Mathématique discrètes

2015-16, premier quadrimèstre

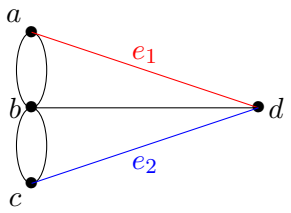
Table des matières

1 Théorie des graphes :

1.1 Définitions

1.1.1 Introduction

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 **arrêtes** ;
— γ est une fonction qui associe à chaque arrête $e \in E$ une paire de sommets $\{x, y\} \in V$.
Qu'on notera plus généralement $\Gamma = (V, E)$



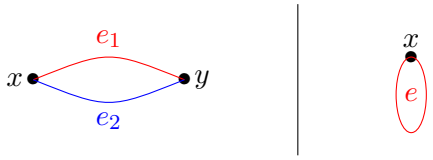
$V = \{a, b, c, d\}$
$E = \{e_1, e_2, ...\}$
$\gamma(e_1) = \{a, d\}$
$\gamma(e_2) = \{c, d\}$

Exemple de graphe.

Soit $\gamma(e) = \{x, y\}$ pour $e \in E, \{x, y\} \in V$. On dit que x et y sont **adjacents** et que e est **incidente** à x et y.

1.1.2 Cas particuliers d'arêtes

On appelle **arêtes multiples** toutes les arêtes incidentes à 2 mêmes points.
Un **lacet** est une arête incidente à un seul point.



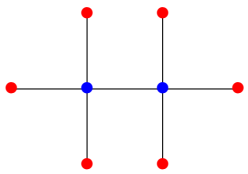
Graphe avec arête multiple et graphe avec lacet.

Un graphe est dit **simple** s'il ne contient pas d'arête multiple ni de lacet.

1.1.3 Degré d'un sommet

Le **degré** d'un sommet $v \in V$ est le nombre d'arêtes incidentes à v (les lacets comptent pours 2 arêtes). On le note : $deg(v)$.

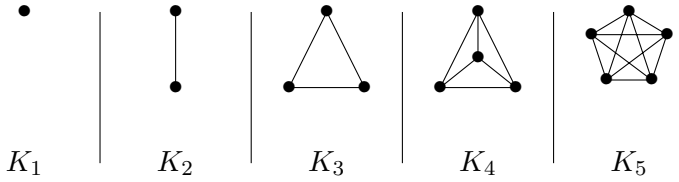
Théorème : Soit $\Gamma = (V, E)$, alors $\sum_{v \in V} deg(v) = 2\#E$. Autrement dit la somme des degrés de tout les sommets est égale au nombre d'arête $\times 2$. Ce qui implique que la somme des degrés d'un graphe est toujours paire.



7 arêtes
2 sommets (bleu) de degré 4
6 sommets (rouge) de degré 1
$2 \times 4 + 6 \times 1 = 14 = 2\times$ nombre d'arête totale

1.1.4 Graphe complet

Le **graphe complet** K_n est le graphe simple à n sommets pour lequel chaque paire de sommet est relié par **une et une seule** arête. Autrement dit, les sommets sont tous adjacents entre-eux.



1.1.5 Sous-graphes

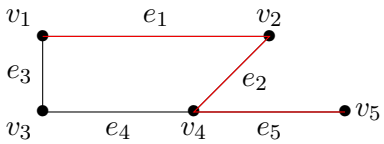
Un graphe $\Gamma' = (U, F)$ est un **sous-graphe** de $\Gamma = (V, E)$ si :
$U \subseteq$ et $F \subseteq E$. On notera $\Gamma' \leq \Gamma$

1.2 Chemins

1.2.1 Definition

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 $v_0, v_1, ..., v_n$ et de n arêtes $e_1, e_2, ..., e_n$ de la forme : $(v_0, e_1, v_1, e_2, v_2, ..., v_{n-1}, e_n, v_n)$.

Un chemin est **simple** si aucun sommet ne se répète, sauf peut-être celui de départ ou d'arrivée.



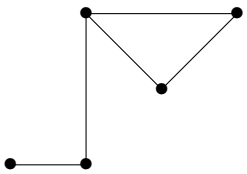
$(v_1, e_1, v_2, e_2, v_4, e_5, v_5)$ est un chemin simple de longueur 3 entre v_1 et v_5

Remarque : Dans un graphe simple on notera juste la suite des sommets (car il existe qu'un seul chemin les reliants). Avec l'exemple ci-dessus : (v_1, v_2, v_4, v_5)

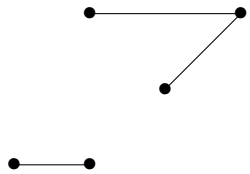
1.2.2 Graphe connexe

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

Soit $\Gamma = (V, E)$ un graphe et $x \in V$, la **composante connexe** de Γ contenant x est le sous-graphe Γ' de Γ dont les sommets et les arêtes sont contenues dans un chemin de Γ démarrant en x.



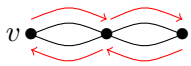
Graphe connexe.



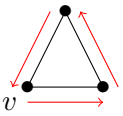
Graphe non-connexe avec 2 composantes connexes.

1.2.3 Cycles

Soit $\Gamma = (V, E)$ et $v \in V$, un **cycle** est un chemin allant de v à v. Il est **simple** si on ne passe pas plusieurs fois sur le même sommet (à part v).



Cycle non-simple.

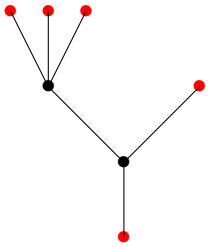


Cycle simple.

1.3 Arbres

1.3.1 Définition

Un **arbre** est un graphe simple, connexe qui ne contient aucun cycle. Ses sommets de degré 1 sont appelés **feuilles**.



Exemple d'arbre (feuilles en rouge).

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

Théorème : Soit T un graphe simple à p sommets, alors :
T est un arbre $\Leftrightarrow$ T a $(p-1)$ arêtes et aucun cycle $\Leftrightarrow$ T à $(p-1)$ arêtes et est connexe.

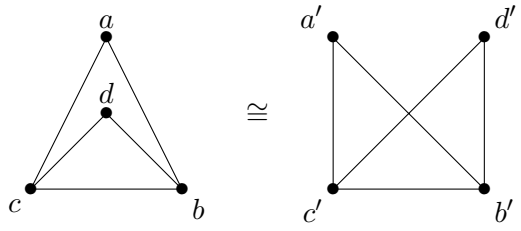
1.3.2 Arbre couvrant

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

Il est utile entre autres pour résoudre le problème du voyageur de commerce.

1.4 Isomorphisme

2 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 $f : V_1 \to V_2$ et une bijection $g : E_1 \to E_2$ telles que $\forall e \in E_1$, e est incident à $v, w \in V_1$ si et seulement si $g(e)$ est incident à $f(v), f(w) \in V_2$. On note cela : $\Gamma_1 \cong \Gamma_2$.
Autrement dit, les graphes ont le même nombre de sommets et sont connectés de la même façon. Autrement dit, si les deux graphes venaient à être dessinés, alors il n'y aurait qu'à déplacer les sommets de l'un pour obtenir la copie conforme de l'autre.



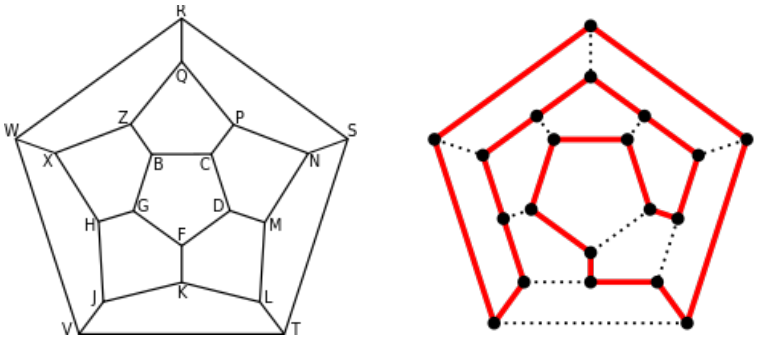
$$f(a) = a'$$
$$f(b) = b'$$
$$f(c) = c'$$
$$f(d) = d'$$

Exemple de graphes isomorphes.

Pour prouver que 2 graphes sont isomorphe on montre la bijection de chaque sommet (il doit avoir le même degré dans le graphe isomorphe et être adjacent aux mêmes sommets).
Inversement pour prouver que 2 graphes ne sont pas isomorphe, il nous suffit de trouver un sommet qui n'est pas dans une bijection.

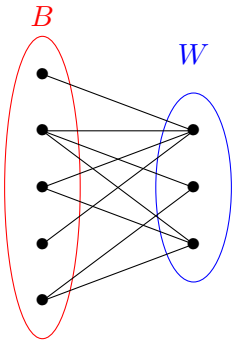
1.5 Graphe Hamiltonien

Un **graphe hamiltonien** est un graphe possédant au moins un cycle passant par tous les sommets une et une seule fois. Ces cycles sont appelés **cycles hamiltoniens**.



Exemple de graphe hamiltonien et d'un cycle hamiltonien.

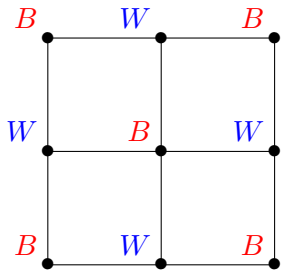
Un graphe $\Gamma = (V, E)$ est **biparti** si on peut écrire $V = B \cup W$ avec $B \cap W = \emptyset$ et toute arête de Γ joint un sommet de B à un sommet de W. Avec B et W des sous-ensembles de sommets.



Exemple de graphe biparti.

Si un graphe est biparti, alors tout ses cycles simples sont de longueur paire.

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

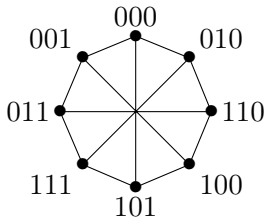


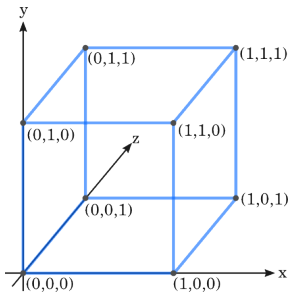
Exemple de graphe biparti non-hamiltonien.

Théorème : Soit Γ un graphe simple avec $p \geq 3$ sommets et $\forall v \in V : deg(v) \geq \frac{1}{2}p$, alors Γ est hamiltonien.

1.6 Illustration - Le code de Gray

Un code de Gray d'ordre n est un arrangement cyclique de 2^n mots binaires de longueur n tel que 2 mots ne différent qu'en une seule position. Par exemple pour $n = 3$:





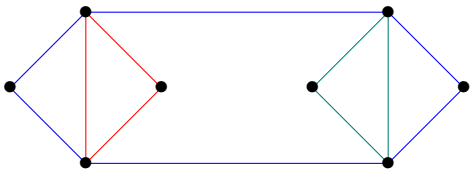
Comparable aux sommets d'un cube.

1.7 Graphe Eulérien

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 tel cycle.

Proposition : Si un graphe est eulérien, alors tout 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 [1] en une union de cycles (arête-)disjoints.



toutes les arêtes se trouvent dans un seul cycle.

Théorème : Soit Γ un graphe connexe. Γ est un graphe eulérien $\Leftrightarrow$ chaque sommet est de degré pair.

1.8 Ordre partiel

Soit P un ensemble. Un **ordre partiel** sur P est une relation sur P (c'est-à-dire un ensemble de couples $(p_1, p_2) \in P \times P$) notée $p_1 \leq p_2$ telle que :
- Réflexivité : $p \leq p$;
- Anti-symétrie : $p \leq q$ et $q \leq p \Rightarrow p = q$;
- Transitivité : $p \leq q$ et $q \leq r \Rightarrow p \leq r$.

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

Un ordre partiel $(P, \leq)$ peut se représenter à l'aide d'un graphe. Si l'on place les arêtes entre les différents sommets en respectant les 3 règles d'un ordre partiel et en enlevant les arêtes pouvant être obtenues par transitivité, alors on obtient un **diagramme de Hasse**. C'est à dire le graphe simple $\Gamma = (P, E)$ tel que :
- $e = \{x, y\} \in E \Leftrightarrow x \leq y$ et $\nexists z | (x \leq z) \wedge (z \leq y)$;
- Dans sa représentation : si $x \leq y, x$ sera placé plus bas que y.

1. collection de sous-ensembles $C_1, ..., C_n$ de E telle que $E = \bigcup_{i=1}^{n} C_i$ et $\forall i \neq j, C_i \cap C_j = \emptyset$.

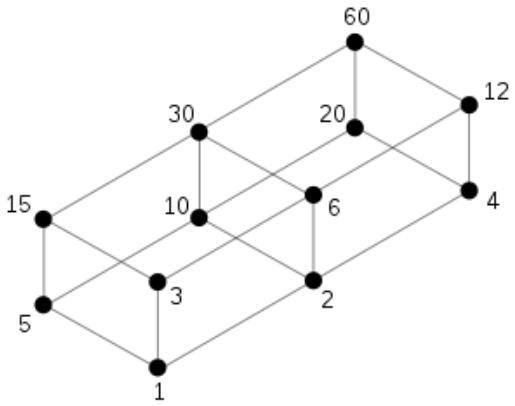


Diagramme de Hasse de l'ensemble des diviseurs de 60, $A = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$, ordonnés par la relation de divisibilité.

Soit $(P, \leq)$ un ordre partiel :

— Une **chaine** dans P est un sous-ensemble C de P tel que :
$\forall c_1, c_2 \in C : c_1 \leq c_2$ ou $c_2 \leq c_1$.
(Dans l'exemple ci-dessus : $\{1, 2, 4, 20, 60\}$ en est une (1 divise 2, qui divisent 4, qui divisent 20, qui divisent 60)).

— Une **antichaîne** dans P est un sous-ensemble A de P tel que :
$\forall a_1 \neq a_2 \in A : a_1 \not\leq a_2$ et $a_2 \not\leq a_1$. Autrement dit c'est une partie dont les éléments sont 2 à 2 incomparables. (Dans l'exemple ci-dessus : $\{5, 3, 2\}$ en est une (5 ne divise pas 3 et 3 ne divise pas 2)).

Théorème (Dilworth) : Soit $(P, \leq)$ un ensemble fini partiellement ordonné. Alors $\exists$ une antichaine A une partition de P par des chaînes $Q = \{C_1, C_2, ..., C_n\}$ tels que $\#Q = \#A$. Autrement dit, le théorème de Dilworth établit, pour un ordre fini, l'existence d'une antichaîne A et d'une partition de l'ensemble ordonné en une famille Q de chaînes, telles que A et Q aient même cardinal.

Remarques :

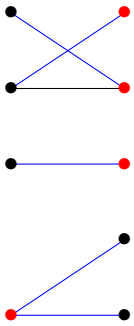
— Q une partition de P et A une antichaîne dans P alors $\#A \leq \#Q$;

— $(P, \leq)$ ordre total. Alors une antichaîne non-vide a exactement 1 élément.

Lien avec les graphes bipartis :

Soit $\Gamma = (V, E)$ un graphe simple ; un **couplage** M de Γ est un sous-ensemble d'arêtes de E qui sont 2 à 2 non-adjacentes. Les sommets incidents aux arêtes de M sont dits couplés. Autrement dit, c'est un ensemble d'arêtes qui n'ont pas de sommets en commun.

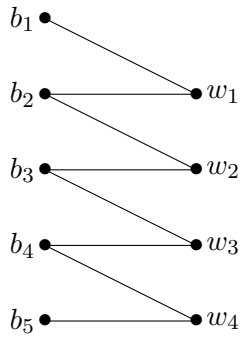
Un **transversal** de Γ est un sous-ensemble T de sommets de V tel que toute arête de E est incidente à au moins 1 sommet de T.



En rouge : transversal à 4 sommets,
en bleu : couplage à 4 arêtes

Théorème (König) : Soit $\Gamma = (V = B \amalg W^{2}, E)$ un graphe biparti. Alors la cardinalité maximale d'un couplage de Γ est égale à la cardinalité minimale d'un transversal de Γ.

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



Exemple de chemin alterné

Proposition : Le théorème de König est équivalent au théorème de Dilworth.

2 Arithmétique modulaire et introduction aux graphes et anneaux

2.1 Les entiers et la division euclidienne

2.1.1 Les entiers

L'ensemble des entiers est noté $\mathbb{Z}$, il contient les entiers naturels ($\mathbb{N}$) et leurs opposé.
Cet ensemble est régi par 2 opérations :

— L'addition usuelle dans $\mathbb{Z} : +\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (a, b) \mapsto a + b$
Propriétés :

1. est commutative $\Leftrightarrow a + b = b + a$
2. est associative $\Leftrightarrow a + (b + c) = (a + b) + c$
3. admet un élément neutre noté $0 \Leftrightarrow 0 + a = a$
4. admet un opposé noté $-a \Leftrightarrow a + (-a) = 0$

On dit que ($\mathbb{Z}$, +) est un groupe (2,3,4) commutatif (1).

— Multiplication : $\cdot : \mathbb{Z} \times Z \to Z : (a, b) \mapsto a \cdot b$
Propriétés :

1. est associative : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. est distributive par rapport à l'addition : $a \cdot (b + c) = a \cdot b + a \cdot c$ et $(a + b) \cdot c = ac + bc$
3. est commutative : $a \cdot b = b \cdot a$
4. $a \cdot b = a \cdot c \Leftrightarrow c = b$
5. admet un neutre : $1 \in \mathbb{Z}, 1 \cdot a = a = a \cdot 1$

On dit que $(\mathbb{Z}, +, \cdot)$ est un anneau [3] unital [4], commutatif [5] et intègre [6].

On à sur $\mathbb{Z}$, une relation d'ordre $\leq$ tels que :

2. $B \cup W = V$ et $B \cap W = \emptyset$
3. $(\mathbb{Z}, +)$ est un groupe commutatif, satisfait propriétée 1 et 2
4. propriétée 5
5. propriétée 3
6. propriétée 4

1. $\leq$ est un ordre total
2. $a \leq b \Rightarrow a + c \leq b + c$
3. $a \leq b, c \geq 0 \Rightarrow a \cdot c \leq b \cdot c$

2.1.2 La division euclidienne

L'équation $a \cdot x = b$ avec $a, b \in \mathbb{Z}$, n'a pas toujours de solutions dans $\mathbb{Z}$.
Soir $a, b \in \mathbb{Z}$, on dit que a divise b et on note a/b, si $\exists c \in \mathbb{Z} | a \cdot c = b$. / est une relation.
Propritétés :

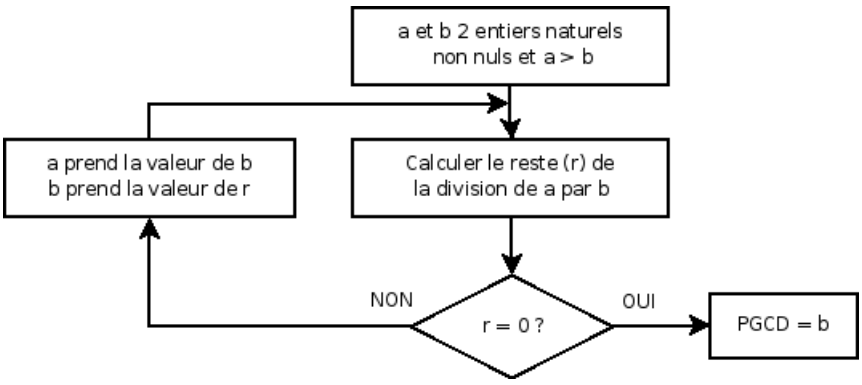
1. Réflexion : a/a
2. transitivité : a/b et $b/c \Rightarrow a/c$
3. Anti-symétrique : a/b et $b/a \Rightarrow a = \pm b$

Théorème (**Division Euclidienne**) : $\forall a, b \in \mathbb{Z}, b \neq 0, \exists$ des entiers uniques q (quotient), r (reste) tel que $a = b \cdot q + r$ et $0 \leq r < |b|$

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 $-p$.

Un entier d est un plus grand commun diviseur de 2 entier non nuls a et b si et seulement si :
— d/a et d/b
— $c \in c/a$ et $c/b \Rightarrow c/d$
On note $pgcd(a, b)$ le plus grand commun diviseur positif de a et $b \in \mathbb{Z}_0$ et on pose $pgcd(a, 0) = |a| \forall a \in Z$

L'algorithme d'Euclide : Si $a, b \in \mathbb{Z}, b \neq 0$, soit $q, r, \in \mathbb{Z} : a = b \cdot q + r$ alors $pgcd(a, b) = pgcd(b, r)$.
Pour calculer le $pgcd(a, b) \forall a, b \in \mathbb{Z}, b \neq 0$ on procède comme suit :
On peut supposer que a et $b \geq 0$ car $pgcd(a, b) = pgcd(-a, b) = pgcd(a, -b) = pgcd(-a, -b)$
Par le théorème de la division euclidienne :
— $a = b \cdot q_1 + r_1$ pour $q_1 \in \mathbb{Z}, 0 \leq r_1 < b$
— $\Rightarrow pgcd(a, b) = pgcd(b, r_1)$
— Si $r_1 = 0 : pgcd(a, b) = pgcd(b, 0) = b$
— Sinon $r_1 > 0$: on itère : $b = r_1 \cdot q_1 + r_2 pour q_2 \in \mathbb{Z}, 0 \leq r_2 < r_1$
— $\Rightarrow pgcd(b, r_1) = pgcd(r_1, r_2)$
— On itère pour obtenir des restes $r_1 > r_2 > r_3 > \ldots > r_n > r_{n+1} = 0$
— On a $pgcd(a, b) = pgcd(b, r_1) = pgcd(r_1, r_2) = \ldots = pgcd(r_n - 1, r_n) = pgcd(r_n, r_{n+1}(= 0)) = r_n$



Soient $a, b \in \mathbb{Z}, b \neq 0, alors \exists s, t \in \mathbb{Z} : pgcd(a, b) = s \cdot a + t \cdot b$

Exemple ; $pgcd(51, 42)$:

$$\begin{aligned} 51 &= 42 \cdot 1 + 9 \\ 42 &= 9 \cdot 4 + 1 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 \\ pgcd(51, 42) &= 3 \end{aligned}$$

Trouvons s et t tel que $s \cdot 51 + t \cdot 42 = 3$

$$\begin{aligned} s_1 = 1 \quad & t_1 = -1 \\ s_2 = -1 \quad & t_2 = 1 - (-1) \cdot 4 = 5 \\ s_3 = 5 \quad & t_3 = -1 - 5 \cdot 1 = -6 \\ 5 \cdot 51 + (-6) \cdot 42 &= 3 \end{aligned}$$

Décomposition en facteurs premiers :
2 nombres entiers non-nuls a et b sont premiers entre eux (ou relativement premiers) si $pgcd(a, b) = 1$.

Proposition (de Bézout) : Deux entiers a et b sont premiers entre eux si et seulement si $\exists s, t \in \mathbb{Z}$ tel que $s \cdot a + t \cdot b = 1$

Proposition (de Gauss) : Si a et b sont premiers entre eux et $c \in \mathbb{Z}$ tel que $b/a \cdot c \Rightarrow b/c$
Corrolaire : Si p est premier et p/ab, avec $a, b \in \mathbb{Z} \Rightarrow p/a$ ou p/b.

Théorème (Factorisation) : $\forall$entier$z \in \mathbb{Z}_0, \exists n \in \mathbb{N}, \exists p_1, \ldots, p_n$ des nombres premiers positifs deux à deux différents et $\exists e_1, \ldots, e_n \in N_0$ tel que :
$z = (\pm 1)p_1^{e_1}, p_2^{e_2}, \ldots, p_n^{e_n}$
Cette expression est unique à l'ordre dans lequel on écrit $p_i^{e_i}$ près.

2.2 Groupes, anneaux et entiers modulo h

2.2.1 Définition

Un groupe $(G, *)$ est un ensemble non-vide G muni d'une loi de composition

$$\begin{aligned} * : G \times G &\to G \\ (g, h) &\mapsto g * h \end{aligned}$$

tels que :

1. $*$ est associatif : $\forall g, h, k \in G : (g * h) * k = g * (h * k)$
2. $\exists$ un neutre $e \in G : g * e = g = e * g \qquad \forall g \in G$
3. $\forall g \in G : \exists$ un inverse $g^{-1} \in G$ tel que $g * g^{-1} = e = g^{-1}g$

Par exemple :
— $(\mathbb{Z}, +) \to$ groupe
— $(\mathbb{Z}_0, \cdot) \to$ pas un groupe (3. pas respecté, ex : $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$)
— $(\mathbb{R}, \cdot) \to$ pas un groupe (3. pas respecté, car 0 n'a pas d'inverse ; $0 \cdot x = 0 \neq e = 1$)
— $(\mathbb{R}_0, \cdot) \to$ un groupe
— V espace vectoriel $\to$ groupe
— $(Gl(V) = \{f : V \to V \setminus f$ isomorphisme linéaire $\}, 0) \to$ groupe

— $(Gl2(\mathbb{R}) = \{\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} | a,b,c,d \in \mathbb{R} a \cdot d \check{} b \cdot c \neq 0\}, \cdot) \rightarrow$ groupe

Définition : Soit $(G, *)$ un graphe. Un sous ensemble H de G est un sous-graphe de G si $(H, *)$ est un graphe. On note $(H, *) \leq (G, *)$ ou bien $H \leq G$

Proposition : $(G, *)$ un groupe et $H \in G$
H est un sous-groupe de G si et seulement si :

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

Exemple : Dans $(\mathbb{Z}, +), 2\mathbb{Z} = \{..., -2, 0, 2, ...\} = \{2z | z \in \mathbb{Z}\}$

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

Exemple : Interprétation du $pgcd$:
$k, l \in \mathbb{Z}$ on définit $k\mathbb{Z} + l\mathbb{Z} = \{k\mathbb{Z}1 + l\mathbb{Z}2 | \mathbb{Z}1, \mathbb{Z}2 \in \mathbb{Z}\}$ si $l \neq$: $k\mathbb{Z} + l\mathbb{Z} = pgcd(k, l)\mathbb{Z}$

2.3 Groupes quotients

Dans cette section, on considère $(G, +)$ un groupe commutatif. Dans ce cas, l'inverse de $g \in G$ se note $-g$ on l'appelle aussi l'opposé de g.

Définition : Soit $(H, +) \leq (G+)$. Une **classe latérale** de H est un ensemble : $g + H = \{g + h | h \in H\}$ pour un $g \in G$ fixé
Proposition : $(H, +) \leq (G, +), g, g' \in G : g + H = g' + H <=> \forall h \in H, \exists !$ [7] $h' \in H : g + h = g' + h'$.

Définition : On notre G/H l'ensemble des classes latérales de H, pour $(H, +) \leq (G, +)$
$G/H = \{g + h | g \in G\}$ $g + h$ seras noté $\overline{g}$
Exemple : $(\mathbb{Z}, +)$ et $7 \in \mathbb{Z} : \mathbb{Z}/7\mathbb{Z} = 0 + 7\mathbb{Z}, 1 + 7\mathbb{Z}, 2 + 7\mathbb{Z}, \ldots, 6 + 7\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

Division euclidienne : $\forall \mathbb{Z} \in \mathbb{Z} : \exists rtelquel : \mathbb{Z} = 7q + r => \mathbb{Z} \in \overline{z} = r + 7\mathbb{Z}$

Proposition : $(\mathbb{Z}, +)$ et $k \in \mathbb{Z}$ alors $\mathbb{Z}/k\mathbb{Z}$ est une partition de $\mathbb{Z}$
Théorème : Soit $(G, +)$ un groupe (commutatif) et $H \leq G$ Alors G/H est muni d'une loi $\mp$ tel que $(G/H, \mp)$ est un groupe commutatif. Précisément, on définit : $\forall g, g' \in G : \overline{g} \mp \overline{g'} := \overline{(g + g')}$
ou bien $(g + H) \mp (g' + H) := (g + g') + H$ Démonstration : Montrons que I est bien défini :
$g, \tilde{g}, g', \tilde{g'} \in G : \overline{g} = \overline{\tilde{g}}$ et $\overline{g'} = \overline{\tilde{g'}}$
Montrons que $\overline{g} \overline{+} \overline{g'} = \overline{\tilde{g}} \overline{+} \overline{\tilde{g'}}$
$\overline{g} = \overline{\tilde{g}} \Rightarrow g + (-\tilde{g}) = h \in H, \overline{g'} = \overline{\tilde{g'}} \Rightarrow g' + (\tilde{g'}) = h' \in H$
$\overline{g} \overline{+} \overline{g'} = \overline{g + g'} = ((\tilde{g} + h) + \tilde{g'} + h') = (\tilde{g} + \tilde{g'} + \overline{h + h'}$ et (c'est égal à) $\overline{\tilde{g}} \overline{+} \overline{\tilde{g'}} = \overline{\tilde{g} + \tilde{g'}}$

— $\overline{+}$ est associatif, commutatif : on les récupère des propriété de $+$
— $g \in G : -\overline{g} = -(g + H) := (-g) + H = -\overline{g}$
— $e \in G$ alors $\overline{e} \in G/\mathrm{H}$ est le neutre pour I

Définition (Exemple principal de groupe quotient) : Pour $n \in N_0, nZ \leq Z$, on définit le groupe des entiers modulo n comme le groupe quotient $(Z/nZ, I)$où$\overline{a} \overline{+} \overline{b} = \overline{a + b} \forall a, b \in Z$
Exemple : $Z/8Z = \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{2} \mp \overline{5} = \overline{7}, \overline{6} \overline{+} \overline{7} = \overline{13} = \overline{5}$
$\overline{0}$ est le neutre : $\overline{4} + \overline{0} = \overline{4 + 0} = \overline{4}$
L'opposé : $-\overline{3} = \overline{-3} = \overline{5}$

7. Il existe un unique

2.4 Isomorphisme de groupes

2.4.1 Définition

Soient $(G, *)$ et $(G', *')$ deux groupes. Un morphisme de groupe est une application f : G -> G' tel que $\forall g, h \in G : f(g * h) = f(g) *' f(h)$
Exemple :

- $(R, +)$ et $(R_0+, .)$
  Exponentiel : $R \to R_0^+ : x \mapsto e^x$ morphisme car $\forall x, y \in R : e^{x+y} = e^x \cdot e^y$
- Logarithme : $R_0^+ \to R$
  Morphisme : $log(x, y) = log(x) + log(y)$
- $Z, p : Z \to Z/kZ : z \mapsto \overline{z}$ morphisme surjectif mais pas injectif.
- $(Z/8Z, +)$ et $(R_4, .)$ racine 4ème de l'unité dans C (complexe)
  $f : Z/8Z \to R_4 : \overline{l} \mapsto e^(2\pi i 2l)/8)$ morphisqme surjectif mais pas injectif
- $(Gl_2(R), \cdot) et (R_0, \cdot)$
  dét : $G\overline{l}2(R) \to R_0 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$ est un morphisme de groupe.

Définition : Un morphisme de groupe $f : G \to G'$ est dit :

- **injectif** : si $\forall g1, g2 \in G : f(g1) = f(g2) \Rightarrow g1 = g2$
- **surjectif** : si $\forall g' \in G' : \exists g \in G$ tel que $f(g) = g'$

Définition : Soient $(G, *)$ et $(G', *')$ 2 groupe et $f : G \to G'$ un morphisme de groupe :

- L'image de f est l'ensemble : $Im(f) = \{f(g) | g \in G\} \subseteq G$
- Le noyau de f est l'ensemble : $Ker(f) = \{g \in G | f(g) = e'\} \subseteq G$

Propriété :

- $Ker(f)$ est un sous-groupe de G
- $Im(f)$ est un sous-graoupe de G'.

Exemple (en reprenant ceux plus haut) :

3 $p : Z- > Z/kZ // \ l- > \overline{l}$ $Ker(p) = kZ \leq K$
4 $Ker(f) = \{\overline{0}, \overline{4}\} \leq Z/8Z$
5 $Ker(det) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} a, b, c, d \in \mathbb{R}$ tel que $det(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = 1\} S\overline{l}2(\mathbb{R})$

Propriété : Soient $(G, *)$ et $(G', *')$ deux groupes et $f : G \to G'$ un morphisme de groupe. Alors :

1. f est injectif $\Leftrightarrow Ker(f) = \{e\}$
2. f est surjectif $\Leftrightarrow Im(f) = G'$

Démonstration :

1. [$\Rightarrow$]
   - Montrons que $e \in Ker(f) : f(e) = f(e * e) = f(e) *' f(e)$
     $\Rightarrow f(e) = f(e) *' f(e) \Rightarrow f(e) = e'$
     Or dans un groupe $(F', *')$ si $x \in G' : x *' x = x \Rightarrow x = e'$
     $\to x *' x = x \Leftrightarrow x *' x *' x^-1 = x * x^-1 = x *' e' = e' \Leftrightarrow x = e'$
   - $\forall g \in Ker(f) : f(g) = e' = f(e) \Rightarrow g = e \Rightarrow Ker(f) = e$
2. [$\Leftarrow$] Exercice

Montrons que f est injectif $g1, g2 \in G : f(g1) = f(g2) \Leftrightarrow f(g1) *' (f(g2))^-1 = f(g2) *' (f(g2))^1 = e'$
Or si $x \in G : (f(x))^-1 = f(x^-1)$
$f(x^-1)*' = f(x^-1 * x) = f(e) = e'$
$\Rightarrow f(x^-1) = (f(x))^-1$
$e' = f(g1) *' (f(g2))^-1 = f(g1) * f(g2^-1) = f(g1 * g2^-1) \Rightarrow g1 * g2^-1 \in Ker(f) = parhypothsee \in g1 * g2^-1 = e \Rightarrow g1 = g2$

Définition : Soient $(G,*)$ et $(G',*')$ 2 groupes
— Un **isomorphisme** de groupe est un morphisme bijectif : $f : G \to G'$
— $(G,*)$ et $(G',*')$ sont dits isomorphes s'il existe un isomorphisme de groupe $f : G \to G'$
On note : $(G,*)\tilde{=}(G',*')$

Exemple :
— Exponentiel $R \to R_0^+$ est un isomorphisme entre $(R,+)$ et $(R_0^+,.)$
— $(\mathbb{Z}/k\mathbb{Z},\overline{+})\tilde{=}(\mathbb{R}_k,\cdot)$
— $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\tilde{\neq}\mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} = (\overline{0},\overline{0}),(\overline{1},\overline{0}),(\overline{0},\overline{1}),(\overline{1},\overline{1})$ et $\forall g \in \mathbb{Z}/2\mathbb{Z}\times Z/2\mathbb{Z} : g+g = (\overline{0},\overline{0})$ [Exemple : $\mathbb{Z}/4\mathbb{Z} : \overline{1} = 1+4\mathbb{Z}$ et $\overline{1}\overline{+}\overline{1} = \overline{2} \neq \overline{0} \Rightarrow$ les groupes ne sont pas isomorphes.

2.5 Les anneaux

2.5.1 Définition

Un anneau $(A,+,.)$ est un ensemble non vide A et de 2 opérations $+ : AxA \to Aet. : AxA \to A$
Tel que :

1. $(A,+)$ est un groupe commutatif
2. . est associatif : $a(bc) = (ab)c \forall a,b,c \in A$
3. La multiplication . est distributive par rapport à l'addition $+$
$\forall a,b,c \in A$
$(a+b)c = ac+bc$
$a(b+c) = ab+ac$

Définition :
— On dit que $(A,+,.)$ est un anneau commutitif si . est commutatif.
— On dit que $(A,+,.)$ est un anneau unital si $\exists 1 \in A : 1.a = a = a.1 \forall a \in A$

Exemple :
— $0.a = 0 = a.0$ désigne le neutre pour $+$
$0.a = (0+0).a = 0.a + 0.a)$ (distributivité) $\Rightarrow 0.a = 0 car(A,+)$ est un groupe.
— $(A,+,.)$ unital $(\exists 1 \in A)$
Montrons que $(-1).a = -a \forall a \in A$

Exemple

1. $(H_2(R) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a,b,c,d \in \mathbb{R}\},+,\cdot)$ est un anneau unital
Le neutre pour $\cdot : 1 := Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
2. $(Hom(R^2,R^2) = \{f : R^2 \to R^2 | f \text{linéaire}\},+,\circ))$ est un anneau unital
Le neutre pour $\circ 1 := Id$

2.5.2 Propriétés

Soit $k \in mathbbZ_0, k \neq 1$ alors $(\mathbb{Z}/k\mathbb{Z},I,\bar{\cdot})$ est un anneau commutatif où $\bar{\cdot}$. est définie par :
$\overline{l} - \overline{l'} = \overline{l.l'} \forall l,l' \in \mathbb{Z}$

Démonstration $l,\tilde{l},l',\tilde{l'} \in Z$ tel que $\overline{l} = \overline{\tilde{l}}(= l+kZ = \tilde{l}+kZ)$ et $\overline{l'} = \overline{\tilde{l'}} \Rightarrow l = \tilde{l}+kz_1$ et $l' = \tilde{l'}+kz_2$ pour $z_1,z_2 \in \mathbb{Z}$
$\overline{\tilde{l}}\cdot\overline{\tilde{l'}} = \overline{\tilde{l}.\tilde{l'}} = \overline{(l-kz_1)\cdot(l'-kz_2)} = \overline{ll'-kz_1l'-kz_2l+kkz_1z_2} = \overline{ll'} = \overline{l} - \overline{l'}$ On a montré que $\bar{\cdot}$ est bien définie

Les autres propriétés de I et $\bar{\cdot}$ découlent des propriété de + et $\cdot$ dans $\mathbb{Z}$. Exemple : Dans $(\mathbb{Z}/10\mathbb{Z}, I\bar{\cdot})$: $\overline{1}\bar{\cdot}\overline{2} = \overline{1.2} = \overline{2}, \overline{1} est le neutre pour \bar{\cdot}$
$\overline{2}\bar{\cdot}\overline{5} = \overline{10} = \overline{0}$

2.6 Intreprétation des pgcd et nombre premiers, premiers entre eux

2.6.1 Définition

Soit $(A, +, .)$ un anneau unital.

- $a \in A$ est inversible si $\exists b \in A$ tel que $a \cdot b = 1 = b \cdot a$
- $0 \neq a \in A$ est un diviseur de 0 si $\exists 0 \neq b \in A : a \cdot b = 0$

Exemple : Soient $0 < a \leq b < k \in N_0 : a.b = k$
$\Rightarrow \overline{a}$ et $\overline{b}$ sont des diviseurs de 0 dans Z/kZ

2.6.2 Propriétés

Si $a \in A$ est un diviseur de $0 \Rightarrow$ a n'est pas inversible.
Exemple : Dans $\mathbb{Z}/4\mathbb{Z} : \overline{2} \cdot \overline{2} = \overline{0}$ dont $\overline{2}$ n'est pas inversible.
Démonstration : $0 \neq a, \exists 0 \neq 6 \in A$ tel que $a.b = 0$
Supposons a inversible $\Rightarrow \exists c \in A$ tel que $c.a = 1 = a.c$
$\Rightarrow b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$
Contradition !

Soit $k \in N_0, k > 1$ et soit $l \in Z$, alors $\overline{l}$ est inversible dans $(Z/kZ, \overline{+}, \bar{\cdot}) \Leftrightarrow ketl$ sont premiers entre eux.

2.6.3 Proposition

Soit k $\in \mathbb{N}_0$, $k > 1$ et soit $l \in \mathbb{Z}$
Alors $\overline{l} \in \mathbb{Z}/k\mathbb{Z}$ est inversible $\Leftrightarrow$ l et k soit premiers entre eux.
Démonstration :

- l et k premiers entre eux $\Leftrightarrow pgcd(k, l) = 1 \Leftrightarrow \exists s, t \in \mathbb{Z}$ tel que $sk + tl = 1$
- $\Longleftarrow$ Montrons que l et k premiers entre eux $\Rightarrow \overline{l}$ inversible.
  $\overline{t}\overline{l} = \overline{tl} = \overline{1 - sk} \in \mathbb{Z}/k\mathbb{Z}$
  $= \overline{1}$
  Donc $\overline{t}$ est l'inverse de $\overline{l}$ dans $\mathbb{Z}/k\mathbb{Z}$
- $\Longrightarrow$ Montrons que $\overline{l}$ inversible $\Rightarrow$ k et l premiers entre eux.
  $\overline{l}$ inversible $\Rightarrow \exists t \in \mathbb{Z}$ tel que $\overline{t}\overline{l} = \overline{1}$
  $\Rightarrow \exists t \in \mathbb{Z}$ tel que $\overline{tl} = \overline{1}$
  $\Rightarrow \exists t \in \mathbb{Z}$ et $s \in \mathbb{Z}$ $tl - 1 = sk$
  $\Rightarrow \exists t, s \in \mathbb{Z} : 1 = tl + (-s)k$
  $\Rightarrow pgcd(k, l) = 1$

Remarque : Quand le pgcd(k,l)=n, on a vu un algorithme qui permet de trouver s et $t \in \mathbb{Z}$ tel que $sk + tl = n$.
Si $n = 1$, on sait trouver l'inverse de $\overline{l}$ dans $\mathbb{Z}/k\mathbb{Z}$
Exemple : Dans $\mathbb{Z}/5\mathbb{Z}$: $\overline{2}$ est inversible : $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$

2.6.4 Définition (champ)

$(K, +, \cdot)$ est un **champ** si $(K, +, \cdot)$ est un anneau commutatif unital tel que $\forall 0 \neq k \in K : \exists$ un inverse $k^{-1} \cdot k = 1$
Exemple :

- $\mathbb{Z}/2\mathbb{Z}$ est un champ

— $\mathbb{Z}/3\mathbb{Z}$ est un champ
— $\mathbb{Z}/4\mathbb{Z}$ pas un champ (car $\overline{3}$ n'a pas de k^{-1} dans l'ensemble)

2.6.5 Proposition

Soit $k \in \mathbb{N}_0, k > 1$. Alors $\mathbb{Z}/k\mathbb{Z}$ est un champ $\Leftrightarrow$ k est un nombre premier.
Remarque :
— la démonstration est un corollaire de la proposition précédente.
— $\forall p \in \mathbb{Z}$ premier, on a un champ à p éléments : $\mathbb{Z}/p\mathbb{Z}$

2.7 Relation de congruence

2.7.1 Définition

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
$a \equiv b(\text{mod k})$
Si $a - b \in k\mathbb{Z}$ ou de manière équivalente : $\overline{a} = \overline{b}$ dans $\mathbb{Z}/k\mathbb{Z}$

2.7.2 Propriétés

1. La congruence modulo k est une relation d'équivalence :
   — réflexivité : $\forall a \in \mathbb{Z} : a \equiv a(\text{mod k})$
   — symétrie : $\forall a, b \in \mathbb{Z} : a \equiv b(\text{mod k}) \Leftrightarrow b \equiv a(\text{mod k})$.
   — transitivité : $\forall a, b, c \in \mathbb{Z}$:
   $a \equiv b(\text{mod k})$
   $b \equiv c(\text{mod k})$
   $\Rightarrow a \equiv c(\text{mod k})$.
2. $\forall a_1, b_1, a_2, b_2 \in \mathbb{Z}, k \neq 0, 1, -1$
   Si $a_1 \equiv a_2(\text{mod k})$ et $b_1 \equiv b_2(\text{mod k})$.
   Alors
   — $a_1 + b_2 \equiv a_2 + b_2(\text{mod k})$
   — $a_1 b_1 \equiv a_2 b_2(\text{mod k})$
   En conséquence : $\forall c \in \mathbb{Z} : a_1 c \equiv a_2 c(\text{mod k})$

Exemple : $6 \equiv 2(\text{mod } 4)$, $7 \equiv 0(\text{mod } 7)$

2.8 Cryptologie le système clés RSA

Lemme : $\forall n \in \mathbb{N} : (n+1)^p \equiv n^p + 1(\text{mod p})$ si p est un nombre premier

2.8.1 Petit théorème de Fermat

$p \in \mathbb{N}$ un nombre premier
$ain\mathbb{N}$ tel que $p \nmid a$ (p ne divise pas a)
Alors $a^{p-1} \equiv 1(\text{mod p})$.

Démonstration : Montrons par récurrence que $\forall a \in \mathbb{N} : aP \equiv a(\text{mod p})$.
$a = 1 : 1^p \equiv 1(\text{mod p})$

— Supposons que ce soit vrai pour $a \in \mathbb{N}$ (c'est à dire $a^p \equiv a(\text{mod p})$) et montrons le pour $(a+1)$ (c'est à dire montrer que $(a+1)^p \equiv a + 1(\text{mod p})$.
Par le lemme : $(a+1)^p \equiv a^p + 1(\text{mod p})$
Par l'hypothèse de récurence : $(a+1)^p \equiv a + 1(\text{mod p})$

On va maintenant utiliser $p \nmid a$. On a : $\forall a \in \mathbb{N} : a^p \equiv a(\text{mod p})$. $\Rightarrow$ 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 $\overline{a}$.
$\Rightarrow \overline{b}\overline{a^p} = \overline{b}.\overline{a}$
$\Rightarrow \overline{b}\overline{a}^p = \overline{1}$
$\Rightarrow \overline{a}^{p-1} = \overline{1} \Leftrightarrow a^{p-1} \equiv 1(\text{mod p})$

Démonstration $(n+1)^p = \Sigma_{i=0}^{p} \binom{p}{i} n^i = n^p + \Sigma_{i>0}^{p-1} \binom{p}{i} n^i + 1$

$\Rightarrow (p+1)^p \equiv n^p + 1 + \Sigma_{i=1}^{p-1} \binom{p}{i} (\text{mod p})$.

Rappel : $\binom{p}{i} = \frac{p!}{i!(p-1)!}$

Par récurence sur i : on va montrer que $p| \binom{p}{i}$ pour $i = 1, ..., (p-1)$

— $i = 1$: $\binom{p}{i} = p$ et $p|p$

— Supposons que $p| \binom{p}{i}$ pour $1 \leq i < p-1$ et montrons que $p| \binom{p}{i+1}$

$\binom{p}{i+1} = \frac{p!}{(i+1)!(p-i-1)!} = \binom{p}{i} \frac{(p-1)}{(i+1)}$ $p| \binom{p}{i} \Rightarrow \binom{p}{i} = p.b$ pour un $b \in \mathbb{Z} \Rightarrow \binom{p}{i} = \frac{p.b.(p-1)}{(i+1)} \in \mathbb{N}$

p premier et $1 < i+1 \leq p-1$
$\Rightarrow (i+1)|b.(p-i)$ (car $(i+1) \nmid p$)
$\Rightarrow \binom{p}{i+1} = p.\frac{b(p-1)}{(i+1)(\in\mathbb{Z}} \Rightarrow p| \binom{p}{i+1}$
$\Rightarrow \binom{p}{i} \equiv O(\text{mod p})$ pour $i = 1, ..., p-1$
$\Rightarrow (n+1)^p \equiv n^p + 1(\text{mod p})$

2.8.2 Fonctionnement des clés de chiffrement

2 personnes : A et B veulent communiquer de manière sûre etnre elles.
— A choisit 2 nombres premiers p et q (ont 100 chiffres) $\in \mathbb{N}$ appelé clé privée. A calcule :
  — $N = p.q$
  — $\phi(N) = (p-1)(q-1)$
  — $e \in \mathbb{Z}$ tel que $pgcd(e, \phi(N)) = 1$ (appelé l'exposant de chiffrement) (e et $\phi(N)$ sont premiers entre eux).
  $\Rightarrow \exists 0 < s < \phi(N) : es \equiv 1(\text{mod } \phi(N))$. ($\overline{s}$ est l'invserse de $\overline{l}$ dans $\mathbb{Z}/\phi(N)\mathbb{Z}$).
  (En fait $\exists s, t \in \mathbb{Z}$ tel que $t\phi(N) + se = 1$)
  s est gardé secret.
  A publie les nombres (N, e) appelé la clé publique.
— B souhaite envoyer un message à A. Dans le système RSA : Message : $0 < M < N$ et $M \in \mathbb{Z}$
  Exemple : _ $\rightarrow 01$, $A \rightarrow 02, B \rightarrow 03, ...$
  BONJOUR $\rightarrow$ 03151410152118
  B utilise la clé publique et envoie le message chiffré.
  $\tilde{M} \equiv M^e(\text{mod N})$.
— Pour déchiffrer le message : A utilise s et obtient :
  $\tilde{M}^s \equiv M^{es}(\text{mod N}) \equiv M(\text{mod N})$ (par le théorème suivant).

2.8.3 Théorème

$\forall 0 < M < N = p.q \in \mathbb{N}, p, q$ premier.
Soit $u \equiv 1 (\text{mod } \phi(N)$
Alors $M^u \equiv M (\text{mod N})$
Démonstration : $0 < M < N \Rightarrow p \nmid M$ ou $q \nmid M$

— Cas 1 $p \nmid M et q \nmid M$
$u = 1 + t\phi(N) = 1 + t(p-1)(p-1)$
$M^u = M^{1+t(p-1)(q-1)} = MM^{t(p-1)(q-1)}$
$p \nmid M$, Petit théorème de Fermat : $(M^{t(q-1)})^{p-1} \equiv 1 (\text{mod p})$
$q \nmid M$, Petit théorème de Fermat : $(M^{t(p-1)})^{q-1} \equiv 1 (\text{mod q})$
$\rightarrow M^u \equiv M (\text{mod p})$
$\rightarrow M^u \equiv M (\text{mod q})$
$\Rightarrow p | M^u - M$
$\Rightarrow q | M^u - M$
$\Rightarrow pq | M^u - M \Rightarrow M^u \equiv M (\text{mod N})$

— Cas 2 $p | M$ et $q \nmid M$
$u = 1 + t(p-1)(q-1)$
$q \nmid M \Rightarrow$ (Petit théorème de Fermat) $(M^{t(p-1)})^{q-1} \equiv 1 (\text{mod q})$
$\Rightarrow M^{t(p-1)(q-1)} = 1 + lq$ pour $l \in \mathbb{Z}$
$M^u = M(1 + lq) = M + lMq = M + lc.p.q \Rightarrow M^u \equiv M (\text{mod N})$
$(p | M \Rightarrow M = p.c$ pour $c \in \mathbb{Z}$

— Cas 3 $p \nmid M$ et $q | M$ ($\rightarrow Exercice$)

3 Combinatoire énumérative

3.1 Comptage élémentaire