorème 2 (ATTENTION! Ce théorème et sa démonstration font partie de ceux à connaître par coeur à l'examen! (pour l'année 2015-2016))

Soit T un graphe simple à p sommets. Alors les 3 assertions suivantes sont équivalentes :

- i T est un arbre.
- ii T a $(p - 1)$ arêtes et aucun cycle.
- iii T a $(p - 1)$ arêtes et est connexe.

Démonstration

(i) \Rightarrow (ii) : **Montrer qu'un arbre à p sommets a $(p-1)$ arêtes.**

Par récurrence :

1. $p = 1$ OK
2. Supposons que ce soit vrai pour tout arbre à $k \geq 1$ sommets et montrons le pour un arbre à $(k+1)$ sommets. Soit T un tel arbre, il a au moins 2 feuilles (par Proposition 1). Enlevons une de ces feuilles ainsi que l'arête incidente. On obtient un arbre T' à k sommets. Par l'hypothèse de récurrence : T' a $(k-1)$ arêtes, donc T a k arêtes.

(ii) \Rightarrow (iii) : **Supposons (ii) et T ne soit pas connexe.**

Notons T_1, T_2, \dots, T_t les composantes connexes de T avec $t \geq 2$. Chaque T_i est un arbre, pour $1 \leq i \leq t$ (car pas de cycle). Soit p_i le nombre de sommets de T_i , alors chaque T_i a $(p_i - 1)$ arêtes.

$$\sum_{i=1}^t p_i = p$$

et

donc $\Rightarrow t = 1$

$$p - 1 = \sum_{i=1}^t (p_i - 1) = p - t$$

(iii) \Rightarrow (i) : *Supposons que T ne soit pas un arbre.*

Alors, T contient un cycle C . Enlevons une arête de C . On obtient le sous-graphe T' de T qui est toujours connexe. Si T' contient un cycle, alors on itère le processus. Sinon, T' est un arbre à p sommets qui a strictement moins que $(p-1)$ arêtes.

1.3.2 Arbres couvrants et arbres à poids

Définition 11

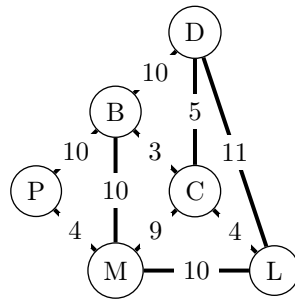
Un arbre couvrant dans un graphe Γ est un arbre qui est un sous-graphe de Γ et qui contient tous les sommets de Γ .

Dans certains problèmes, certaines arêtes sont plus importantes que d'autres. En théorie des graphes, on modélise cela en assignant une valeur à chaque arête.

Définition 12

Un arbre à poids est un couple (Γ, w) où Γ est un arbre w est une fonction $w : E \rightarrow \mathbb{R}^+$. Le nombre $w(e)$ est appelé le poids de l'arête e .

Exemple



1.4 Isomorphisme

Définition 13

Deux graphes $\Gamma_1 = (V_1, E_1, \gamma_1)$ et $\Gamma_2 = (V_2, E_2, \gamma_2)$ sont isomorphes s'il existe une bijection $f : V_1 \rightarrow V_2$ et une bijection $g : E_1 \rightarrow E_2$ telles que $\forall e \in E_1 : e$ est incident à $v, w \in V_1$ ssi $g(e)$ est incident à $f(v), f(w) \in V_2$. Le couple (f, g) est appelé un isomorphisme de graphe et on note $\Gamma_1 \cong \Gamma_2$.

Deux graphes isomorphes ont les mêmes propriétés.

Exemple

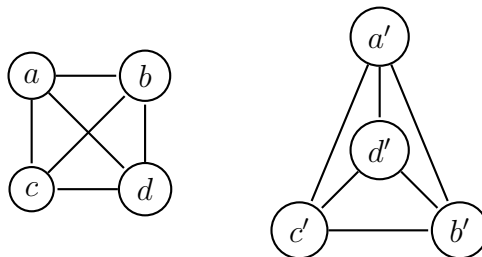


FIGURE 2 – Deux graphes isomorphes

1.5 Graphes hamiltoniens

Hamilton propose le problème suivant : Considérons le graphe du dodécaèdre. Est-il possible, en partant d'un des vingt sommets et en suivant les arêtes du graphe, de visiter tous les sommets une et une seule fois et de revenir au sommet de départ ?

L'exemple suivant montre un chemin qui réponds à ce problème.

Exemple

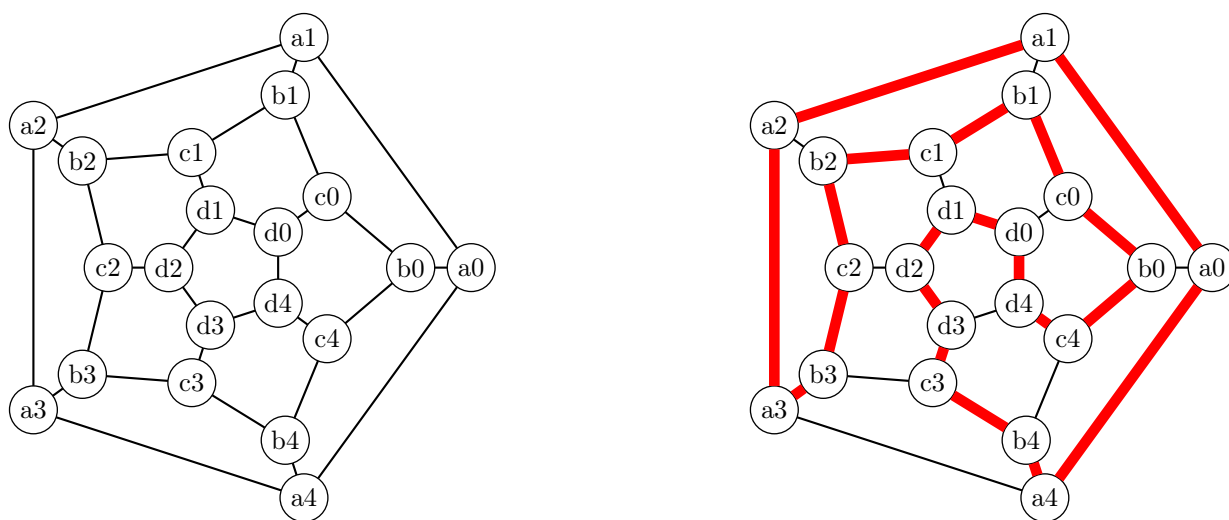


FIGURE 3 – Graphe hamiltonien et cycle hamiltonien

Définition 14

Un cycle hamiltonien dans un graphe Γ est un cycle simple contenant tous les sommets de Γ .

Pour donner un exemple de graphe non-hamiltonien on introduit la notion de graphe biparti.

Définition 15

Un graphe $\Gamma = (V, E)$ est biparti si on peut écrire $V = B \cup W$ avec $B \cap W = \emptyset$ et toute arête de Γ joint un sommet dans B à un sommet dans W .

Exemple

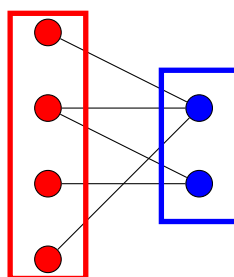


FIGURE 4 – B en rouge, W en bleu

Lemme

Si Γ est biparti, alors Γ ne contient pas de cycle simple de longueur impaire.

Théorème 3

Un graphe biparti avec un nombre impair de sommets n'est pas hamiltonien.

Démonstration

Pour être hamiltonien, il doit admettre un cycle simple passant par tous ses sommets, donc de longueur impaire. Ce n'est pas possible à cause du Lemme précédent.

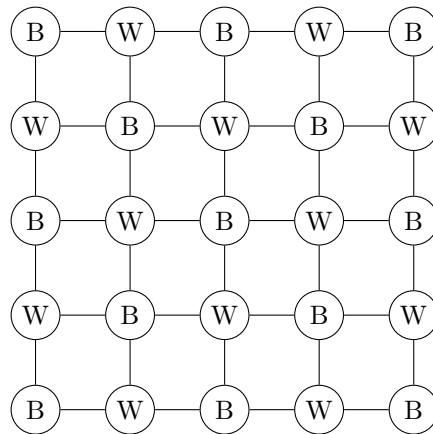
Exemple

FIGURE 5 – Graphe biparti mais non hamiltonien.

Théorème 4 (Dirac 1950)

Soit $\Gamma = (V, E)$ un graphe simple avec $p \geq 3$ sommets. Si $\forall v \in V : \deg(v) \geq \frac{1}{2}p$, alors Γ est Hamiltonien.

Démonstration

Γ est connexe. Soit $C = (v_0, v_1, \dots, v_k)$ un plus long chemin simple dans Γ avec $v_0 \neq v_k, k < p$.

$\deg(v_0) \geq \frac{p}{2}$, tous les sommets adjacents à v_0 sont dans $\{v_1, \dots, v_k\}$

$\deg(v_k) \geq \frac{p}{2}$, tous les sommets adjacents à v_k sont dans $\{v_0, \dots, v_{k-1}\}$

Comme $k < p$, il doit exister $i \in \{0, \dots, k-1\}$ tel que $\{v_i, v_k\} \in E$ et $\{v_0, v_{i+1}\} \in E$.

On obtient un cycle $\tilde{C} = (v_0, v_1, \dots, v_i, v_k, v_{k-1}, \dots, v_{i+1}, v_0)$

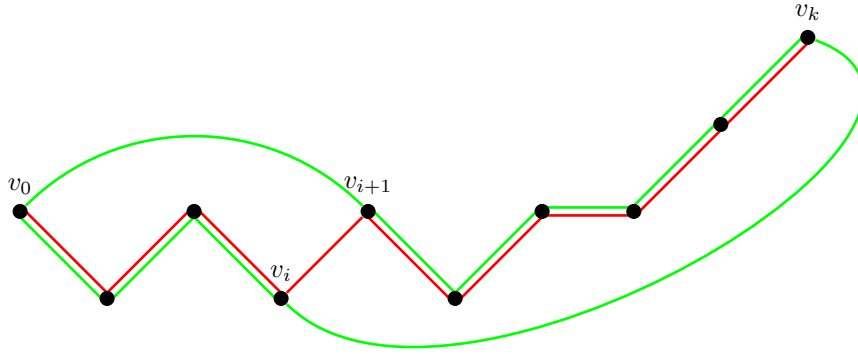


FIGURE 6 – Les 2 chemins, C en rouge, \tilde{C} en vert.

On note que \tilde{C} est un cycle Hamiltonien.

Supposons :

$\exists y \in \tilde{C} \Rightarrow$ On peut supposer que $\{v_j, y\} \in E$ pour $j = \{0, \dots, k\}$.

\Rightarrow On construit un chemin $\overline{C} = (y, v_j, v_{j-1}, \dots, v_0, v_{i+1}, \dots, v_k, v_i, v_{i-1}, \dots, v_{j-1})$. \overline{C} est un chemin plus long que C .

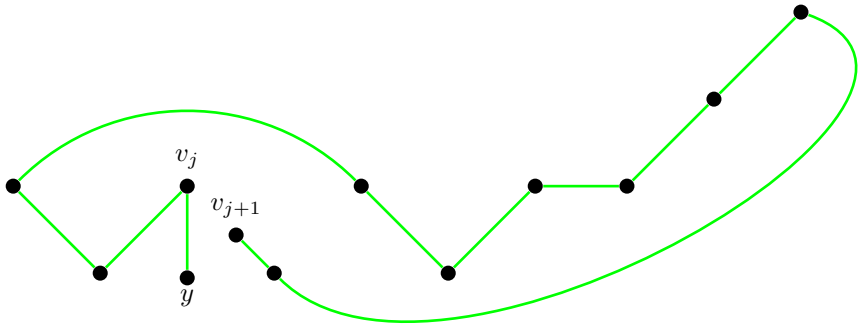


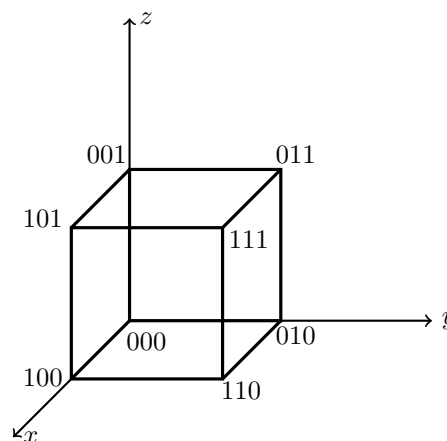
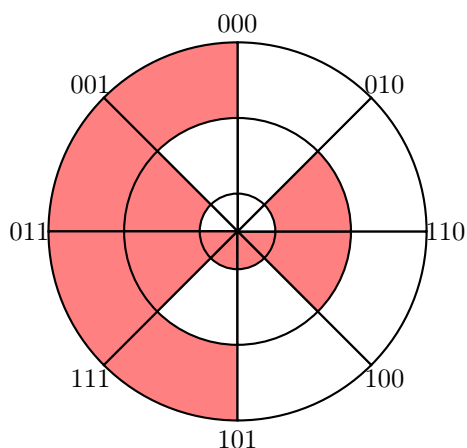
FIGURE 7 – Chemin \overline{C}

Illustration : Code de Gray

Un code de Gray d'ordre n est un arrangement cyclique de 2^n mots binaires de longueur n tels que 2 mots adjacents ne diffèrent qu'en une seule position.

Exemple

Le code de Gray ci-dessous provient d'un cycle hamiltonien sur le graphe du cube :



Un code de Gray d'ordre $(n+1)$ se construit à partir d'un code de Gray d'ordre n comme suit :

1. On écrit le code de Gray donné d'ordre n en ajoutant à la fin de chaque mot un zéro.
2. On le fait suivre par le même code de Gray parcouru dans l'autre sens et en ajoutant à la fin de chaque mot un 1.

1.6 Graphes Eulériens**Définition 16**

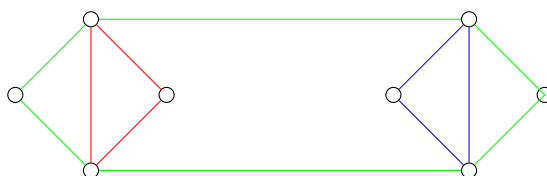
Un cycle Eulérien dans un graphe Γ est un cycle qui contient toutes les arêtes de Γ . Un graphe est Eulérien s'il contient un cycle Eulérien.

Proposition 2

Si un graphe est Eulérien, alors tous ses sommets sont de degré pair.

Lemme

Soit Γ un graphe dans lequel chaque sommet est de degré pair, alors l'ensemble E se partitionne en une union de cycles (arête-)disjointe.

Exemple

Démonstration

Par récurrence, sur le nombre d'arêtes

1. Le lemme est vrai pour $q = 2$.
2. Supposons qu'il soit vrai pour tout graphe à $q \leq k$ arêtes et montrons-le pour un graphe à $(k+1)$ arêtes.
3. Soit v_0 un sommet de Γ . On démarre un chemin en v_0 et on le suit jusqu'à ce qu'un sommet soit répété 2 fois. On le note v_j et C le cycle de v_0 à v_j .
4. Soit Γ' le sous-graphe de Γ , obtenu par $V = V'$ et $E' = E \setminus C$. Γ' a $\#E' \leq k$ arêtes. Par hypothèse de récurrence, les arêtes de Γ' se partitionnent en une union arête-disjointe de cycles $C_1 \cup C_2 \cup \dots \cup C_n$.
5. Donc, $C_1 \cup C_2 \cup \dots \cup C_n$ est une partition arête-disjointe des arêtes de Γ .

Théorème 5 (ATTENTION! Ce théorème et sa démonstration ainsi que le lemme et la proposition utilisés dans la démonstration font partie de ceux à connaître par coeur à l'examen! (pour l'année 2015-2016))

Soit Γ un graphe connexe. Alors, Γ est eulérien si et seulement si chaque sommet a un degré pair.

Démonstration

\Rightarrow OK par proposition précédente.

\Leftarrow Par le Lemme : E se partitionne en une union (arête-)disjointe de cycles $C_1 \cup C_2 \cup \dots \cup C_n$.

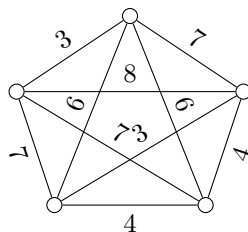
1. Si $n=1$, c'est bon.
2. Si $n > 1$, comme Γ est connexe, \exists une arête incidente à un $v \in C_1$ et un $w \notin C_1$. Cette arête est dans C_j pour un $j = 2, \dots, n$ (car on a une partition de E). On attache ce cycle en v . S'il reste des cycles dans la partition, on itère ce procédé jusqu'à avoir utilisé tous les cycles.

1.7 Application : le problème du voyageur de commerce (TSP)

1.7.1 Énoncé du problème

Énoncé : Un vendeur de livres démarre de chez lui et doit visiter un certain nombre de librairies avant de rentrer chez lui. Comment doit-il choisir sa route pour minimiser la distance parcourue?

Objet mathématique : Un graphe valué (à chaque arête est associé un nombre appelé poids) où les sommets représentent les librairies et les arêtes représentent les routes.



Objectif : Trouver un cycle hamiltonien de poids minimal.

Remarque : Un graphe complet K_n à n sommets possède $\frac{1}{2}(n-1)!$ cycles hamiltoniens différents. Par exemple, pour $n = 10 \Rightarrow 181440$ cycles. On ne connaît pas encore d'algorithme efficace qui donne une solution au problème.

1.7.2 Arbres couvrant minimum

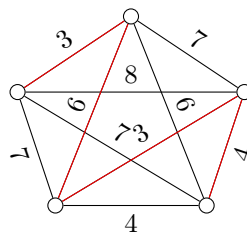
Définition 17

Un arbre couvrant dans un graphe Γ est un arbre qui est un sous-graphe de Γ et qui contient tous les sommets de Γ .

Il existe un algorithme qui donne des arbres couvrants de poids minimum dans un graphe valué.

Algorithme de Kruskal :

- i Choisir une arête de plus petit poids.
- ii Choisir parmi les arêtes restantes une arête de plus petit poids dont l'inclusion ne crée pas un cycle.
- iii Continuer jusqu'à obtenir un arbre couvrant.

Exemple


Remarque : Si C est un cycle hamiltonien dans un graphe Γ , alors $\forall e \in E$ arête de C : $C \setminus \{e\}$ est un arbre couvrant.

\Rightarrow (Solution de TSP) \geq (longueur minimum d'un arbre couvrant)

Mieux : Soit v un sommet de Γ . Tout cycle hamiltonien contient 2 arêtes incidentes à v . Le reste du chemin est un arbre couvrant de $\Gamma \setminus \{v\}$.

\Rightarrow (Solution de TSP) \geq (\sum des longueurs des 2 plus courtes arêtes incidentes à v) + (longueur minimum d'un arbre couvrant de $\Gamma \setminus \{v\}$)

Remarque : Il existe une borne supérieure à TSP en utilisant des cycles eulériens.

1.8 Ordres partiels

Définition 18

Soit P un ensemble. Un ordre partiel sur P est une relation sur P , c'est à dire un ensemble de couples $(p_1, p_2) \in P \times P$, noté $p_1 \leq p_2$ tel que :

1. $p \leq p$ (réflexive)
2. $(p \leq q \text{ et } q \leq p) \Rightarrow p = q$ (anti-symétrique)
3. $(p \leq q \text{ et } q \leq r) \Rightarrow p \leq r$ (transitive)

On note (P, \leq) un ensemble partiellement ordonné.

Remarque : Soit (P, \leq) un ensemble partiellement ordonné, alors on définit un ordre partiel \geq par :

$$x \geq y \Leftrightarrow y \leq x$$

Définition 19

Soit P un ensemble.

1. (P, \leq) est dit totalement ordonné si $\forall p_1, p_2 \in P, p_1 \leq p_2 \text{ ou } p_2 \leq p_1$
2. Soit (P, \leq) un ordre partiel : une chaîne C est un sous-ensemble de P qui est totalement ordonné.

Exemple

(\mathbb{N}, \leq)

$(\mathbb{N}, |)$ où $a \mid b$ si $\exists c \in \mathbb{Z}$ tel que $a \cdot c = b$ ($a, b \in \mathbb{Z}$)

Lien avec la théorie des graphes :

Une relation d'ordre partiel peut se représenter à l'aide d'un graphe dirigé, mais il est très compliqué. On le simplifie en laissant tomber toutes les relations qui s'obtiennent par transitivité et les lacets.

Par transitivité et anti-symétrie : on sait qu'il n'y a pas de cycles, on peut se passer des flèches et on note de bas en haut.

Ex : $(\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}, |)$

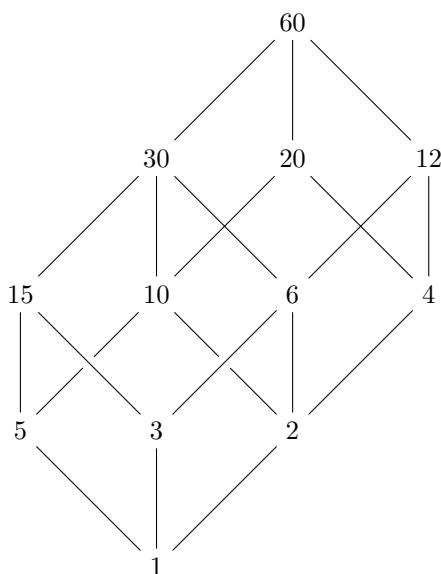


FIGURE 8 – Diagramme de Hasse

Définition 20

Soit (P, \leq) un ensemble partiellement ordonné. Une anti-chaîne est un sous-ensemble A de P tel que $\forall a_1, a_2 \in A : a_1 \not\leq a_2$ et $a_2 \not\leq a_1$.

Exemple

$(\{1, 2, 3, 6, 8\}, /)$, $A = \{2, 3\}$ est une anti-chaîne.

Théorème 6 (Dilworth)

Soit (P, \leq) un ensemble fini partiellement ordonné. Alors il existe une anti-chaîne A et une partition Q de P par des chaînes telle que $\#Q = \#A$.

Lien avec les graphes bipartis :**Théorème 7**

Soit $\Gamma = (V, E)$ un graphe simple.

1. Un couplage M de Γ est un sous-ensemble d'arêtes de Γ , 2 à 2 non adjacentes. Les sommets incidents aux arêtes de M sont dits couplés.
2. Un transversal de Γ est un sous-ensemble T de V tel que toute arête de Γ est incidente à au moins un sommet de T .

Théorème 8 (König)

Soit $\Gamma = (B \amalg W, E)$ un graphe biparti. La cardinalité maximale d'un couplage de Γ est égale à la cardinalité minimum d'un transversal de Γ .

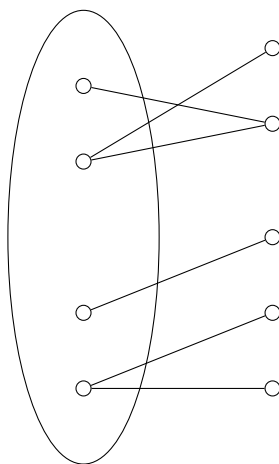
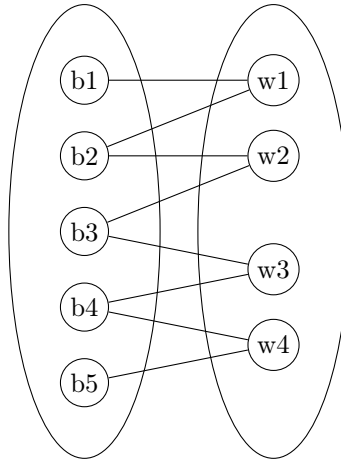
Exemple

FIGURE 9 – Couplage : 4 arêtes. Transversal : 4 sommets.

Définition 21

Soit $\Gamma = (B \amalg W, E)$ un graphe biparti et M un couplage. Un chemin alterné est un chemin qui démarre en un sommet non-couplé de B et alterne une arête de E/M puis une arête dans M et ainsi de suite.

ExempleFIGURE 10 – Couplage max : $(b1, w1, b2, w2, b3, w3, b4, w4, b5)$ **Démonstration**

Soit M un couplage de cardinalité maximale. \forall arête de M , choisissons un de ses sommets incidents comme suit :

1. Le sommet dans W s'il existe un chemin alternant arrivant à ce sommet.
2. Le sommet dans B sinon.

Notons U cet ensemble de sommets. Il faut montrer que cet ensemble U de $\#M$ sommets est un transversal de Γ .

Soit $e = \{b, w\} \in E$, il faut montrer que soit $b \in U$, soit $w \in U$. On peut supposer que $e \notin M$.

M est maximal $\Rightarrow \exists e' \in M$ tel que $b' = b$ ou $w' = w$

On peut supposer $b' = b$ (car si b n'est pas couplé et $w' = w \Rightarrow \{b, w\} = \{b, w'\}$ est donc un chemin alterné et $w' \in U$ par construction).

Donc, il existe un chemin alterné P terminant en w' .

Donc, il existe un chemin alterné P' terminant en w :

1. Soit $P' = P \setminus \{\{w, b\}, \{b, w'\}\} \Rightarrow w \in U$ car P' est un chemin alterné arrivant en W .
2. Soit on définit un nouveau chemin en rajoutant 2 arêtes $P' = P \cup \{w', b\} \cup \{b, w\}$.

(a) Si w est couplé $\Rightarrow w \in U$

(b) Si w pas couplé, on construit un matching + grand en gardant les arêtes de M qui ne sont pas dans P' et en ajoutant les arêtes de P' qui ne sont pas dans M (impossible ?).

Démonstration

On va montrer $König \Rightarrow Dilworth$.

Soit (P, \leq) un ordre partiel. On construit un graphe biparti $\Gamma = (B \amalg W, E)$ où $B = \{(p, 1) | p \in P\}$ et $W = \{(p, 2) | p \in P\}$ et $\{(p, 1), (q, 2)\} \in E \Leftrightarrow p \leq q$ et $p \neq q$.

Soit M un couplage de cardinalité maximale de Γ et T un transversal de cardinalité minimale de Γ . Par $König$, $\#M = \#T$.

On définit $A \subseteq P$ par $A = \{p \in P | (p, 1) \in T \text{ et } (p, 2) \notin T\}$ et $\#A \geq \#P - \#T$.

On construit des chaînes comme suit : $Q = \{C_1, \dots, C_n\}$ où

$$\left\{ \begin{array}{l} \text{Soit } C_i = \{p_0, \dots, p_e\}, \text{ } l \geq 1 \text{ si } \{(p_k, 1), (p_{k+1}, 2)\} \in M \text{ et } (p_e, 1) \text{ n'est pas incident à } M, (p_0, 2) \text{ n'est pas incident à } M. \\ \text{Soit } C_i = \{p\} \text{ si } (p, 1) \text{ et } (p, 2) \text{ ne sont pas incidents à } M. \end{array} \right.$$

Alors, Q est une partition de P (car, par construction, $P = \bigcup_{i=1}^n C_i$ et $C_i \cap C_j = \emptyset, \forall i \neq j$)

$$\text{Et } \#P = \sum_{i=1}^n \#C_i = \#M + \#Q$$

$$\Rightarrow \#Q = \#P - \#M$$

$$\xrightarrow{(König)} \#Q = \#P - \#T \leq \#A$$

$$\Rightarrow \#Q = \#A$$

2 Arithmétique Modulaire

2.1 Les entiers et la division euclidienne

L'ensemble des entiers est noté \mathbb{Z} , il contient les entiers naturels (\mathbb{N}) et leur opposé. Il est naturellement muni de 2 opérations qui satisfont les propriétés suivantes :

1. **L'addition** $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} : (a, b) \rightarrow a + b$

Propriétés :

- (a) **Associativité** $(a + b) + c = a + (b + c), \forall a, b, c \in \mathbb{Z}$
- (b) **Élément neutre** $0 \in \mathbb{Z} : a + 0 = a = 0 + a, \forall a \in \mathbb{Z}$
- (c) **Opposé** $\forall a \in \mathbb{Z} : \exists -a \in \mathbb{Z}$ tel que $a + (-a) = 0 = (-a) + a$
- (d) **Commutativité** $\forall a, b \in \mathbb{Z} : a + b = b + a$

On dit que $(\mathbb{Z}, +)$ est un groupe (a,b,c) commutatif (d).

2. **La multiplication** $\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} : (a, b) \rightarrow a \cdot b$

Propriétés :

- (a) **Associativité** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- (b) **Distributivité par rapport à l'addition**

$$a \cdot (b + c) = ab + ac \quad \forall a, b, c \in \mathbb{Z}$$

$$(a + b) \cdot c = ac + bc$$
- (c) **Commutativité** $a \cdot b = b \cdot a, \forall a, b \in \mathbb{Z}$
- (d) **Élément neutre** $1 \in \mathbb{Z} : 1 \cdot a = a = a \cdot 1, \forall a \in \mathbb{Z}$
- (e) $\forall a, b, c \in \mathbb{Z} : a \cdot c = a \cdot b \Rightarrow c = b$

On dit que $(\mathbb{Z}, +, \cdot)$ est un anneau ($(\mathbb{Z}, +)$ est un groupe commutatif et \cdot satisfait (a) et (b)) unital (d), commutatif (c) et intègre (e).

On a aussi sur \mathbb{Z} une relation d'ordre \leq telle que :

1. \leq est un ordre total
2. $\forall a, b, c \in \mathbb{Z}, a \leq b \Rightarrow a + c \leq b + c$
3. $\forall a, b, c \in \mathbb{Z}, a \leq b, c \geq 0 \Rightarrow ac \leq bc$

La valeur absolue est une application

$$| \cdot | : \mathbb{Z} \rightarrow \mathbb{N} : a \rightarrow \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a \leq 0 \end{cases}$$

telle que :

1. $\forall a \in \mathbb{Z} : |a| = 0 \text{ ssi } a = 0$
2. $\forall a, b \in \mathbb{Z} : |a \cdot b| = |a| \cdot |b|$

Remarque : L'équation $ax = b, a, b \in \mathbb{Z}$ n'a pas toujours de solution dans \mathbb{Z} .

Définition 22

Soit $a, b \in \mathbb{Z}$, on dit que a divise b , et on note $a|b$, si $\exists c \in \mathbb{Z}$ tel que $ac = b$. On dit aussi que b est un multiple de a .

Proposition 3

/ est une relation :

1. **Réflexive** $\forall a \in \mathbb{Z} : a|a$
2. **Transitive** $\forall a, b, c \in \mathbb{Z} : a|b \text{ et } b|c \Rightarrow a|c$
3. **Anti-symétrique** $\forall a, b \in \mathbb{Z} : a|b \text{ et } b|a \Rightarrow a = \pm b$

Théorème 9 (Division Euclidienne)

$\forall a, b \in \mathbb{Z}, b \neq 0, \exists$ des entiers uniques q (quotient) et r (reste) tels que $a = bq + r$ et $0 \leq r < |b|$

Définition 23

Un nombre $p \in \mathbb{Z}$ est premier si $p \neq 1, -1, 0$ et p n'est divisible que par 1, -1, p et $-p$.

Définition 24

Un entier d est un plus grand commun diviseur (pgcd) de 2 entiers a et b ssi :

1. $d|a, d|b$
2. Si $c \in \mathbb{Z} : c|a \text{ et } c|b \Rightarrow c|d$

On note $\text{pgcd}(a, b)$ le pgcd positif de a et $b \in \mathbb{Z}_0$ et on pose $\text{pgcd}(a, 0) = |a|, \forall a \in \mathbb{Z}_0$

2.1.1 L'algorithme d'Euclide**Proposition 4**

Si $a, b \in \mathbb{Z}, b \neq 0$ et $q, r \in \mathbb{Z}$ tel que $a = bq + r$, alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Démonstration

Comme $a = bq + r$, si $c|b$ et $r \Rightarrow c|a$. Comme $a - bq = r$, si $c|a$ et $b \Rightarrow c|r$. Donc, l'ensemble des diviseurs communs de b et r est égal à l'ensemble des diviseurs communs de a et b .

Algorithme d'Euclide : Pour trouver explicitement $\text{pgcd}(a, b) \forall a, b \in \mathbb{Z}, b \neq 0$, on procède comme suit :

On suppose que a et $b \geq 0$ car $\text{pgcd}(a, b) = \text{pgcd}(-a, b) = \text{pgcd}(a, -b) = \text{pgcd}(-a, -b)$.

Par le théorème de division euclidienne : $a = bq_1 + r_1$ pour $q_1 \in \mathbb{Z}$ et $0 \leq r_1 < b$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$.

Si $r_1 = 0$ alors $\text{pgcd}(a, b) = \text{pgcd}(b, 0) = b$. Sinon, $r_1 > 0$ et par division euclidienne : $b = r_1q_2 + r_2$ $0 \leq r_2 < r_1$.

Si $r_2 = 0 \Rightarrow \text{pgcd}(a, b) = r_1$. Sinon, on itère $r_1 = r_2q_3 + r_3$ $0 \leq r_3 < r_2$.

On obtient des restes r_1, r_2, \dots qui sont des entiers non négatifs décroissants. Il doit donc exister $n \in \mathbb{N}_0$ tel que $r_{n+1} = 0$ et $r_n \neq 0$.

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_1, r_2) = \dots = \text{pgcd}(r_{n-1}, r_n) = \text{pgcd}(r_n, 0) = r_n$$

Proposition 5

Soit $a, b \in \mathbb{Z}$, alors $\exists s, t \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = sa + tb$.

Démonstration

Supposons que a et $b > 0$. Soient r_1, \dots, r_n les restes de la division euclidienne donnés par l'algorithme d'Euclide tels que :

$$\begin{aligned} a &= bq_1 + r_1 & 0 < r_1 < b \\ b &= r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_i &= r_{i+1}q_{i+2} + r_{i+2} & 0 < r_{i+2} < r_{i+1} \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} & 0 < r_{i+2} < r_{i+1} \\ r_{n-2} &= r_{n-1}q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + 0 \end{aligned}$$

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \text{pgcd}(r_2, r_3) = \dots = \text{pgcd}(r_{n-1}, r_n)$$

On pose $r_0 = b$ et $r_{-1} = a$ pour l'algo.

On construit s et t comme suit :

$$\text{pgcd}(a, b) = r_n = r_{n-2} - q_n r_{n-1} = s_1 r_{n-2} + t_1 r_{n-1} \quad \text{avec } s_1 = 1, t_1 = -q_n$$

Ensuite, on utilise $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \Leftrightarrow r_{n-1} = r_{n-3} - q_{n-1}r_{n-2}$

$$\begin{aligned} \text{Donc, } \text{pgcd}(a, b) &= s_1 r_{n-2} + t_1 (r_{n-3} - q_{n-1} r_{n-2}) = t_1 r_{n-3} + (s_1 - q_{n-1} t_1) r_{n-2} \\ &= s_2 r_{n-3} + t_2 r_{n-2} \quad \text{avec } s_2 = t_1, t_2 = s_1 - q_{n-1} t_1 \end{aligned}$$

Inductivement, on construit $s_k = t_{k-1}$ et $t_k = s_{k-1} - t_{k-1}q_{n-(k-1)}$ tel que $\text{pgcd}(a, b) = s_k r_{n-(k+1)} + t_k r_{n-k}$
 $\Rightarrow \text{pgcd}(a, b) = \text{pgcd}(r_{-1}, r_0) = s_n r_{-1} + t_n r_0 = s_n a + t_n b$ avec $s_n = t_{n-1}$ et $t_n = s_{n-1} - t_{n-1}q_1$

2.2 Groupes, anneaux et entiers modulo n**2.2.1 Définitions**

Les groupes apparaissent naturellement dès qu'on parle des symétries d'un objet.

Définition 25

Un groupe $(G, *)$ est un ensemble non vide G muni d'une loi de composition $*$: $G \times G \rightarrow G$ tel que :

- (i) $*$ soit associative
- (ii) $\exists e \in G : g * e = g = e * g$ (e est appelé le neutre)
- (iii) $\forall g \in G : \exists g^{-1} \in G$ tq $g * g^{-1} = e = g^{-1} * g$

Exemple 1. $(\mathbb{Z}, +)$ est un groupe

2. (\mathbb{Z}_0, \cdot) n'est pas un groupe

3. (\mathbb{R}, \cdot) n'est pas un groupe

4. (\mathbb{R}_0, \cdot) est un groupe

Définition 26

Soit $(G, *)$ un groupe. Un sous-ensemble $H \subseteq G$ est un sous-groupe de G si $(H, *)$ est un groupe. On note $H \leq G$ ou $(H, *) \leq (G, *)$

Proposition 6

Soit $(G, *)$ un groupe. $H \subseteq G$ est un sous-groupe de G ssi :

1. $e \in H$
2. $\forall g, h \in H : g * h^{-1} \in H$

Exemple

$2\mathbb{Z} = \{\dots, -2, 0, 2, \dots\} = \{2z | z \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$

$3\mathbb{Z} = \{\dots, -3, 0, 3, \dots\} = \{3z | z \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$

Proposition 7

Soit $S \subseteq \mathbb{Z}$ un sous-ensemble non-vidé tel que $(S, +) \leq (\mathbb{Z}, +) \Rightarrow \exists k \in \mathbb{Z}$ tel que $S = k\mathbb{Z}$

Démonstration

Posons k le plus petit entier positif dans $S \Rightarrow k\mathbb{Z} \subseteq S$

Supposons que $\exists s \in S : s \notin k\mathbb{Z}$ (on peut supposer $s > 0$)

$\xrightarrow{\text{DivEucl}} s = kq + r$ avec $0 < r < k$

$\Rightarrow r = s - kq \in S \Rightarrow$ Incompatible avec le fait que k est le plus petit entier.

Exemple

Interprétation du pgcd : Soit $k, l \in \mathbb{Z}$. On définit $k\mathbb{Z} + l\mathbb{Z} = \{kz_1 + lz_2 | z_1, z_2 \in \mathbb{Z}\}$. On a $k\mathbb{Z} + l\mathbb{Z} = \text{pgcd}(k, l)\mathbb{Z}$.

Démonstration

- 1) Montrer que $\text{pgcd}(k, l)\mathbb{Z} \subseteq k\mathbb{Z} + l\mathbb{Z}$: On sait que $\exists s, t$ tel que $\text{pgcd}(k, l) = ks + lt \in k\mathbb{Z} + l\mathbb{Z}$.
- 2) Montrer que $k\mathbb{Z} + l\mathbb{Z} \subseteq \text{pgcd}(k, l)\mathbb{Z}$: Soit $z_1, z_2 \in \mathbb{Z}$ et $kz_1 + lz_2 \in k\mathbb{Z} + l\mathbb{Z}$. Par définition du pgcd : $\exists y_1, y_2$ tel que $k = \text{pgcd}(k, l)y_1$, $l = \text{pgcd}(k, l)y_2 \Rightarrow kz_1 + lz_2 = \text{pgcd}(k, l)(y_1z_1 + y_2z_2) \in \text{pgcd}(k, l)\mathbb{Z}$

2.2.2 Groupes quotients

Soit $(G, +)$ un groupe commutatif. Dans ce cas, on note l'inverse de g , \bar{g} .

Définition 27

Soit $(N, +) \leq (G, +)$. Une classe latérale de N est un ensemble $g + N : \{g + n | n \in N\}$ pour un élément fixé $g \in G$.

Proposition 8

Deux éléments $g, g' \in G$ dét. la même classe latérale de N ssi $g + N = g' + N \Leftrightarrow \forall n \in N, \exists n' \in N$ tel que $g + n = g' + n'$

Démonstration

$\Leftarrow OK$

\Rightarrow

$\cdot \forall n \in N : g + n \in g + N = g' + N \Rightarrow \exists n' \in N$ tq $g + n = g' + n'$

\cdot Unicité : n' et n'' tels que $g' + n' = g' + n'' \Rightarrow g' + (-g') = n'' + (-n') \Rightarrow e = n'' + (-n') \Leftrightarrow n' = n''$

Définition 28

On note G/N l'ensemble de classe latérale de N . $G/N = \{g + N | g \in G\}$

Exemple

$(\mathbb{Z}, +)$ et $7 \in \mathbb{Z} : \mathbb{Z}/7\mathbb{Z} = \{0 + 7\mathbb{Z}, 1 + 7\mathbb{Z}, \dots, 6 + 7\mathbb{Z}\}$ que l'on note $\{\bar{0}, \bar{1}, \dots, \bar{6}\}$. Remarque : $\bar{7} = \bar{0}$

Proposition 9

Soit le groupe $(\mathbb{Z}, +)$ et $k \in \mathbb{Z}$. Alors $\mathbb{Z}/k\mathbb{Z}$ est une partition de \mathbb{Z} .

Démonstration

- $z \in \mathbb{Z} \Rightarrow \exists q, r \text{ tq } z = kq + r \in r + k\mathbb{Z}$
- $r_1, r_2 \in \mathbb{Z} : \text{montrer que } r_1 + k\mathbb{Z} (\dots)$

<PAGES 10 a 11>

2.2.3 Isomorphismes de groupe

<PAGES 11 a 15>

2.2.4 Les anneaux**Définition 29**

Un anneau $(A, +, \cdot)$ est un ensemble non vide A muni de 2 lois de composition : $+: A \times A \rightarrow A \quad (a, b) \rightarrow a + b$ et $\cdot: A \times A \rightarrow A \quad (a, b) \rightarrow a \cdot b$

1. $(A, +)$ est un groupe commutatif
2. La multiplication est associative : $(ab)c = a(bc), \forall a, b, c \in A$.
3. La multiplication est distributive : $(a+b)c = ac + bc$ et $a(b+c) = ab + ac, \forall a, b, c \in A$.

Définition 30

Lorsque \cdot est commutative : $(A, +, \cdot)$ est un anneau commutatif.

Si $\exists 1 \in A \text{ tq } a \cdot 1 = a = 1 \cdot a \quad \forall a \neq 0 \in A \Rightarrow (A, +, \cdot)$ est un anneau unital.

Exemple 1. $(\mathbb{Z}, +, \cdot)$ anneau commutatif unital.

2. $(M_2(\mathbb{R}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{R}, +, \cdot)$ anneau unital (non commutatif)

<PAGE 16 a 18>

2.2.5 Relation de congruence**Définition 31**

Soient $a, b, k \in \mathbb{Z}, k \neq 0, 1, -1$. On dit que a est congru à b modulo k et on note $a \equiv b \pmod{k}$ si $a - b \in k\mathbb{Z}$ (ou encore si $\bar{a} = \bar{b}$ dans $\mathbb{Z}/k\mathbb{Z}$).

Propriétés :

1. La congruence modulo k est une relation d'équivalence.

- **Réflexivité** $\forall a \in \mathbb{Z} : a \equiv a \pmod{k}$
- **Symétrie** $\forall a, b \in \mathbb{Z} : a \equiv b \pmod{k} \Leftrightarrow b \equiv a \pmod{k}$
- **Transitivité** $\forall a, b, c \in \mathbb{Z} : \begin{cases} a \equiv b \pmod{k} \\ b \equiv c \pmod{k} \end{cases} \Rightarrow a \equiv c \pmod{k}$

2. $\forall a_1, b_1, a_2, b_2, k \in \mathbb{Z}, k \neq 0, 1, -1$.

Si $a_1 \equiv a_2 \pmod{k}$ et $b_1 \equiv b_2 \pmod{k}$, alors $\begin{cases} a_1 + b_1 \equiv a_2 + b_2 \pmod{k} \\ a_1 b_1 \equiv a_2 b_2 \pmod{k} \end{cases}$

En conséquence : $\forall c \in \mathbb{Z} : a_1 c \equiv a_2 c \pmod{k}$

Exemple

$$6 \equiv 2(mod\ 4)$$

$$7 \equiv 0(mod\ 7)$$

2.3 Cryptologie : Le système RSA

Pour comprendre le système de cryptage RSA, on aura besoin d'un résultat technique.

Lemme

$\forall z \in \mathbb{N} : (z + 1)^p \equiv z^p + 1 \pmod{p}$ si p est un nombre premier.

Théorème 10 (Le petit théorème de Fermat (**ATTENTION! Ce théorème, le lemme le précédent, et leurs démonstrations mutuelles font partie de ceux à connaître par coeur à l'examen! (pour l'année 2015-2016))**)

Soit $p \in \mathbb{N}$ un nombre premier.

Soit $a \in \mathbb{N}$ un nombre tel que $p \nmid a$ (p ne divise pas a).

Alors, $a^{p-1} \equiv 1 \pmod{p}$

Démonstration

Nous allons procéder par plusieurs étapes.

1. Montrons par récurrence que $\forall a \in \mathbb{N} : a^p \equiv a \pmod{p}$.

$$a = 1 : 1^p = 1 \pmod{p}$$

Supposons vrai pour $a \in \mathbb{N}$ et montrons pour $a + 1$.

Par le lemme, on sait que $(a + 1)^p \equiv a^p + 1 \pmod{p}$. Alors, par hypothèse de récurrence : $(a + 1)^p \equiv a + 1 \pmod{p}$.

2. On va maintenant utiliser $p \nmid a$.

On a : $\forall a \in \mathbb{N} : a^p \equiv a \pmod{p}$.

\Rightarrow Dans $\mathbb{Z}/p\mathbb{Z} : \overline{a^p} = \overline{a}$ et comme $p \nmid a : \exists \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ un inverse de \overline{a} .

$$\Rightarrow \overline{b} \overline{a^p} = \overline{b} \overline{a}$$

$$\Rightarrow \overline{b} \overline{a^p} = \overline{1}$$

$$\Rightarrow \overline{a^{p-1}} = \overline{1} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}$$

Démonstration (du Lemme)

<PAGE 20>

2.3.1 Fonctionnement des clés de chiffrement RSA

2 personnes (A et B) veulent communiquer de manière sûre entre elles.

A choisit 2 nombres premiers p et $q \in \mathbb{N}$ appelés clé privée. A calcule :

$$1. N = pq$$

$$2. O(N) = (p - 1)(q - 1)$$

$$3. e \in \mathbb{Z} \text{ tel que } \text{pgcd}(e, O(N)) = 1$$

appelé l'exposant de chiffrement.

$O(N)$ et e sont premiers entre eux $\Rightarrow \exists 0 < s < O(N) : es \equiv 1 \pmod{O(N)}$, c'est à dire que \overline{s} est l'inverse de \overline{e} dans $\mathbb{Z}/O(N)\mathbb{Z}$. **s est gardé secret.**

A publie les nombres (N, e) appelés la clé publique.

B souhaite envoyer un message à A. Dans le système RSA, la taille du message est $0 < M < N$.

B utilise la clé publique et envoie le message chiffré : $\tilde{M} = M^e \pmod{N}$

Pour déchiffrer le message, A utilise s et obtient : $\tilde{M}^s = M^{es} \pmod{N} = M \pmod{N}$ (par le théorème suivant)

3 Suite

Pour la suite, voir le syllabus de l'année passée. Il faut étudier les 3 premiers chapitres (“Comptage élémentaire”, “Relations de récurrence” et “Fonctions génératrices”)