Algèbre 1
Généralités et Arithmétique dans $\mathbb{Z}$

Table des matières

1 Logique et ensembles

1.1 Introduction

► La logique mathématique s'intéresse aux règles de construction de phrases mathématiques correctes : propositions ou énoncés, et aux règles permettant d'établir la vérité de ces phrases.
► Le but de ce chapitre est de rappeler et de compléter les notions fondamentales sur les ensembles et la logique.
► La notion **d'ensemble** est une notion première, qu'on admet et qu'on ne peut pas définir à partir d'autres notions.
► Intuitivement, on peut considérer un ensemble E comme une "collection" d'objets qui sont ses éléments.
► Dans certaines situations, les éléments d'un ensemble sont écrits entre deux accolades $\{...\}$. Par exemple $E = \{a, b, c, d\}$.
► On note $x \in E$ pour signifier que x **appartient** à E ou que x est **un élément** de E. Si x n'est pas un élément de E on note $x \notin E$

Exemples 1.1. $E = \{1, 2, 3\}$ est l'ensemble constitué des nombres 1,2 et 3. On a $2 \in E$ mais $5 \notin E$.

► Les ensembles de nombres sont supposés connus, aussi nous les considérerons d'une manière systématique, sans les redéfinir. On rapelle les notations usuelles :
$\mathbb{N}$, l'ensemble des nombres entiers naturels, $\mathbb{N} = \{0, 1, 2, \ldots\}$.
$\mathbb{Z}$, l'ensemble des entiers relatifs, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
$\mathbb{Q}$, l'ensemble des nombres rationnels, $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z}^*\}$
$\mathbb{R}$, l'ensemble des nombres réels contenant $\mathbb{Q}$ et les nombres irrationnels tels que $\sqrt{2}, \pi, e$.
$\mathbb{C}$, l'ensemble des nombres complexes, $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$, où $i^2 = -1$.

1.2 Notion de proposition

► Les énoncés mathématiques sont constitués de phrases qu'on appelle **propositions** ou **assertions**. Une proposition est un enoncé qui peut être vrai ou faux. Par exemple " 2+2=4" est une proposition vraie, " $5 < 3$" est une proposition fausse. A toute proposition P on attribue sa **valeur de vérité**, 1 ou "V" si elle est vraie et 0 ou "F" si elle est fausse.
► Deux propositions P et Q sont dites **équivalentes** si elles ont la même valeur de vérité (elles expriment alors le même contenu). On note alors $P \equiv Q$. Ainsi, pour $x \in \mathbb{N}$, les deux propositions $P :'' x \leq 7''$ et $Q :'' x + 2 \leq 9''$, sont équivalentes.
► Si $P \equiv Q$, on dira aussi que "P est vraie, si et seulement si, Q est vraie", ou que Q est une condition nécessaire et suffisante pour P.
► **Négation d'une proposition.** A partir d'une proposition P on peut former sa négation (ou son contraire) non$P$ notée aussi $\neg P$ ou encore $\overline{P}$, qui a la valeur de vérité contraire à celle de P, suivant la table de vérité :

P	$\overline{P}$
V	F
F	V

Par exemple la négation de $x \in E$ est $x \notin E$. La négation de $x = y$ est $x \neq y$.

Proposition 1.2. $P \equiv \overline{\overline{P}}$.

PREUVE. Vérification immédiate sur la table de vérité.

P	$\overline{P}$	$\overline{\overline{P}}$
V	F	V
F	V	F

■

1.3 Prédicat et quantificateurs

► On appelle **prédicat** ou **forme propositionnelle**, une proposition $P(x, y, \ldots)$, contenant des variables $x, y, \ldots$, et dont la valeur de vérité dépend de ces variables. "x est pair" est un prédicat. (La variable ici est x).
Les variables dans les prédicats sont souvent précédées par des **quantificateurs**. Dans le langage mathématique, il y a deux quantificateurs :
► Le quantificateur **universel :** $\forall$ (quelque soit ou pour tout). L'enoncé $\forall x \in E$ on a $P(x)$, veut dire que tous les éléments $x \in E$ vérifie $P(x)$.

Exemple 1.3. $\forall x \in \mathbb{R}, x^2 \geq 0$.

► Le quantificateur **existentiel :** $\exists$ (il existe au moins). L'énoncé $\exists x \in E : P(x)$ veut dire qu'il existe au moins $x \in E$ qui vérifie $P(x)$.

Exemple 1.4. $\exists x \in \mathbb{R} : x^2 = 2$.

► On utilise parfois aussi le symbole $\exists!$ pour l'existence et l'unicité. $\exists! x \in E : P(x)$, veut dire qu'il existe un seul x tel que $P(x)$.

Exemple 1.5. $\exists! x \in \mathbb{R}_+ : x^2 = 2$.

► Un enoncé peut contenir deux ou plusieurs quantificateurs, l'ordre dans lequel ils sont écrits est important. Ainsi une assertion qui commence par $\forall x$, $\exists y$ n'est pas nécessairement équivalente à celle qui commence par $\exists y$, $\forall x$.

Exemple 1.6. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : x < y$ est vraie, alors que $\exists y \in \mathbb{R} : \forall x \in \mathbb{R}, x < y$ est fausse.

► **Négation d'un prédicat avec quantificateur** La négation des prédicats avec quantificateurs obéit aux règles suivantes :
► La négation de $\forall x \in E, P(x)$ est $\exists x \in E : \overline{P(x)}$.

Exemple 1.7. la négation de $''\forall x \in \mathbb{R}, x^2 \geq 0''$, est $''\exists x \in \mathbb{R} : x^2 < 0''$.

► La négation de $\exists x \in E : P(x)$ est $\forall x \in E,\ \overline{P(x)}$.

Exemple 1.8. la négation de $''\exists n \in \mathbb{N} : n + 1 = 0''$, est $''\forall n \in \mathbb{N} : n + 1 \neq 0''$.

1.4 Connecteurs logiques

► A partir de deux propositions P et Q on peut former d'autres propositions à l'aide de connecteurs logiques. Les plus importants sont les connecteurs et, ou, $\Rightarrow, \Leftrightarrow, \ldots$.

► **La conjonction :** P et Q, notée aussi $P \wedge Q$, qui est vraie seulement si les deux propositions P et Q sont vraies. On a la table de vérité suivante.

P	Q	P et Q
V	V	V
V	F	F
F	V	F
F	F	F

Exemple 1.9. Soit $x \in \mathbb{N}$, on considère les propositions $P :''$ x est un diviseur de $24\,(x \mid 24)''$ et $Q :''$ $x \leq 6''$. P et Q est vraie pour $x = 1, 2, 3, 4, 6$, elle est fausse pour 8 et pour 5 par exemple.

Proposition 1.10. *Soient P, Q, R trois propositions, alors :*
1 - P et Q $\equiv$ Q et P
2 - $(P$ et Q$)$ et R $\equiv$ P et (Q et R)
3 - P et P $\equiv$ P.
4 - Principe de non contradiction : P et (non P) *est toujours fausse.*

Une théorie (ou un raisonnement) est dite contradictoire, si elle contient une proposition et sa négation qui soient toutes les deux vraies.

▶ **La disjonction** P ou Q, notée aussi $P \vee Q$ qui est vraie si l'une au moins des propositions P et Q est vraie :

P	Q	P ou Q
V	V	V
V	F	V
F	V	V
F	F	F

Exemple 1.11. Dans l'exemple 1.9 précédent P ou Q est vraie pour $x = 0, 1, 2, 3, 4, 5, 6, 8, 12, 24$.

Proposition 1.12. *Soient P, Q, R trois propostions :*
1 - P ou Q $\equiv$ Q ou P.
2 - $(P$ ou Q$)$ ou R $\equiv$ P ou (Q ou R).
3 - P ou P $\equiv$ P
4 - Principe du tiers exclu : P ou (non P) *est toujours vraie.*

Proposition 1.13. *(Lois de De Morgan). Soient P et Q deux propositions, alors on a :*
$\overline{P \text{ et } Q} \equiv \overline{P}$ ou $\overline{Q}$
$\overline{P \text{ ou } Q} \equiv \overline{P}$ et $\overline{Q}$

▶ **L'implication logique** P implique Q, notée aussi $P \Rightarrow Q$, est donnée par la table de vérité :

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Proposition 1.14. *Soient P et Q deux propositions, alors :*
1 - $P \Rightarrow Q \equiv \overline{P}$ ou Q.
2 - $P \Rightarrow Q \equiv \overline{Q} \Rightarrow \overline{P}$ *(principe de contraposition).*
3 - $\overline{(P \Rightarrow Q)} \equiv P$ et $\overline{\text{Q}}$

Exemple 1.15. La proposition $\forall x \in \mathbb{R} : x \leq 2 \Rightarrow x \leq 4$ est vraie. Sa négation est $\exists x \in \mathbb{R} : x \leq 2$ et $x > 4$ est fausse.

► **Double implication** notée $P \Leftrightarrow Q$, c'est la proposition $(P \Rightarrow Q)$ et (Q ⇒ P) :

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Remarque 1.16. Soient P et Q deux propositions. $P \Leftrightarrow Q$ est vraie, si et seulement si, $P \equiv Q$. Aussi, on écrira souvent $P \Leftrightarrow Q$ pour signifier que $P \equiv Q$.

Remarque 1.17. On peut combiner plusieurs connecteurs logiques avec plusieurs propositions par exemple $(P$ et Q$) \Rightarrow$ R ; $(P \Rightarrow Q) \Rightarrow P$, etc.

1.5 Raisonnements mathématiques.

Les théories mathématiques se basent sur un certain nombre de résultats admis sans démonstration qu'on appelle **axiomes**. Par exemple, l'existence de l'ensemble $\mathbb{N}$ est l'un de ces axiomes. Le but de ces théories est d'établir à partir de ces axiomes et la logique, des résultats qu'on appelle **théorèmes, propositions, lemmes, propriétés**, etc. . Les **démonstrations** ou **preuves** de ces résultats, s'appuient sur des **raisonnements logiques**. Dans la suite on expose les principales méthodes de raisonnements.

1 - **Raisonnement par déduction ou raisonnement direct :** On veut montrer que $P \Rightarrow Q$. On suppose que P est vraie et avec une succession d'implications, on montre que Q est vraie.

Exemple 1.18. Montrons que $\forall x \in \mathbb{R},\ x \geq 1 \Rightarrow x^2 + x - 2 \geq 0$. Supposons que $x \geq 1$, on a $x^2 + x \geq 1 + 1 = 2$, Donc $x^2 + x - 2 \geq 0$

2 - **Raisonnement par contraposition :** Pour montrer que $P \Rightarrow Q$, il est parfois plus simple de démontrer que $\overline{Q} \Rightarrow \overline{P}$.

Exemple 1.19. Montrons que $\forall x \in \mathbb{N}$, si x^2 est pair alors x est pair. Par contraposition, supposons que x est impair et montrons que x^2 est impair. On a : $x = 2k + 1$ avec $k \in \mathbb{N}$. Donc $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2k' + 1$, où $k' = 2k^2 + 2k$, donc x^2 est impair.

Exemple 1.20. Pour montrer que $\forall x \in \mathbb{R}; x^2 \notin \mathbb{Q} \Rightarrow x \notin \mathbb{Q}$, il est plus facile de montrer que $x \in \mathbb{Q} \Rightarrow x^2 \in \mathbb{Q}$.

3 - **Raisonnement par l'absurde :** Si on suppose qu'une propriété P est fausse et qu'à la fin du raisonnement on aboutit à une contradiction, alors P est vraie. (une contadiction est une assertion du type Q et non Q).

Exemple 1.21. Montrons la proposition P"$\sqrt{2} \notin \mathbb{Q}$". On suppose que P est fausse. i.e. $\sqrt{2} \in \mathbb{Q}$. Par conséquent $\exists x = \frac{p}{q} \in \mathbb{Q}$, avec $p, q \in \mathbb{N}$ premiers enre eux (n'ont pas de diviseurs communs), tels que $2 = x^2 = \frac{p^2}{q^2}$. Donc $2q^2 = p^2$. Ce qui implique que $2 \mid p$. On pose alors $p = 2p'$. On a $2q^2 = 4p'^2$. Ce qui entraîne $q^2 = 2p'^2$, ou encore $2 \mid q$. On a $2 \mid p$ et $2 \mid q$, ce qui est absurde car p et q sont supposés premiers entre eux. Cette contradiction montre que non P est fausse. Donc P est vraie. C'est à dire que $\sqrt{2} \notin \mathbb{Q}$. ■

4 - **Raisonnement par contre-exemple :** Pour montrer que la proposition $''\forall x, P(x)''$ est fausse on montre que $\exists x : P(x)$ n'est pas vérifié.

Exemple 1.22. l'assertion $P :'$ $\forall n \in \mathbb{N}$, $2n^2 + 1$ est un multiple de $3'$ est fausse car, par exemple, $n = 3$ ne vérifie pas cette propriété. C'est un contre-exemple.

5 - **Raisonnement par récurrence :** Soit P une propriété, et $n_0 \in \mathbb{N}$. Si $P(n_0)$ est vraie et si $\forall n \geq n_0, P(n) \Rightarrow P(n+1)$, alors $\forall n \geq n_0$, $P(n)$ est vraie.
Ainsi pour démontrer une propriété $P(n)$ est vraie $\forall n \geq n_0$, on adopte alors le schéma suivant :
Initialisation : On vérifie que $P(n_0)$ est vraie.
Hérédité : On montre que $\forall n \geq n_0, P(n) \Rightarrow P(n+1)$.

Exemple 1.23. Pour $n \in \mathbb{N}$, posons $S_n = \sum_{k=0}^{n} k$. Montrons la propriété ;

$$P(n) : \ \forall n \in \mathbb{N}, S_n = \frac{n(n+1)}{2}$$

Initialisation : $P(0)$ est vraie.
Hérédité : Soit $n \in \mathbb{N}$, On suppose que $P(n)$ est vraie (Hypothèse de récurrence H.R). On a $S_{n+1} = S_n + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$. Donc $P(n+1)$ est vraie. On en déduit qu'elle est vraie pour tout n.

Exemple 1.24. Montrons que $\forall n \in \mathbb{N}, n \geq 4 \Rightarrow n^2 \leq 2^n$.
Initialisation : pour $n = 4$, $4^2 = 2^4 = 16$. L'inégalité est vraie.
Hérédité : soit $n \geq 4$, supposons que $n^2 \leq 2^n$. On a $2^{n+1} = 2.2^n = 2^n + 2^n$. D'après l'hypothèse de récurrence, $2^{n+1} \geq n^2 + n^2$. Or $n^2 \geq 2n + 1, \forall n \geq 4$, il en résulte que $2^{n+1} \geq n^2 + 2n + 1 = (n+1)^2$.

Récurrence forte dans la récurrence forte on procède selon le schéma de démonstration suivant :
Initialisation : On vérifie que $P(n_0)$ est vraie.
Hérédité : On montre que si $k \in \mathbb{N}$ est tel que $n_0 \leq k < n$, $P(k) \Rightarrow P(n)$.
Alors $\forall n \geq n_0, P(n)$ est vraie.

Exemple 1.25. Montrer que tout entier naturel supérieur ou égal à 2 possède un diviseur premier.
Initialisation : On démontre que 2 possède un diviseur premier qui est lui-même.
Hérédité : Soit n un entier supérieur ou égal à 2, on suppose que tous les entiers k tels que $2 \leq k < n$ possèdent un diviseur premier (hypothèse de récurrence) et l'on cherche à prouver qu'il en est de même pour n.
Ou bien n est premier alors il possède un diviseur premier qui est lui-même
Ou bien n est composé et il existe un entier d supérieur ou égal à 2 et strictement inférieur n qui divise n. Alors, par hypothèse de récurrence, d possède un diviseur premier, qui est aussi un diviseur de n.

1.6 Inclusion et égalité entre deux ensembles

Définition 1.26. Soient E et F deux ensembles. On dit que E est **inclus** dans F, noté $E \subset F$, si

$$\forall x,\ x \in E \Rightarrow x \in F$$

On dit aussi que E est un **sous-ensemble** ou **une partie** de F.
La négation est $E \not\subset F$. On a

$$E \not\subset F \Leftrightarrow \exists x \in E : x \notin F$$

Exemple 1.27. $E = \{0, 1, 2\}$, $F = \{1, 2, 3\}$, $G = \{0, 1, 2, 4\}$ On a $E \subset G$ mais $E \not\subset F$.

Proposition 1.28. *Si $E \subset F$ et $F \subset G$ alors $E \subset G$.*

Egalité de deux ensembles : Soient E et F deux ensembles alors

$$(E = F) \Leftrightarrow (E \subset F \text{ et } F \subset E)$$

1.7 Ensemble défini par un prédicat

Soit $P(x)$ un prédicat admissible, alors il existe un ensemble $E = \{x : P(x)\}$, qui est l'ensemble de tous les éléments qui vérifient P.

Exemple 1.29. $E = \{x \in \mathbb{N} : 3 \leq x \leq 8\} = \{3, 4, 5, 6, 7, 8\}$

Ensemble vide. Il existe un ensemble qui ne contient aucun élément, l'ensemble vide, noté $\varnothing$.

Proposition 1.30. *Pour tout ensemble E on a $\varnothing \subset E$.*

PREUVE. Sinon, $\exists x \in \varnothing : x \notin E$. Absurde car $\exists x \in \varnothing$ est une proposition fausse. ■

Singleton et paire : Soient x, y deux objets mathématiques distincts. Il existe un ensemble $\{x\}$ contenant seulement x appelé singleton de l'élément x et un ensemble contenant x et y noté $\{x, y\}$, appelé paire de x et y.

Ensemble des parties d'un ensemble : Soit E un ensemble. Il existe un ensemble noté $\mathcal{P}(E)$ dont les éléments sont les sous-ensembles de E. $\mathcal{P}(E) = \{A : A \subset E\}$.

Exemple 1.31. Si $E = \{a, b, c\}$, alors $\mathcal{P}(E) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, E\}$.

1.8 Opérations sur les ensembles :

Soient E et F deux ensembles, on définit :
La réunion : de E et F, $E \cup F = \{x : x \in E \text{ ou } x \in F\}$ (lire E union F).
L'intersection : de E et F, $E \cap F = \{x : x \in E \text{ et } x \in F\}$. (lire E inter F).
Deux ensembles dont l'intersection est vide sont dits **disjoints**.

Proposition 1.32. *Soient A, B, C trois ensembles, alors :*
i - $A \cup A = A$, $A \cup B = B \cup A$, $A \cup (B \cup C) = (A \cup B) \cup C)$.
ii - $A \cap A = A$, $A \cap B = B \cap A$, $A \cap (B \cap C) = (A \cap B) \cap C)$.
iii - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Différence de deux ensembles E et F, $E\backslash F = \{x \in E : x \notin F\}$. (lire E moins F).
Si $A \subset E$, on définit **le complémentaire** de A dans E par $\bar{A}$ ou A^c ou C_E^A, $\overline{A} = E\backslash A$. On a : $E\backslash F = E \cap \overline{F}$.

Proposition 1.33. *(Lois de De Morgan)*
Soient A et B deux parties d'un ensemble E, alors :
i - $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
ii - $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Différence symétrique de deux ensembles E et F, $E\Delta F = (E\backslash F) \cup (F\backslash E)$. On a : $E\Delta F = (E \cup F)\backslash(E \cap F)$.

1.9 Partitions

Définition 1.34. Soit E un ensemble non vide. On appelle **partition** de E un ensemble $\mathcal{A}$ de parties de E, ($\mathcal{A} \subset \mathcal{P}(E)$, telle que :
1. Les éléments de $\mathcal{A}$, sont non vides, ($\forall A \in \mathcal{A}, A \neq \varnothing$).
2. Tout élément de E est contenue dans un et un seul élément de $\mathcal{A}$, ($\forall x \in E, \exists! A \in \mathcal{A} : x \in A$)

Exemple 1.35. Soit $E = \{0, 1, 2, 3, 4, 5\}$.
$\mathcal{A}_1 = \{\{0, 1\}, \{4\}, \{2, 3, 5\}\}$ est une partition de E.
$\mathcal{A}_2 = \{\varnothing, \{0, 1, 2\}, \{4\}, \{3, 5\}\}$ n'est une partition de E car contient $\varnothing$.
$\mathcal{A}_3 = \{\{0, 1, 2\}, \{2, 4\}, \{3, 5\}\}$ n'est une partition de E car 2 appartient à deux éléments différents de $\mathcal{A}_3$
$\mathcal{A}_4 = \{\{0, 1, 2\}, \{4, 5\}\}$ n'est une partition de E car 3 n'appartient à aucun élément de $\mathcal{A}_4$.

2 Correspondances et Applications

2.1 Couples et produit cartésien

Définition 2.1. On appelle **couple** formé par deux éléments x et y l'expression (x, y) telle que

$$(x, y) = (x', y') \Leftrightarrow x = x' \text{ et } y = y'$$

x est la première composante ou première projection du couple.
y est la deuxième composante ou deuxième projection du couple.

Définition 2.2. Soient E et F deux ensembles. **Le produit cartésien** $E \times F$ est l'ensemble des couples (x, y) tels que $x \in E$ et $y \in F$.

$$E \times F = \{(x, y) : x \in E \text{ et } y \in F\}$$

Si $E = F$, $E \times E$ est noté parfois E^2.

On définit de même les triplets (x, y, z), les quadriplets (x, y, z, t), et plus généralement les n-uplets $(x_1, x_2 \ldots, x_n)$. Ainsi que les produits cartésiens $E \times F \times G$, $E \times F \times G \times H$, et plus généralement $E_1 \times E_2 \times \ldots \times E_n$.

2.2 Correspondances

Définition 2.3. On appelle **correspondance**, la donnée d'un triplet $\varphi = (E, F, \mathcal{G})$ où E et F sont deux ensembles et $\mathcal{G}$ une partie de $E \times F$.
E est appelé l'ensemble de **départ** de φ, F est l'ensemble **d'arrivée**. $\mathcal{G}$ est le **graphe** de φ.
Si $(x, y) \in \mathcal{G}$, y est une **image** de x par φ, x est un **antécédent** de y par φ.
Le **domaine de définition** de φ est l'ensemble $D_\varphi = \{x \in E : \exists y \in F, (x, y) \in \mathcal{G}\}$.

Exemple 2.4. $E = \{0, 1, 2, 3\}$, $F = \{a, b, c\}$, $\mathcal{G} = \{(0, b), (0, c), (2, a), (3, a)\}$.

Définition 2.5. On appelle **fonction** une correspondance dans laquelle tout élément de l'ensemble de départ possède au plus une image.

Exemple 2.6. Soit $E = \mathbb{R}, F = \mathbb{R}, \mathcal{G} = \{(x, y) \in E \times F : x = y^2\}$. Alors $\mathcal{G}$ est le graphe d'une fonction f. Son domaine de définition est $\mathbb{R}_+$. Pour $x \in D_f = \mathbb{R}_+$, $(x, y) \in G \Leftrightarrow y = \sqrt{x}$.

2.3 Applications

Définition 2.7. Une **application** $f : E \to F$ est une correspondance $(E, F, \mathcal{G})$ telle que $\forall x \in E, \exists! y \in F : (x, y) \in \mathcal{G}$. i.e. tout élément de E possède une et une seule image.
On note F^E ou $\mathcal{F}(E, F)$ l'ensemble de toutes les applications de E dans F.

▶ Une application est complétement définie par son ensemble de départ, son ensemble d'arrivée et l'image de chaque élément de l'ensemble de départ.
▶ Deux applications f et g sont égales si elles ont même ensemble de départ, même ensemble d'arrivée et pour tout élément x dans l'ensemble de départ on a $f(x) = g(x)$.

Exemple 2.8. On a une application $f : \mathbb{R} \to \mathbb{R}$, définie par :

$$f(x) = \begin{cases} 2x^2 - 3x + 1 & \text{si } x \leq 1 \\ \frac{1}{|x-1|}, & \text{sinon.} \end{cases}$$

► Soit $E \subset F$. L'application $\imath : E \to F$, définie par $\imath(x) = x$, s'appelle **l'injection canonique** de E dans F. Si $E = F$, l'application $I_E : E \to E$, $I_E(x) = x$, notée aussi Id_E, est appelée **l'application identique** de E ou **identité** de E.
► Soit $f : E \to F$ une application. $A \subset E$. L'application $f_{|A} : A \to F$, définie par $f_{|A}(x) = f(x)$, $\forall x \in A$, est appelée **la restriction** de f, à A. On dit aussi que f est un prolongement de $f_{|A}$.
► Très souvent, par abus de notation, une application et sa restriction sont désignées par le même symbole. Ainsi, l'application $x \mapsto \sin x$, désigne aussi bien l'application sinus $\mathbb{R} \to \mathbb{R}$, que cette application de $[0, 2\pi]$ dans $\mathbb{R}$.
► **Composée de deux applications** : Soient $f : E \to F$, $g : F \to G$, la composée de g et de f est l'application $g \circ f : E \to G$, définie par $g \circ f(x) = g(f(x))$.

Exemple 2.9. Soient $f, g : \mathbb{R} \to \mathbb{R}$, définies par $f(x) = x^2$ et $g(x) = x + 1$ $\forall x \in \mathbb{R}$. On a $g \circ f(x) = x^2 + 1$, $f \circ g(x) = (x + 1)^2 = x^2 + 2x + 1$. Noter que $f \circ g \neq g \circ f$.

Proposition 2.10. *Soit $f : E \to F$ une application $f \circ I_E = f$ et $I_F \circ f = f$.*
Soient $f : E \to F$, $g : F \to G$, $h : G \to H$, trois applications : on a : $(h \circ g) \circ f = h \circ (g \circ f)$.

- Soit $f : E \to F$ une application, A une partie de E, B une partie de F.
- On appelle **image directe** de A par f l'ensemble $f(A) = \{y \in F : \exists x \in E,\ y = f(x)\}$.
- On appelle **image réciproque** de B par f l'ensemble $\overset{-1}{f}(B) = \{x \in E : f(x) \in B\}$.

Exemple 2.11. Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$. On a $f(\mathbb{R}) = \mathbb{R}_+$, $\overset{-1}{f}(\{4\}) = \{2, -2\}$, $\overset{-1}{f}(\{-1\}) = \varnothing$.

2.4 Injection, surjection, bijection

Définition 2.12. Soit $f : E \to F$ une application :
f est dite **injective** si $\forall x, x' \in E, f(x) = f(x') \Rightarrow x = x'$. i.e. tout élément de F admet au plus un antécédent.
On dit aussi que f est une injection de E dans F.
f est dite **surjective**, si tout $y \in F$ admet un antécédent dans E.
On dit aussi que f est une surjection de E sur F.
f est dite **bijective**, si tout élément de F possède un et un seul antécédent.
f est bijective, si et seulement si, elle est injective et surjective.
On dit aussi que f est une bijection de E sur F.

Exemple 2.13.
1 - L'application $\mathbb{N} \to \mathbb{N}$, $n \mapsto n + 1$, est injective non surjective. (0 n'a pas d'antécédent).
2 - L'application $f : \mathbb{N} \to \mathbb{N}$, définie par $f(0) = 0$ et $f(n) = n - 1$, si $n \geq 1$, est surjective non injective.
3 - L'application $\mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$, n'est ni injective ni surjective.

Proposition 2.14. *Soient $f : E \to F$ et $g : F \to G$ deux applications.*
Si f et g sont injectives, alors $g \circ f$ est injective.
Si f et g sont surjectives, alors $g \circ f$ est surjective.

Théorème 2.15. *Soit $f : E \to F$ une application. Alors :*
1 - f est injective, si et seulement si, il existe une application $g : F \to E$ telle que $g \circ f = Id_E$
2 - f est surjective, si et seulement si, il existe une application $g : F \to E$ telle que $f \circ g = Id_F$

PREUVE.
1 - $\Rightarrow$ Supposons que f est injective. Posons $G = f(E)$ et $H = F \setminus G$. Soit $a \in E$ fixé. Si $y \in G$, il existe $x \in E$ unique tel que $y = f(x)$. On peut alors définir l'application $g : F \to E$ de la manière suivante.

$$g(y) = \begin{cases} x, & \text{si } y = f(x) \in G \\ a, & \text{si } x \in H \end{cases}$$

Alors, $\forall x \in E$, $g(f(x)) = x$. i.e $g \circ f = I_E$.
$\Leftarrow$. Supposons qu'il existe $g : F \to E$ telle que $g \circ f = I_E$. Montrons que f est injective. Soient $x, x' \in E$, tels que $f(x) = f(x')$. On compose alors à gauche par g, on a alors $g(f(x)) = g(f(x'))$. Donc $x = x'$, par conséquent f est injective.
2 - $\Rightarrow$. Supposons que f est surjective. Pour chaque $y \in F$, $\overset{-1}{f}(\{y\}) \neq \varnothing$, et les ensembles $\overset{-1}{f}(\{y\})$ forment une partition de E. Grâce à l'axiome du choix, on peut choisir pour chaque $y \in F$ un $x \in E$ unique tel que $f(x) = y$. Posons alors $g(y) = x$. On a alors $f(g(y)) = y, \forall y \in F$. Donc $f \circ g = I_F$.
$\Leftarrow$. Supposons qu'il existe $g : F \to E$ telle que $f \circ g = I_F$. Montrons que f est surjective. Soit $y \in F$. Posons $x = g(y) \in E$. Alors $f(x) = f(g(y)) = y$. f est surjective. ■

Théorème 2.16. *Soit $f : E \to F$ une application :*
1 - *f est bijective $\Leftrightarrow$ il existe une application $g : F \to E$ telle que $g \circ f = I_E$ et $f \circ g = I_F$. Lorsque c'est le cas, l'application g est unique on la note f^{-1}, on l'appelle* **l'application réciproque** *de f. De plus, f^{-1} est bijective et $(f^{-1})^{-1} = f$.*
2 - *Soient $f : E \to F$ et $g : F \to G$ deux bijections, alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

PREUVE.
1 - $\Rightarrow$ Supposons que f est bijective. Alors f est injective et f est surjective. D'après le théorème 2.15, il existe $g : F \to E$ telle que $g \circ f = I_E$ et il existe $h : F \to E$ telle que $f \circ h = I_F$. On a alors $h = I_E \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ I_F = g$. Donc $h = g$. D'où il existe une application $g : F \to E$ tel que $g \circ f = I_E$ et $f \circ g = I_F$. Ceci montre aussi l'unicité de g.
La réciproque est claire d'après le théorème 2.15.
2 - $g \circ f \circ f^{-1} \circ g^{-1} = I_G$ et $f^{-1} \circ g^{-1} \circ g \circ f = I_F$. Donc $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
■

Exemples 2.17.
1 - L'application $f : \mathbb{R}_+ \to \mathbb{R}_+$, $f(x) = x^2$ est bijective. Sa bijection réciproque est $x \mapsto \sqrt{x}$.
2 - L'application $\ln : \mathbb{R}_+^* \to \mathbb{R}$, est bijective, sa réciproque est la fonction exponentielle.

2.5 Familles d'éléments et familles de parties

Définition 2.18. Soit E un ensemble.On appelle **famille** d'éléments de E indexée par un ensemble I, toute application $I \to E$; $i \mapsto x_i$. On note la famille par $(x_i)_{i \in I}$, où $x_i \in E$. I est appelé l'ensemble d'indices.

▶ Cas particulier : lorsqu'on prend $I \subset \mathbb{N}$, une famille d'éléments de E est alors appelée **une suite** d'éléments de E, qu'on note alors : $x_0, x_1, \ldots, x_n, \ldots$.

Définition 2.19.
1 - On appelle famille de parties d'un ensemble E, toute famille d'éléments $(A_i)_{i \in I}$ de $\mathcal{P}(E)$, ensemble de parties de E. i.e. $A_i \subset E, \forall i \in I$.

2 - On appelle réunion de la famille, l'ensemble $\cup_{i\in I}A_i = \{x \in E : \exists i \in I, x \in A_i\}$.
Cas particulier, si $I = \{1, 2\}$, $\bigcup_{i\in I} A_i = \{x \in E : x \in A_1 \text{ ou } x \in A_2\} = A_1 \bigcup A_2$.
3 - On appelle intersection de la famille, l'ensemble $\cap_{i\in I}A_i = \{x \in E : \forall i \in I, x \in A_i\}$.
Cas particulier, si $I = \{1, 2\}$, $\bigcap_{i\in I} A_i = \{x \in E : x \in A_1 \text{ et } x \in A_2\} = A_1 \bigcap A_2$.

Exemples 2.20.
1 - $\bigcup_{n\in\mathbb{N}}]-n, n[= \mathbb{R}$.
2 - $\bigcap_{n\in\mathbb{N}^*}[-\frac{1}{n}, \frac{1}{n}] = \{0\}$.

2.6 Applications entre ensembles finis

Un ensemble E est dit **fini** s'il existe $n \in \mathbb{N}$ et une bijection de E à $\{1, \ldots, n\}$. L'entier n est alors unique et il est appelé **cardinal** de E ou le nombre d'éléments de E. On le note $\text{card}(E)$.
L'ensemble vide est fini et son cardinal est égal à zéro.
Un ensemble fini E de cardinal n, peut s'écrire $E = \{x_1, x_2, \ldots, x_n\}$.
Un ensemble qui n'est pas fini est dit **infini**.
L'ensemble $\mathbb{N}$ est infini.

Proposition 2.21. *Soient E et F deux ensembles finis. Alors les trois assertions suivantes sont équivalentes :*
(i) $card(E) \leq card(F)$.
(ii) Il existe un injection $f : E \to F$.
(iii) Il existe un surjection $g : F \to E$.

Preuve. Montrons que $(i) \Leftrightarrow (ii)$.
$(i) \Rightarrow (ii)$. Supposons que $card(E) \leq card(F)$. On peut supposer que $E = \{1, 2, \ldots, n\}$ et $F = \{1, 2, \ldots, m\}$ avec $n \leq m$. L'application $E \to F$, $k \mapsto k$ est injective.
$(ii) \Rightarrow (i)$. Soit $f : E \to F$ une application injective. On considère l'application $g : E \to f(E)$, définie par $g(x) = f(x)$. Alors g est bijective. D'où $card(E) = card(f(E)) \leq card(F)$.
$(ii) \Leftrightarrow (iii)$, d'après la proposition 2.15. ■

Proposition 2.22. *Soient E et F deux ensembles tels que E soit fini et $f : E \to F$ une application. Alors :*
1. *$f(E)$ est fini et* $\text{card}f(E) \leq \text{card}E$.
2. *f est injective* $\Leftrightarrow \text{card}f(E) = \text{card}E$.

Preuve.
1. Comme l'application $g : E \to f(E)$, $x \mapsto f(x)$ est surjective, d'après la proposition précédente, on a $card(f(E)) \leq card(E)$.
2. Si f est injective, alors $g : E \to f(E)$, $x \mapsto f(x)$ est bijective. Donc $\text{card}f(E) = card(E)$. Supposons que f n'est pas injective. On peut supposer que $f(x_1) = f(x_2)$. Donc $f(E) = \{f(x_1), f(x_3) \ldots, f(x_n)\}$. Par conséquent, $\text{card}f(E) < card(E)$. ■

Théorème 2.23. *Soient E et F deux ensembles finis tels que* $\text{card}E = \text{card}F$, *alors les assertions suivantes sont équivalentes :*
(i) f est injective.
(ii) f est surjective.
(iii) f est bijective.

Preuve. Il suffit de montrer l'équivalence entre (i) et (ii). On a
f est injective $\Leftrightarrow \text{card}f(E) = card(E) = card(F) \Leftrightarrow f(E) = F \Leftrightarrow f$ est surjective ■

3 Relations binaires, Relations d'équivalence, Relations d'ordre

3.1 Relations binaires

Une **relation binaire** $\mathcal{R}$ sur un ensemble E est la donnée d'une correspondance $(E, E, \mathcal{G})$. On note $x\mathcal{R}y$, pour signifier que $(x, y) \in \mathcal{G}$ et note $(E, \mathcal{R})$ l'ensemble E muni de la relation $\mathcal{R}$.

Exemple 3.1. La relation de divisibilité : Dans $\mathbb{Z}$ on définit la relation de divisibilité notée $|$ par :

$$\forall x, y \in \mathbb{Z},\ x \mid y \Leftrightarrow \exists k \in \mathbb{Z} : y = kx$$

Définition 3.2. Soit E un ensemble muni d'une relation binaire $\mathcal{R}$.
$\mathcal{R}$ est dite **réflexive** si $\forall x \in E$ on a : $x\mathcal{R}x$.
$\mathcal{R}$ est dite **symétrique** si $\forall x, y \in E$ on a : $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
$\mathcal{R}$ est dite **antisymétrique** si $\forall x, y \in E$ on a : $x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$.
$\mathcal{R}$ est dite **transitive** si $\forall x, y, z \in E$, $x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

3.2 Relations d'équivalences

Définition 3.3. Une relation binaire $\mathcal{R}$ sur un ensemble E est dite une **relation d'équivalence** si elle est réflexive, symétrique et transitive.
Soit $(E, \mathcal{R})$ un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Pour $x \in E$, on appelle **classe de** x **modulo** $\mathcal{R}$ l'ensemble $\bar{x} = \{y \in E : y\mathcal{R}x\}$. Notons que $\bar{x} = \bar{y} \Leftrightarrow x\mathcal{R}y$.

Exemple 3.4.
1 - Dans un ensemble non vide E, la relation d'égalité $x = y$, est une relation d'équivalence.
2 - Soit $n \in \mathbb{N}$. Dans $\mathbb{Z}$, on définit la relation $x\mathcal{R}y \Leftrightarrow n|x - y$, qu'on note encore $x \equiv y \pmod{n}$. On l'appelle relation d'équivalence modulo n. C'est une relation d'équivalence. Pour tout $k \in \mathbb{Z}$, on a $\bar{k} = k + n\mathbb{Z}$.
3 - Soit $f : E \to F$ une application. La relation $x\mathcal{R}y \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence.

Proposition 3.5. *Deux classes d'équivalences sont ou bien disjointes ou bien confondues.*

Preuve. Soit $\mathcal{R}$ une relation d'équivalence. Supposons que $\bar{x} \cap \bar{y} \neq \varnothing$. Soit $z \in \bar{x} \cap \bar{y}$, on a $z \in \bar{x}$ donc $x\mathcal{R}z$ et $z \in \bar{y}$, donc $z\mathcal{R}y$. Il en résulte que $x\mathcal{R}y$, d'où $\bar{x} = \bar{y}$. ■

Définition 3.6. soit $(E, \mathcal{R})$ un ensemble E muni d'une relation d'équivalence $\mathcal{R}$. On appelle **ensemble quotient** de E par $\mathcal{R}$, l'ensemble noté $E/\mathcal{R}$ des classes d'équivalences modulo $\mathcal{R}$.

Proposition 3.7. *L'ensemble quotient $E/\mathcal{R}$ d'un ensemble E par une relation d'équivalence $\mathcal{R}$ est une une partition de E. De plus, l'application $\pi : E \to E/\mathcal{R}$, $x \mapsto \bar{x}$ est une surjection appelée* **surjection canonique** *associée à $\mathcal{R}$.*

Preuve. Les classes d'équivalences sont non vides, disjointes deux à deux et leur réunion est l'ensemble E. ■

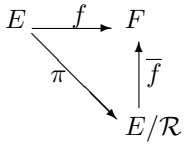
Exemple 3.8. L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n, est noté $\mathbb{Z}/n\mathbb{Z}$. En utilisant la division euclidienne, on montre que $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

Théorème 3.9. *(Décomposition canonique d'une application). Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$, F un ensemble et $f : E \to F$ une application. On suppose que*

$$\forall x, y \in E,\ x\mathcal{R}y \Rightarrow f(x) = f(y)$$

Alors il existe une application $\bar{f} : E/\mathcal{R} \to F$ unique telle que $f = \bar{f} \circ \pi$, où $\pi : E \to E/\mathcal{R}$ est la surjection canonique.
Si de plus $\forall x, y \in E,\ x\mathcal{R}y \Leftrightarrow f(x) = f(y)$, alors $\bar{f}$ est injective.

► On interprète ce théorème en disant qu'il existe une application $\overline{f} : E/\mathcal{R} \to F$ unique telle que le diagramme suivant soit commutatif.



3.3 Relations d'ordre

Définition 3.10. Une relation binaire $\prec$ sur E est dite **relation d'ordre** si elle est réflexive, antisymétrique et transitive. Le couple $(E, \prec)$ est dit ensemble ordonné.
Deux éléments x et y sont dits **comparables**, si $x \prec y$ ou $x \prec y$. Un ordre est dit **total** si deux éléments quelcoques sont comparables.
Un ordre qui n'est pas total est dit **partiel**.
Soit $(E, \prec)$ un ensemble ordonné. On appelle **chaîne** de E, toute partie de E totalement ordonnée.

Exemple 3.11.
1 - Dans $\mathbb{R}$, les relations $x \leq y$ et $x \geq y$, sont des relations d'ordre total.
2 - Dans $\mathbb{N}$, la relation de divisibilité est une relation d'ordre partiel.
3 - Soit E un ensemble. La relation d'inclusion $\subset$ dans $\mathcal{P}(E)$ est une relation d'ordre. Si E contient au moins deux éléments, cet ordre est partiel.

Définition 3.12. Soit A une partie d'un ensemble ordonné $(E, \prec)$. Un élément M (resp. m) de E est dit **majorant** (resp. **minorant**) de A si $\forall x \in A$, on a $x \prec M$ (resp. $m \prec x$).
Lorsqu'un majorant (resp. un minorant) appartient à A (ce qui n'est pas toujours le cas), on dit que c'est le plus grand élément ou maximum (resp. plus petit élément ou minimum) de A.

Exemple 3.13. Dans $(\mathbb{R}, \leq)$, l'intervalle $[0, 1[$ possède un plus petit élément qui est 0. Tout réel supérieur à 1 est un majorant de $[0, 1[$, mais $[0, 1[$ ne possède pas de plus grand élément.

Définition 3.14. Soit $(E, \prec)$ un ensemble ordonné et A une partie majorée (resp. minorée) de E.
On appelle **borne supérieure** (resp. **borne inférieure**) de A s'il existe, le plus petit des majorants (resp. plus grand des minorants) de A.
La borne supérieure de A dans $(E, \prec)$ est notée $\sup(A)$ et la borne inférieure est notée $\inf(A)$.

Exemple 3.15. Dans $(\mathbb{R}, \leq)$ toute partie non vide majorée possède une borne supérieure et toute partie non vide minorée possède une borne inférieure. (voir cours d'Analyse). Ce n'est pas le cas pour $(\mathbb{Q}, \leq)$, en effet, $A = \{x \in \mathbb{Q}_+ : x^2 \leq 2\}$ est majorée par 2, mais n'a pas de borne supérieure dans $\mathbb{Q}$.

3.4 Ordre naturel sur $\mathbb{N}$

Théorème 3.16. *Toute partie non vide de* $(\mathbb{N}, \leq)$ *possède un plus petit élément.*

PREUVE. Soit A une partie non vide de $\mathbb{N}$. Notons E l'ensemble de tous les minorants de A. E n'est pas vide car $0 \in E$. Montrons qu'il existe $n_0 \in E$ tel que $n_0 + 1 \notin E$. Sinon, $\forall n \in E$, on a $n + 1 \in E$. Ceci impliquerait par récurrence que $E = \mathbb{N}$. Ce qui est absurde. Soit alors $n_0 \in E$ tel que $n_0 + 1 \notin E$. Montrons que $n_0 \in A$. Sinon, $n_0 < x, \forall x \in A$, entraînant $n_0 + 1 \leq x$, $\forall x \in A$, c'est à dire $n_0 + 1 \in E$, c'est une contradiction. Par suite, $n_0 \in A$. Comme n_0 est un minorant de A, c'est le plus petit élément de A. ■

Théorème 3.17. *Toute partie non vide majorée* E *de* $\mathbb{N}$ *est finie et possède un plus grand élément.*

PREUVE. Considérons l'ensemble $F \subset \mathbb{N}$ des majorants de E. Alors F possède un plus petit élément m. Montrons que $m \in E$. Sinon, $\forall n \in E$, $n < m$. Il en résulte que $m - 1$ est un majorant de E, une contradiction. Donc $m \in E$ et on a $E \subset \{0, 1, \ldots, m\}$. Par conséquent E est fini. ■

Théorème 3.18. *Toute suite décroissante* x_n *dans* $\mathbb{N}$ *est stationnaire. i.e. il existe* $n_0 \in \mathbb{N}$, *tel que* $x_n = x_{n_0}$, $\forall n \geq n_0$

PREUVE. Par l'absurde, supposons que la suite n'est pas stationnaire, alors $\forall k$, il existe $n > k$ tel que $x_k > x_n$. Par conséquent il est possible de construire une suite $x_{k_0} > x_{k_1} > , \ldots, > x_{k_s} > \ldots$ strictement décroissante. L'ensemble $E = \{x_k : k \in \mathbb{N}\}$ est alors une partie infinie de $\mathbb{N}$ majorée par x_0. Contradiction. ■

Théorème 3.19. *(division euclidienne) Soient* $a, b \in \mathbb{Z}$, *avec* $b \neq 0$. *Alors il existe* $q, r \in \mathbb{Z}$, *uniques tels que* $a = bq + r$ *et* $0 \leq r < |b|$.
q *et* r *sont appelés respectivement* **quotient** *et* **reste** *de* **la division euclidienne** *de* a *par* b.

PREUVE. Soit $E = \{a - bs \in \mathbb{N} : s \in \mathbb{Z}\} \cap \mathbb{N}$, $E \neq \varnothing$. Donc E possède un plus petit élément r. Montrons que $r < |b|$.
► Si $b > 0$ et $r > b$, on a $a - b(q + 1) = a - bq - b = r - b > 0$. Donc $a - b(q + 1) \in E$ et $a - b(q + 1) < r$ ce qui contredit la minimalité de r.
► Si $b < 0$ et $r > -b$, on a $a - b(q - 1) = a - bq + b = r + b > 0$. Donc $a - b(q - 1) \in E$ et $a - b(q - 1) < r$ ce qui contredit la minimalité de r.
Unicité : Supposons que $a = bq + r = bq' + r'$ et $0 \leq r, r' < |b|$. Supposons que $r \neq r'$. On peut supposer que $r < r'$, alors $b(q - q') = r' - r$. Donc $|b| \mid r' - r$, par suite, $|b| \leq r' - r$. Comme $r' - r \leq r'$, il en résulte que $|b| \leq r'$, ce qui est absurde. Donc $r = r'$ et par conséquent $q = q'$. ■

Exemple 3.20. Le quotient et le reste de la division euclidienne de -23 par 6 sont - 4 et 1, car $-23 = 6 \cdot -4 + 1$.

4 Arithmétique dans $\mathbb{Z}$

4.1 Relation de divisibilité

Définition 4.1. (Rappel) Soient $a, b \in \mathbb{Z}$, on dit que a **divise** b ou que a est un **diviseur** de b ou que b est un **multiple** de a, et on note $a \mid b$, s'il existe $q \in \mathbb{Z}$, tel que $b = aq$.
Si $a \neq 0$, l'entier q est alors unique et il est noté $\frac{b}{a}$, c'est le **quotient** de b par a.
► Pour tout $n \in \mathbb{Z}$, On pose $n\mathbb{Z} = \{kn \in \mathbb{Z} : k \in \mathbb{Z}\}$, l'ensemble des multiples de n.

Proposition 4.2.
1 - $a \mid b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$.
2 - $\forall a \in \mathbb{Z}$, $a|a$.
3 - $\forall a, b \in \mathbb{Z}$, $a|b$ *et* $b|a \Rightarrow b = \pm a$.
4 - $\forall a, b, c \in \mathbb{Z}$, $a|b$ *et* $b|c \Rightarrow a|c$.
5 - La relation de divisibilité est une relation d'ordre partiel dans $\mathbb{N}$.
6 - $\forall a, b, c \in \mathbb{Z}$, *si* $a|b$ *et* $a|c$ *alors* $\forall \alpha, \beta \in \mathbb{Z}$, $a|\alpha b + \beta c$.
7 - Si $a \mid b$ *et* b *est non nul, alors* $|a| \leq |b|$. *En particulier, l'ensemble des diviseurs de* b *est fini.*

► On note $\mathcal{D}_a$, l'ensemble des diviseurs positifs de a.

Exemple 4.3. $\mathcal{D}_{12} = \{1, 2, 3, 4, 6, 12\}$.

Proposition 4.4. *Soient* $a, b \in \mathbb{Z}$, *avec* $b \neq 0$, *alors* $b \mid a \Leftrightarrow$ *le reste de la division euclidienne de* a *par* b *est égal à 0.*

4.2 PGCD et PPCM

Définition 4.5. Soient a, b deux entiers naturels non nuls.
On appelle PGCD de a et b noté $a \wedge b$, le plus grand élément de $\mathcal{D}_a \cap \mathcal{D}_b$.
On appelle PPCM de a et de b le plus petit multiple strictement positif commun à a et à b, qu'on note $m \vee n$.
Généralisation : Soient $a_1, a_2, \ldots, a_n$ des entiers naturels non nuls :
Le PGCD de la famille $a_1, a_2, \ldots, a_n$, qu'on note $a_1 \wedge a_2 \wedge \ldots \wedge a_n$, est le plus grand élément de $\mathcal{D}_{a_1} \cap \mathcal{D}_{a_2} \cap \ldots \mathcal{D}_{a_n}$.
Le PPCM noté $a_1 \vee a_2 \vee \ldots \vee a_n$ est le plus petit élément de $a_1\mathbb{N}^* \cap a_2\mathbb{N}^* \cap \ldots \cap a_n\mathbb{N}^*$.

Remarque 4.6. On définit le PGCD et le PPCM d'entiers relatifs comme étant le PGCD et le PPCM de leurs valeurs absolues.

Définition 4.7. Deux entiers a et b sont dits **premiers entre eux**, si les seuls diviseurs de a et b sont 1 et -1. C'est à dire $a \wedge b = 1$

Exemples 4.8.
1. $\mathcal{D}_{12} = \{1, 2, 3, 4, 6, 12\}$, $\mathcal{D}_{15} = \{1, 3, 5, 15\}$. $\mathcal{D}_{12} \cap \mathcal{D}_{15} = \{1, 3\}$. Donc On a $12 \wedge 15 = 3$.
$12\mathbb{N}^* = \{12, 24, 36, 48, 60, 72, \ldots\}$, $15\mathbb{N}^* = \{15, 30, 45, 60, 75, 90, \ldots\}$. On a $12\mathbb{N}^* \cap 15\mathbb{N}^* = \{60, \ldots\}$, donc $12 \vee 15 = 60$.
2. $\mathcal{D}_{12} = \{1, 2, 3, 4, 6, 12\}$, $\mathcal{D}_{35} = \{1, 5, 7, 35\}$. On a $\mathcal{D}_{12} \cap \mathcal{D}_{35} = \{1\}$. Par conséquent 12 et 35 sont premiers entre eux.

Proposition 4.9. *Soient* a, b *deux entiers naturels non nuls, alors :*
1 - $a \wedge b = d \Leftrightarrow d \in \mathcal{D}_a \cap \mathcal{D}_b$, et $\forall c \in \mathcal{D}_a \cap \mathcal{D}_b$, on a $c \mid d$.
2 - $a \wedge b = a \Leftrightarrow a \vee b = b \Leftrightarrow a \mid b$

Théorème 4.10. *Soient a, b deux entiers naturels non nuls, alors :*
1 - $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.
2 - $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

PREUVE.
1 - Posons $H = a\mathbb{Z} + b\mathbb{Z} = \{z = ax + by : x, y \in \mathbb{Z}\}$, alors H est un sous-groupe de $(\mathbb{Z}, +)$. D'après la caractérisation des sous-groupes de $(\mathbb{Z}, +)$, il existe $c \in \mathbb{N}$, tel que $H = c\mathbb{Z}$. Montrons que c est égal à d le PGCD de a et b.
D'une part en posant $x = 1$ et $y = 0$, on obtient $a \in c\mathbb{Z}$, donc $c \mid a$. D'autre part, en prenant $x = 0$ et $y = 1$, on obtient $b \in c\mathbb{Z}$, donc $c \mid b$. Il en résulte que $c \mid d$.
Réciproquement, on a $d \mid a$ et $d \mid b$. Donc $a \in d\mathbb{Z}$ et $b \in d\mathbb{Z}$, par suite $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$, d'où $c\mathbb{Z} \subset d\mathbb{Z}$, ce qui implique que $d \mid c$.
2 - Posons $G = a\mathbb{Z} \cap b\mathbb{Z}$. On a G est un sous-groupe de $\mathbb{Z}$, car intersection de deux sous-groupes. Il existe $s \in \mathbb{N}$, tel que $G = s\mathbb{Z}$. Montrons que $m = s$. On a $s \in a\mathbb{Z}$ et $s \in b\mathbb{Z}$, donc $a \mid s$ et $b \mid s$, d'où $m \mid s$.
Réciproquement, puisque $m \in a\mathbb{Z}$ et $m \in b\mathbb{Z}$, on a $m \in a\mathbb{Z} \cap b\mathbb{Z} = s\mathbb{Z}$, d'où $s \mid m$. ■

Corollaire 4.11. *Soient a, b deux entiers et $d = a \wedge b$. Alors il existe $u, v \in \mathbb{Z} : ua + vb = d$.*

Théorème 4.12. *(Bézout) Soient $a, b \in \mathbb{Z}$, alors a et b sont premiers entre eux, si et seulement si, il existe $\alpha, \beta \in \mathbb{Z}$: $\alpha a + \beta b = 1$.*

PREUVE. Supposons que $a \wedge b = 1$, alors d'après le corollaire 4.11, il existe $\alpha, \beta \in \mathbb{Z}$: $\alpha a + \beta b = a \wedge b = 1$.
Réciproquement, si'il existe $\alpha, \beta \in \mathbb{Z} : \alpha a + \beta b = 1$, alors $a \wedge b \mid \alpha a + \beta b = a \wedge b = 1$. Donc $a \wedge b = 1$. ■

Exemple 4.13.
Montrons que $\forall n \in \mathbb{Z}$, $x = 11n + 5$ et $y = 9n + 4$ sont premiers entre eux. Soit d un diviseur commun à x et à y. On a $d \mid 9x - 11y = 45 - 44 = 1$

Proposition 4.14.
1 - Soient $a, b, c \in \mathbb{N}^*$, alors $ac \wedge bc = c(a \wedge b)$.
2 - Soient $a, b \in \mathbb{N}^*$ et $s \in \mathcal{D}_a \cap \mathcal{D}_b$. Alors $\frac{a}{s} \wedge \frac{b}{s} = \frac{a \wedge b}{s}$.
3 - Soient $a, b \in \mathbb{N}^*$ et $d \in \mathcal{D}_a \cap \mathcal{D}_b$. Alors : $a \wedge b = d \Leftrightarrow \frac{a}{d} \wedge \frac{b}{d} = 1$.

PREUVE.
1 - Posons $d = a \wedge b$. On a $cd \mid ac$ et $cd \mid bc$. Donc $cd \mid ac \wedge bc$. Réciproquement, soient $\alpha, \beta \in \mathbb{Z} : d = \alpha a + \beta b$. Donc $dc = \alpha ac + \beta bc$. Par suite $dc \mid ac \wedge bc$.
2 - Posons $d = a \wedge b$. Alors $s \mid d$ et $\frac{d}{s} \mid \frac{a}{s} \wedge \frac{b}{s}$. Réciproquement, il existe $u, v \in \mathbb{Z} : ua + vb = d$. Donc $u\frac{a}{s} + v\frac{b}{s} = \frac{d}{s}$, par suite $\frac{a}{s} \wedge \frac{b}{s} \mid \frac{d}{s}$.
3 - En utilisant 2, $a \wedge b = d \Leftrightarrow \frac{a \wedge b}{d} = 1 \Leftrightarrow \frac{a}{d} \wedge \frac{b}{d} = 1$. ■

Proposition 4.15. *Soient $a, b_1, \ldots, b_n \in \mathbb{N}^*$. On suppose que $\forall k = 1, \ldots, n$ $a \wedge b_k = 1$, alors $a \wedge (b_1 b_2 \cdots b_n) = 1$*

PREUVE. Il suffit de montrer le résultat pour $n = 2$ et procéder par récurrence. Supposons que $a \wedge b_1 = a \wedge b_2 = 1$. $\alpha a + \beta b_1 = 1$. Donc $\alpha a b_2 + \beta b_1 b_2 = b_2$. Il existe $u, v \in \mathbb{Z} : ua + vb_2 = 1$, donc $ua + v(ab_2 + v\beta b_1 b_2) = 1$, $(u + b_2)a + v\beta b_1 b_2 = 1$, d'où $a \wedge b_1 b_2 = 1$ ■

Corollaire 4.16. *Soient $a, b \in \mathbb{N}$ premiers entre eux, alors $\forall m, n \in \mathbb{N}$, a^m et b^n sont premiers entre-eux.*

Théorème 4.17. *(Gauss) Soient a, b, c tois entiers tels que $a \mid bc$ et $a \wedge b = 1$. Alors $a \mid c$.*

PREUVE. $\alpha a + \beta b = 1$. Donc $\alpha ac + \beta bc = c$. Comme $a \mid ac$, et $a \mid \beta bc$, on a $a \mid c$. ■

Théorème 4.18. *Soient $a_1, a_2, \ldots, a_n$ des entiers premiers entre eux deux à deux. Si $a_i \mid b$, $\forall i = 1, \ldots, n$, alors $a_1 \cdot a_2 \cdot \ldots \cdot a_n \mid b$.*

PREUVE. on montre le résultat pour $n = 2$ et on procéde par récurrence sur n. On a $b = c_1 a_1 = c_2 a_2$. Donc $a_1 \mid c_2 a_2$. Comme $a_1 \wedge a_2 = 1$, on a d'après le théorème de Gauss, $a_1 \mid c_2$. Donc $c_2 = d_2 a_1$ et $b = d_2 a_1 a_2$. Par conséquent, $a_1 a_2 \mid b$ ■

Proposition 4.19. *Soient $a, b \in \mathbb{N}^*$, alors $(a \vee b) \times (a \wedge b) = ab$*

PREUVE. Posons $a = a'd$ et $b = b'd$. Alors $a' \wedge b' = 1$. On a $a'b'd = a'b = ab'$. Donc $m \mid a'b'd$. Réciproquement, posons $m = xa = yb$. Donc $xa' = yb'$. Par conséquent $a' \mid yb'$. Or $a' \wedge b' = 1$, donc d'après le théorème de Gauss, $a' \mid y$. On a aussi $b' \mid x$. Posons $y = ka'$, on a $m = ka'b = ka'b'd$. par suite, $a'b'd \mid m$, d'où $m = a'b'd$. $md = a'db'd = |ab|$

Corollaire 4.20. *Soient $a, b \in \mathbb{N}$, alors $a \wedge b = 1 \Leftrightarrow a \vee b = ab$* ■

4.3 Algorithme d'Euclide

Lemme 4.21. *Soient $a, b, q \in \mathbb{Z}$. Alors $a \wedge b = b \wedge (a - bq)$.*

PREUVE. Posons $d = a \wedge b$ et $d' = b \wedge (a - bq)$. On a $d \mid a$ et $d \mid b$, donc $d \mid b$ et $d \mid (a - bq)$, il s'ensuit que $d \mid d'$.
Réciproquement, $d' \mid b$ et $d' \mid (a - bq)$. Donc $d' \mid b$ et $d' \mid bq + (a - bq) = a$. D'où $d' \mid d$. ■

Théorème 4.22. *(Algorithme d'Euclide) :*
Soient $a, b \in \mathbb{N}$. On définit la suite d'entiers positifs $r_0, r_1, \ldots$, par :
$r_0 = a$, $r_1 = b$.
On suppose r_{n-2} et r_{n-1} définis :
Si $r_{n-1} = 0$ on pose $r_n = 0$.
Si $r_{n-1} \neq 0$, on définit r_n comme étant le reste de la division euclidienne de r_{n-2} par r_{n-1}.
Alors :
1 - *Il existe k tel que $r_k = 0$.*
2 - *Le dernier reste non nul est égal au PGCD de a et b.*

PREUVE.
1 - La suite r_k est décroissante dans $\mathbb{N}$, donc elle est stationnaire. Il existe $n \in \mathbb{N}$, tel que $r_n = r_k, \forall k > n$. On a en particulier, $r_n = r_{n+1}$, donc $r_{n+2} = 0$.
2 - Soit r_n le dernier reste non nul. D'après le lemme, on a $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{n-1} \wedge r_n$, comme $r_{n+1} = 0$, on a $r_n \mid r_{n-1}$, ce qui implique que $r_{n-1} \wedge r_n = r_n$. D'où $a \wedge b = r_n$. ■

Exemple 4.23. Soit à déterminer le PGCD de 1386 et 1274

a	b	r	q
1386	1274	112	1
1274	112	42	11
112	42	28	2
42	28	14	1
28	14	0	2

Le dernier reste non nul est 14, c'est le PGCD cherché.

L'algorithme d'Euclide permet aussi de déterminer les entiers u, v tels que $ua + vb = a \wedge b$, appelés les coefficients de Bézout.

Théorème 4.24. *(Algorithme d'Euclide étendu :Détermination des coefficients de Bézout) Soient $a, b \in \mathbb{Z}$. On note :*
$r_0 = a$, $r_1 = b$.
Si r_k et q_k sont respectivement le quotient et le reste de la division euclidienne de r_{k-2} par r_{k-1}
On définit les suites u_k et v_k par :
$u_0 = 1, u_1 = 0$ *et* $u_k = u_{k-2} - q_k u_{k-1}$
$v_0 = 0, v_1 = 1$ *et* $v_k = v_{k-2} - q_k v_{k-1}$
Alors $u_k a + v_k b = r_k$ en particulier, si r_n est le dernier reste non nul, alors $u_n a + v_n b = r_n = a \wedge b$

Preuve. On montre par récurrence sur k que $u_k a + v_k b = r_k$.
Si $k = 0$, on a $u_0 = 1$ et $v_0 = 0$, $u_0 a + v_0 b = a = r_0$.
Si $k = 1$, on a $u_1 = 0$ et $v_1 = 1$, $u_1 a + v_1 b = b = r_1$.
La relation est donc vérifiée pour $k = 0$ et $k = 1$.
Soit $k \geq 2$. Supposons la relation vraie pour $k-1$ et $k-2$. On a :
$u_k a + v_k b = u_{k-2} - q_k u_{k-1} a + v_{k-2} - q_k v_{k-1} b = (u_{k-2} a + v_{k-2} b) - q_k (u_{k-1} a + v_{k-1} b = r_{k-2} - q_k r_{k-1} = r_k$ ■

Exemple 4.25. Déterminons le PGCD et des coefficients de Bézout pour le couple $(224, 175)$

a	b	r	q		
224	175	49	1	49=224-175	49=224-175
175	49	28	3	$28 = 175 - (49 \times 3) = 175 - (224 - 175) \times 3$	$28 = (4 \times 175) - (3 \times 224)$
49	28	21	1	$21 = 49 - 28 = (224 - 175) - ((4 \times 175) - (3 \times 224))$	$21 = (4 \times 224) - (5 \times 175)$
28	21	7	1	$7 = 28 - 21 = (4 \times 175) - (3 \times 224) - (4 \times 224) + (5 \times 175)$	$7 = (9 \times 175) - (7 \times 224)$
21	7	0	3	Fin	

On a donc $224 \wedge 175 = 7$ et $7 = (9 \times 175) - (7 \times 224)$

4.4 L'équation $ax + by = c$ dans $\mathbb{Z}$

Théorème 4.26. *L'équation $ax + by = c$ possède une solution, si et seulement si, $(a \wedge b) \mid c$. Lorsque cette condition est satisfaite, et si (x_0, y_0) est une solution particulière de l'équation, alors tout autre solution (x, y) est de la forme $x = x_0 + kb'$ et $y_0 - ka'$, $k \in \mathbb{Z}$, où $a' = \dfrac{a}{a \wedge b}$ et $b' = \dfrac{b}{a \wedge b}$.*

Pour déterminer une solution particulière, on utilise l'algorithme d'Euclide pour déterminer des coeficients de Bézout (u, v) du couple (a, b). On a alors $au + bv = d = a \wedge b$. On pose $h = \dfrac{c}{d}$, alors $(x_0, y_0) = (uh, vh)$ est une solution particulière de l'équation.

Exemple 4.27. Soit à résoudre l'équation $224x + 175y = 21$. On a $224 \wedge 175 = 7 \mid 21$, donc l'équation possède des solutions. On a d'après l'éxemple précédent, $-(7 \times 224) + (9 \times 175) = 7$. Donc $(-21 \times 224) + (27 \times 175) = 21$. Une solution particulière est donc $(-21, 27)$. $a' = \dfrac{224}{7} = 32$, $b' = \dfrac{175}{7} = 25$. La solution générale de l'équation est $(x, y) = (-21 + 25k, 27 - 32k)$, $k \in \mathbb{Z}$.

4.5 Nombres premiers et factorisation

Définition 4.28. Un nombre entier naturel p est dit **premier**, s'il est différent de 1 et ses seuls diviseurs positifs sont 1 et p.

Exemple 4.29. 2, 3, 5, 7, ... sont premiers. 1, 9, 15 ne sont pas premiers.

Théorème 4.30. *Tout entier > 1 est divisible par un nombre premier.*

PREUVE. Soit $n > 1$ et A l'ensemble des entiers > 1 qui divisent n. A est une partie non vide de $\mathbb{N}$ ($n \in A$), donc A possède un plus petit élément p. Montrons que p est premier. Soit $d > 1$ un diviseur de p. On a $d \leq p$. Or $d \mid n$. D'où, par minimalité de p, $d = p$. ■

Théorème 4.31. *(Euclide) Il existe une infinité de nombres premiers.*

PREUVE. Soit p un nombre premier. Posons $n = p! + 1$. Alors n est divisible par un nombre premier q. Montrons que $q > p$. Raisonnons par l'absurde et supposons que $q \leq p$ alors $q \mid p!$, comme $q \mid p! + 1$, on a $q \mid n - p! = 1$, ce qui est absurde. Donc $q > p$. Ainsi pour tout nombre premier p, il existe un nombre premier q strictement plus grand que p. ■

Remarque 4.32. Les nombres premiers forment une suite d'entiers. A l'heure actuelle, on connait très peu de choses sur cette suite.

Proposition 4.33. *Soit p est un nombre premier et $n \in \mathbb{Z}$, alors ou bien $p \mid n$ ou bien $p \wedge n = 1$.*

PREUVE. Supposons $p \nmid n$ et soit $d = p \wedge n = 1$. Comme $d \mid p$, on a $d = 1$ ou p.
Supposons que $d = p$, alors $p \mid n$. Absurde. Donc $d = 1$. ■

Corollaire 4.34. *Soit p un nombre premier et $a_1, a_2, \ldots, a_n$ des entiers tels que $p \mid a_1 \cdot a_2 \cdot \ldots \cdot a_n$. Alors il existe i tel que $p \mid a_i$.*

PREUVE. Par contraposition. Supposons que $\forall i$, $p \nmid a_i$, alors $\forall i$, $p \wedge a_i = 1$, ce qui implique que $p \wedge (a_1 a_2 \cdots a_n) = 1$ et par suite $p \nmid (a_1 a_2 \cdots a_n)$ ■

Théorème 4.35. *Pour tout entier naturel $a > 1$, il existe des nombres premiers $p_1 < p_2 < \ldots < p_k$, des entiers naturels non nuls $m_1, m_2, \ldots, m_k$ tels que a s'écrit de manière unique sous la forme $a = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$.*

PREUVE. Existence par récurrence. Si n est premier, il n'y a rien à démontrer. Si n n'est pas premier, alors il divisible par par un nombre premier p. Soit p_1 le plus petit nombre premier divisant n. Soit $p_1^{m_1}$ la plus grande puissance de p_1 divisant a. On pose $b = a/p_1^{m_1}$. On a $p_1 \wedge n = 1$ et $b < a$, on applique alors l'hypothèse de récurrence à b. On a alors $b = p_2^{m_2} \ldots p_k^{m_k}$, d'où le résultat.

Unicité, par récurrence, si $a = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} = q_1^{s_1} q_2^{s_2} \ldots q_t^{s_t} \in \mathbb{N}$. D'après le choix de p_1 et q_1 on a $p_1 = q_1$. Donc l'égalité devient $p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} = p_1^{s_1} q_2^{s_2} \ldots q_t^{s_t}$. On applique alors l'hypothèse de récurrence à a/p_1. ■

Exemple 4.36. $1260 = 2 \cdot 630 = 2^2 \cdot 315 = 2^2 \cdot 3 \cdot 105 = 2^2 \cdot 3^2 \cdot 35 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$.

Remarque 4.37. : Alors qu'on connait des algorithmes assez rapides pour tester si un nombre très grand est premier ou non, il n'existe pas avec les ordinateurs actuels de méthode suffisament rapide pour factoriser des nombres de quelques centaines de chiffres.
Cette propriété (difficulté de la factorisation), est utilisée dans certains procédés cryptographiques (méthode RSA) : mots de passe dans les réseaux informatiques, messages secrets, etc....

Proposition 4.38. *Soient $p_1, p_2, \dots p_k$ des nombres premiers distincts et α_i, β_i, $i = 1, \dots, k$, des entiers naturels eventuellement nuls. Alors*
$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \mid p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \Leftrightarrow \forall i = 1, 2, \dots, k, \alpha_i \leq \beta_i$

PREUVE.
$\Rightarrow$ Puisque $p_i \wedge p_j = 1, \forall i \neq j$, on a $p_i^{\alpha_i} \mid p_i^{\beta_i}$, ce qui entraîne $\alpha_i \leq \beta_i$.
$\Leftarrow$ est claire. ■

La factorisation permet de déterminer le PGCD et le PPCM de deux entiers. On a le :

Théorème 4.39. *Si $a = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ et $b = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$, où $s_i, t_i \in \mathbb{N}$ (eventuellement nuls), alors :*
$a \wedge b = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$ *où* $l_i = \min(s_i, t_i)$.
$a \vee b = p_1^{h_1} p_2^{h_2} \dots p_k^{h_k}$ *où* $h_i = \max(s_i, t_i)$

PREUVE.
1 - On a $l_i \leq \alpha_i$ et $_i \leq \beta_i$. Donc $p_i^{l_i} \mid a$ et $p_i^{l_i} \mid b$. Par suite, $p_i^{l_i} \mid a \wedge b$, comme les $p_i^{l_i}$ sont premiers entre eux deux à deux, il s'ensuit que $p_1^{l_1} p_2^{l_2} \dots p_k^{l_k} \mid a \wedge b$.
Réciproquement, si $c \mid a$ et $c \mid b$, alors $c = p_1^{u_1} p_2^{u_2} \dots p_k^{u_k}$ avec $u_i \leq s_i$ et $u_i \leq t_i$, par suite $u_i \leq l_i$, $\forall i$. Donc $c \mid p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$.

2 - Remarquons que $\min(s_i, t_i) + \max(s_i, t_i) = s_i + t_i$. Alors on a $a \vee b = \dfrac{ab}{a \wedge b} = \prod_{i=1}^{k} p_i^{s_i + t_i - \min(s_i, t_i)} = \prod_{i=1}^{k} p_i^{\max(s_i, t_i)}$ ■

Exemple 4.40. $180 = 2^2 \cdot 3^2 \cdot 5$, $42 = 2 \cdot 3 \cdot 7$. On a : $180 \wedge 42 = 2 \cdot 3 = 6$, $180 \vee 42 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$.

5 L'anneau $\mathbb{Z}/n\mathbb{Z}$, et arithmétique modulaire

5.1 Relation de congruence

Soit n un entier naturel non nul. On définit dans $\mathbb{Z}$ la relation de **congruence modulo** n par

$$x \equiv y\ [n] \Leftrightarrow n \mid x-y \Leftrightarrow \exists k \in \mathbb{Z} : x-y = k \cdot n$$

En particulier, $x \equiv 0\ [n] \Leftrightarrow n \mid x$

Théorème 5.1.
1 - La relation de congruence modulo n est une relation d'équivalence dans $\mathbb{Z}$.
2 - Pour tout $x \in \mathbb{Z}$, la classe de x modulo n est l'ensemble $\bar{x} = \{x+kn \in \mathbb{Z} : k \in \mathbb{Z}\} = x+k\mathbb{Z}$.
3 - L'ensemble quotient par cette relation d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$, et on a $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

Preuve.
1 - Montrons que la relation de congruence modulo n est une relation d'équivalence :
La relation $\equiv$ est réflexive, car $\forall x \in \mathbb{Z}$, $n \mid x-x = 0$.
La relation $\equiv$ est symétrique, car $\forall x, y \in \mathbb{Z}$, s $n \mid x-y$, alors $n \mid y-x$.
La relation $\equiv$ est transitive, car $\forall x, y, z \in \mathbb{Z}$, $n \mid x-y$ et $n \mid y-z$ implique $n \mid (x-y)+(y-z) = x-z$.
2 - $y \in \bar{x} \Leftrightarrow n \mid y-x \Leftrightarrow \exists k \in \mathbb{Z} : y = x+kn \Leftrightarrow y \in x = n\mathbb{Z}$.
3 - On a $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\} \subset Z/n\mathbb{Z}$.
Réciproquement, soit $\bar{x} \in Z/n\mathbb{Z}$. La division euclidienne de x par n donne $x = qn+r$, où $0 \leq r \leq n-1$. On a alors $x \equiv r[n]$. Donc $\bar{x} = \bar{r} \in \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.
Enfin, si $0 \leq k, m \leq m-1$, et $\bar{k} = \bar{m}$, alors $0 \leq |k-m| \leq n-1$. Comme $n \mid k-m$, on a $k-m = 0$, d'où $k = m$. Le cardinal de $Z/n\mathbb{Z}$ est donc égal à n. ■

Théorème 5.2. *Sur $\mathbb{Z}/n\mathbb{Z}$ on définit les opérations $+$ et $\cdot$ suivantes $\forall \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}$:*

$$\bar{x} + \bar{y} = \overline{x+y}$$
$$\bar{x} \cdot \bar{y} = \overline{xy}$$

Alors ces opérations sont bien définies et $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

Preuve.
► $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien :
Associativité : $\forall x, y, z \in \mathbb{Z}$, on a :
$(\overline{x}+\overline{y})+\overline{z} = \overline{(x+y)+z} == \overline{x+(y+z)} = \overline{x}+\overline{y+z} = \overline{x}+(\overline{y}+\overline{z})$.
Commutativité : $\forall x, y \in \mathbb{Z}$, $\overline{x}+\overline{y} = \overline{x+y} = \overline{y+x} = \overline{y}+\overline{x}$.
Element neutre : $\overline{0}$ est l'élément neutre de $+$. $\forall x \in \mathbb{Z}$, $\overline{x}+\overline{0} = \overline{x}$.
Elements symétrisables : $\forall x \in \mathbb{Z}$, $\overline{x}+\overline{-x} = \overline{x+(-x)} = \overline{0}$.
► $(\mathbb{Z}/n\mathbb{Z}, \times)$ est un monoïde commutatif :
Associativité : $\forall x, y, z \in \mathbb{Z}$, on a :
$(\overline{x} \times \overline{y}) \times \overline{z} = (\overline{x \times y \times z}) = \overline{x \times y \times z} = \overline{x} \times \overline{y \times z} = \overline{x} \times (\overline{y} \times \overline{z})$.
Commutativité : $\forall x, y \in \mathbb{Z}$, $\overline{x} \times \overline{y} = \overline{x \times y} = \overline{y \times x} = \overline{y} \times \overline{x}$.
Elément neutre : $\overline{1}$ est l'élément neutre de $\times$. $\forall x \in \mathbb{Z}$
$\overline{x} \times \overline{1} = \overline{x \times 1} = \overline{x}$.
► La loi $\times$ est distributive par rapport à $+$.
$\forall x, y, z \in \mathbb{Z}$, $\overline{x} \times (\overline{y}+\overline{z}) = \overline{x} \times (\overline{y+z}) = \overline{xy+xz} = \overline{xy}+\overline{xz} = (\overline{x} \times \overline{y})+(\overline{x} \times \overline{z})$ ■

Corollaire 5.3. *Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ alors : $\forall k \in \mathbb{N}$, $a^k \equiv b^k$*

On rappelle que dans $\mathbb{Z}/n\mathbb{Z}$, on a $n \mid m \Leftrightarrow \bar{m} = \bar{0}$, cette remarque permet parfois de traiter les questions de divisibilité d'une façon plus simple, en utilisant les propriétés de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

Exemple 5.4. Montrons que $\forall n \in \mathbb{N}$, on a $7 \mid 3^{2n+1} + 2^{n+2}$.

Posons $u_n = 3^{2n+1} + 2^{n+2}$. Dans $\mathbb{Z}/7\mathbb{Z}$, on a $\bar{u}_n = \bar{3}^{2n+1} + \bar{2}^{n+2} = \bar{9}^n \cdot \bar{3} + \bar{2}^n \cdot \bar{4}$.

Or $\bar{9} = \bar{2}$, donc $\bar{u_n} = \bar{2}^n \cdot \bar{3} + \bar{2}^n \cdot \bar{4} = \bar{2}^n \cdot (\bar{3} + \bar{4}) = \bar{0}$.

Exponention rapide. dans certaines applications de l'arithmétique modulaire, par exemple en cryptographie, on a besoin de calculer les puissances $a^k[n]$, où k est un très grand nombre entier naturel. Alors on procède de la façon suivante :
1 - On décompose k en base 2, i.e. $k = \sum_{i=0}^{m} \epsilon_i 2^i$, où $\epsilon_i \in \{0, 1\}$.
2 - On calcule $a_i = a^{2^i}[n]$, en utilisant la relation de récurrence $a_{i+1} = (a_i)^2[n]$.
3 - $a^k = \prod_{i:\epsilon_i \neq 0} a_i[n]$.

Exemple 5.5. Calculons $6^{73}[100]$ On a $73 = 64 + 8 + 1 = 1 + 2^3 + 2^6$.
$6^2 = 36[100]$, $6^4 = 36^2 = -4[100]$, $6^8 = (-4)^2 = 16[100]$, $6^{16} = 56[100]$, $6^{32} = 56^2 = 36[100]$, $6^{64} = 36^2 = -4 = 96[100]$. Donc $6^{73} = 6 \times 16 \times -4 = 16[100]$.

5.2 Le théorème des restes chinois

Théorème 5.6 (Théorème des restes chinois). *Soient $m_1, m_2, \ldots, m_s$ des entiers premiers entre eux deux à deux, $a_1, a_2, \ldots, a_s$ des entiers quelconques. Alors il existe au moins un entier x tel que $x \equiv a_i \mod m_i$, $\forall i = 1, \ldots, s$.*
Si x_0 est une solution, alors $\forall x \in \mathbb{Z}$, x est solution, si et seulement si, $m \mid x - x_0$, où $m = m_1 m_2 \ldots m_s$.
De plus, il existe une seule solution dans $\{0, 1, \ldots, m-1\}$

Preuve. Posons $m = m_1 m_2 \cdots m_s$ et $h_k = m/m_k$. Alors $\forall k = 1, 2, \ldots, s$, on a : $m_k \mid h_i$, si $i \neq k$. Par ailleurs, h_k et m_k sont premiers entre eux, donc il existe $u_k, v_k \in \mathbb{Z}$, tels que $u_k m_k + v_k h_k = 1$. Posons $a = \sum_{i=1}^{s} a_i v_i h_i$. Alors modulo m_k, on a

$$\bar{a} = \overline{\sum_{i=1}^{s} a_i v_i h_i} \tag{1}$$

Comme $m_k \mid k_i$, $\forall i \neq k$, on a :

$$\bar{a} = \overline{a_k v_k h_k} = \overline{a_k(1 - u_k m_k)} = \overline{a_k} \tag{2}$$

Exemple 5.7. Déterminons les entiers dont le reste de la division euclidienne par 7 est est 4 et le reste de la DE par 11 est 2.
En utilisant l'algorithme d'Euclide étendu, on a $4 = 11 - 7$, $3 = 7 - 4 = 7 - (11 - 7) = (2 \times 7) - 11$, $1 = 4 - 3 = (11 - 7) - (2 \times 7) + 11 = (2 \times 11) - (3 \times 7)$.
On pose alors $x = (2{\times}11{\times}4) - (3{\times}7{\times}2) = 88 - 42 = 46$. Donc 46 est une solution particulière.

5.3 Entiers inversibles modulo n

Définition 5.8. Soit $n \in \mathbb{N}^*$. Un entier $k \in Z$ est dit inversible modulo n, s'il existe $m \in \mathbb{Z}$ tel que $km \equiv 1$ modulo n.

On note $\mathbb{U}_n = \{k \in \mathbb{N} : k < n \text{ et } k \text{ est inversible modulo } n\}$. Le cardinal de $\mathbb{U}_n$ est noté $\phi(n)$, appelé l'indicatrice d'Euler de n.

Proposition 5.9.
Soit n un entier naturel non nul et k un entier, alors k est inversible modulo n, si et seulement si, k est premier avec n.

PREUVE.
Supposons que k est inversible modulo n. Alors il existe $m \in \mathbb{Z}$ tel que $km \equiv 1$ modulo n. i.e. $n \mid km - 1$. Donc il existe $s \in \mathbb{Z}$ tel que $sn = km - 1$, ou encore $mk - sn = 1$, ce qui entraîne que $k \wedge n = 1$.
Réciproquement, supposons $k \wedge n = 1$, d'après Bézout, il existe $m, s \in \mathbb{Z}$ tels que $mk + sn = 1$. Donc $n \mid mk - 1$. Par suite, $km \equiv 1$ modulo n. ■

Exemples 5.10.
$\mathbb{U}_{18} = \{1, 5, 7, 11, 13, 17\}$. $\phi(18) = 6$
$\mathbb{U}_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. $\phi(15) = 8$

Remarque 5.11. L'inverse de k modulo n est déterminé par l'algorithme d'Euclide. En effet, on a $ak + bn = 1$, donc $\overline{k}\overline{a} = \overline{1}$

Remarque 5.12. On peut résoudre le système de congruences dans le théorème chinois en calculant les inverses modulo n.

Exemple 5.13. Cherchons les entiers x dont le reste de la division euclidienne par 7 est 4 et le reste de la division euclidienne par 11 est 2. (voir exemple 5.7).
On a $x \equiv 4 \pmod 7$ et $x \equiv 2 \pmod{11}$. Comme 7 et 11 sont premiers entre eux, une solution existe d'après le théorème chinois.
On a $x = 7a + 4 = 11b + 2$. Donc $11b - 7a = 2$. Donc modulo 7, on a $11b \equiv 2$. Donc $b \equiv 4$, par suite $b = 7k + 4$.
Donc $x = 11 \times (7k + 4) + 2 = 46 + 77k$.

Théorème 5.14 (Euler). *$\forall a \in \mathbb{Z}$, premier avec n, alors $a^{\phi(n)} \equiv 1$ modulo n.*

PREUVE. Soit $a \in \mathbb{U}_n$. Pour tout $x \in \mathbb{U}_n$, on a $ax \wedge n = 1$. Notons $f(x)$ le reste de la division euclidienne de ax par n, alors $f(x) \in \mathbb{U}_n$. Considérons l'application $f : \mathbb{U}_n \to \mathbb{U}_n$, tel que $x \mapsto f(x)$. Montrons que f est injective. Soient $x, y \in \mathbb{U}_n$ tels que $f(x) = f(y)$, alors $n \mid ax - ay = a(x - y)$. Comme $n \wedge a = 1$, d'après le théorème de Gauss, on a $n \mid x - y$. Or $0 < x, y < n$, il en résulte que $x - y = 0$, donc $x = y$. Par conséquent f est injective. Comme $\mathbb{U}_n$ est fini, f est bijective.
Posons $\mathbb{U}_n = \{x_1, x_2, \ldots, x_m\}$, où $m = \phi(n)$, alors on a $f(x_1)f(x_2)\ldots f(x_m) \equiv x_1x_2\ldots x_m$ modulo n. Donc $a^m x_1x_2\ldots x_m \equiv x_1x_2\ldots x_m$ modulo n. Posons $y = x_1x_2\ldots x_m$, alors $n \mid y(1 - a^m)$. Comme $n \wedge y = 1$, il en résulte que $a^m \equiv 1$ modulo n.
Soit maintenant $a \in \mathbb{Z}$ quelconque premier avec n, on note k le reste de la division euclidienne de a par n. Alors $a = qn + k$, $k \in \mathbb{U}_n$. Alors puisque $a \equiv k$ modulo n, on a $a^{\phi(n)} \equiv k^{\phi(n)} \equiv 1$, modulo n. ■

Théorème 5.15 (Le petit théorème de Fermat). *Soit p un nombre premier. Alors $\mathbb{U}_p = \{1, 2, \ldots, p - 1\}$, $\phi(p) = p - 1$ et on a*

$$\forall a \in \mathbb{Z}, p \mid a^p - a$$

Définition 5.16. Soit $n \in \mathbb{N}^*$ et a un entier premier avec n. Alors le plus petit entier non nul k tel que $a^k \equiv 1$, modulo n est appelé **l'ordre multiplicatif** ou **période** de a modulo n. On le note $\text{ord}_n(a)$.

$$\text{ord}_n = \min\{k \in \mathbb{N}^* : n \mid a^k - 1\}$$

Exemples 5.17.
1 - Modulo 9, on a $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$. Donc $\text{ord}_9(2) = 6$.
2 - Modulo 15, on a $4^2 \equiv 1$. Donc Donc $\text{ord}_{15}(4) = 2$.

Théorème 5.18. *Soit $n \in \mathbb{N}^*$ et a un entier premier avec n. Si $k \in \mathbb{N}$, est tel que $a^k \equiv 1$ modulo n, alors $ord_n(a) \mid k$. En particulier, $ord_n(a) \mid \phi(n)$.*

PREUVE. Notons $d = \text{ord}_n(a)$ et soit r le reste de la division euclidienne de k par d. On a $k = qd + r$ avec $0 \leq r < m$ et $a^k \equiv (a^d)^q.a^r \equiv 1$ modulo n. Supposons que $r \neq 0$, on a $a^d \equiv 1$, par suite $a^r \equiv 1$ modulo n. D'où par minimalité de d, on a $d \leq r$. Une contradiction. par conséquent $r = 0$ et $d \mid k$. ■.

Exemple 5.19. Déterminons suivant les valeurs de n, le reste de la division euclidienne de $u_n = 7^{(7^n)}$ par 10.
Remarquons d'abord $7 \wedge 10 = 1$. Calculons l'ordre de 7 modulo 10. On a $7^2 = 49 \equiv 9[10]$, $7^3 \equiv 63 \equiv 3[10]$, $7^4 \equiv 21 \equiv 1[10]$. Donc l'ordre de 7 modulo 10 est égal à 4.
Posons $7^n = 4k + r$, alors $u_n \equiv 7^{4k+r} \equiv 7^r[10]$, où $r \in \{0, 1, 2, 3\}$.
Comme $7 \equiv 3[4]$, 7 est d'ordre 2 modulo 4. Par conséquent, on le résultat suivant
Si n est pair, $7^n \equiv 1[4]$, $7^n = 4k + 1$, $u_n \equiv 7^{4k+1} \equiv 7[10]$.
Si n est impair, $7^n \equiv 3[4]$, $7^n = 4k + 3$, $u_n \equiv 7^{4k+3} \equiv 3[10]$.
En conclusion, le reste de la division euclidienne de $7^{(7^n)}$ par 10 est égal à 7 si n est pair et égal à 3 si n est impair.

Proposition 5.20. *Soit $n \in \mathbb{N}^*$ et a un entier premier avec n dont l'ordre multiplicatif modulo n égal à d, alors*

$$\forall k \in \mathbb{N}, a^k \text{ est d'ordre } d \text{ modulo } n \iff k \wedge d = 1$$

PREUVE. Supposons que a^k est d'ordre d. Posons $m = \frac{d}{k \wedge d}$. On a $km = \frac{kd}{k \wedge d} = d\frac{k}{k \wedge d}$. Il en résulte que $d \mid km$, par suite $(a^k)^m \equiv 1$. Comme a^k est d'ordre d, on a $d \mid m = \frac{d}{k \wedge d}$. Ce qui implique $k \wedge d = 1$.
Supposons que $k \wedge d = 1$. On a $(a^k)^d \equiv 1$. Soit $m \in \mathbb{N}$, tel que $(a^k)^m \equiv 1$. On a $d \mid km$. Comme $k \wedge d = 1$, d'après le théorème de Gauss, $d \mid m$. ■.

Théorème 5.21. *(Propriétés de la fonction indicatrice d'Euler)*
1 - Soient $m_1, m_2, \ldots, m_k$ sont des entiers premiers entre eux deux à deux, alors

$$\phi(m_1 m_2 \cdots m_k) = \phi(m_1)\phi(m_2) \cdots \phi(m_k)$$

2 - Soient p un nombre premier et $k \in \mathbb{N}^*$. Alors

$$\phi(p^k) = p^k - p^{k-1}$$

en particulier, $\phi(p) = p - 1$
3 - Soient $n = \prod_{k=1}^{s} p^{\alpha_k}$ la factorisation de n en produit de nombres premiers. Alors

$$\phi(n) = \prod_{k=1}^{s} (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = n \prod_{k=1}^{s} (1 - \frac{1}{p_k})$$

4 - $\sum_{d \mid n} \phi(d) = n$.

PREUVE.
1 - Il suffit de montrer le résultat pour $k = 2$ et de procéder par récurrence. Posons $m = m_1m_2$, pour tout $n \in \mathbb{N}^*$, notons, comme d'habitude, $\mathbb{U}_n$, l'ensemble des entiers naturels $< n$ premiers avec n. Soit $x \in \mathbb{U}_m$, notons r_i le reste de la division euclidienne de x par m_i. On a $r_i = x - q_im_i$ et $m_i \wedge r_i = m_i \wedge q_im_i + r_i = m_i \wedge x$. Comme $m \wedge x = 1$, et $m = m_1m_2$, on a $m_i \wedge x = 1$, donc $r_i \in \mathbb{U}_{m_i}$.
Considérons alors l'application $f : \mathbb{U}_m \to \mathbb{U}_{m_1} \times \mathbb{U}_{m_2}$, $x \mapsto (r_1(x), r_2(x))$. où $r_i(x)$ est le reste de la division euclidienne de x par m_i. D'après le théorème des restes chinois, pour tout $(r_1, r_2) \in \mathbb{U}_{m_1} \times \mathbb{U}_{m_2}$, il existe $x \in \mathbb{N}$ unique tel que $x < m$ et $x \equiv r_i[m_i]$. Comme $x \wedge m_i = 1$, pour $i = 1, 2$, on a $x \wedge m = 1$ i.e. $x \in \mathbb{U}_m$. Il en résulte que et f est une bijection. Donc $\phi(m) = \text{card}(\mathbb{U}_m) = \text{card}(\mathbb{U}_{m_1})\text{card}(\mathbb{U}_{m_2}) = \phi(m_1)\phi(m_2)$.
2 - Soit $E = \{1, 2, \ldots, p^k\}$, $F = \{m \in E : m \wedge p^k = 1\}$, $G = \{m \in E : m \mid p^k\}$ On a $\phi(p^k) = \text{card}(F) = \text{card}(E) - \text{card}(G) = p^k - p^{k-1}$.
3 - Soit $n = \prod_{k=1}^{s} p_k^{\alpha_k}$ la factorisation de n en produit de nombres premiers. Alors :
$\phi(n) = \prod_{k=1}^{s} \phi(p_k^{\alpha_k}) = \prod_{k=1}^{s}(p_k^{\alpha_k} - p_k^{\alpha_k - 1}) = \prod_{k=1}^{s} p^{\alpha_k}(1 - \frac{1}{p_k}) = n\prod_{k=1}^{s}(1 - \frac{1}{p_k})$.
4 - Posons $E = \{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{k}{n}, \ldots \frac{n}{n} = 1\}$ et Pour tout $d \mid n$, $F_d = \{\frac{k}{d} : 1 \leq k \leq n, \text{et } k \wedge d = 1\}$.
Montrons que les $(F_d)_{d|n}$ forment une partition de E.
Montrons que $\bigcup_{d|n} F_d = E_n$.
Soit $d \mid n$ et $\frac{k}{d} \in F_d$. Posons $m = \frac{n}{d}$, on a $\frac{km}{dm} = \frac{km}{n} \in E$ car puisque $k \leq d$, $km \leq n$. d'où $F_d \subset E$ et $\bigcup_{d|n} F_d \subset E$.
Réciproquement, soit $\frac{k}{n} \in E$, posons $m = k \wedge n$, $k' = \frac{k}{m}$ et $d = \frac{n}{m}$. Alors $k' \wedge d = 1$ et $\frac{k'}{d} \in F_d$. D'où $E \subset \bigcup_{d|n} F_d$.
Montrons que les $(F_d)_{d|n}$ sont deux à deux disjoints. Supposons que $F_d \cap F_{d'} \neq \varnothing$, Soient $\frac{k}{d} = \frac{k'}{d'} \in F_d \cap F_{d'}$. Alors $kd' = k'd$. On a $d \mid kd'$ comme $k \wedge d = 1$, alors $d \mid d'$. De même on a $d' \mid d$. D'où $d = d'$ et $F_d = F'_d$. ■

Théorème 5.22. *Soit p un nombre premier. Alors pour tout $d \in \mathbb{N}$, l'équation $x^d \equiv 1$, modulo p possède au plus d solutions dans $\mathbb{U}_p$.*

PREUVE. Les solutions de l'équation $x^d \equiv 1$ modulo p sont les racines du polynôme $X^d - 1$ dans le corps $\mathbb{Z}/p\mathbb{Z}$. Le nombre des racines d'un polynôme sur un corps est toujours inférieur ou égal au degré du polynôme. ■

Théorème 5.23. *Soit p un nombre premier. Alors il existe un entier dont l'ordre multiplicatif est égal à $p - 1$*

PREUVE. Posons $n = p-1 = card(\mathbb{U}_p)$. Soit $d \mid n$, notons E_d l'ensemble des éléments d'ordre multiplicatif d dans $\mathbb{U}_p$. Nous allons montrer que $\text{card}(E_d) \leq \phi(d)$.
Tout élément a d'ordre d est solution de l'équation $a^d \equiv 1$ modulo p. Notons $\mathcal{R}_d$ l'ensemble de ces solutions. On a $E_d \subset \mathcal{R}_d$. D'après le Théorème 5.22, on a $\text{card}(E_d) \leq d$. Soit maintenant $a \in \mathbb{U}_p$ un élément d'ordre d. Notons $H = \{1, a, a^2, \ldots, a^{d-1}\}$ modulo p. Comme $(a^k)^d \equiv 1$ modulo p, on a $H \subset \mathcal{R}_d$. D'où $d = card(H) \leq \text{card}(\mathcal{R}_d) \leq d$. Donc $H = \mathcal{R}_d$. Il en résulte que $E_d \subset H$. Or, d'après la proposition 5.20, l'ordre multiplicatif de a^m est égal à d, si et seulement $d \wedge m = 1$. Il en résulte que $\text{card}(E_d) \leq \phi(d)$. Comme tout élément de $\mathbb{U}_p$ est d'ordre un diviseur d de n, on a $n = \sum_{d|n} \text{card}(E_d)$. Par conséquent $n = \sum_{d|n} \text{card}(E_d) \leq \sum_{d|n} \phi(d) = n$, donc $\sum_{d|n} \text{card}(E_d) = \sum_{d|n} \phi(d)$, ou encore $\sum_{d|n}(\phi(d) - \text{card}(E_d)) = 0$. Par suite, $\text{card}(E_d) = \phi(d)$, $\forall d \mid n$, en particulier $\text{card}(E_n) = \phi(n)$. D'où $\mathbb{U}_n$ contient un élément a d'ordre n. ■

Définition 5.24. Tout élément d'ordre $p-1$ modulo p est appelé **élément primitif modulo** p.

Exemple 5.25. Cherchons un élément primitif modulo 17. Cet élément doit avoir un ordre multiplicatif égal à 17-1=16.
Essayons avec 2. On a $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 = 16 \equiv -1$. Donc $2^8 \equiv -1^2 = 1$. D'où l'ordre multiplicatif de 2 est ≤ 8. Donc 2 n'est pas un élément primitif modulo 17.
Essayons avec 3. On a $3^2 = 9$, $3^3 = 10$, $3^4 = 13$, $3^5 = 5$, $3^6 = 15$, $3^7 = 11$, $3^8 = 16 = -1$.
Donc ordre(3) > 8, comme ordre(3) $\mid 16$, on a ordre $(3) = 16$. 3 est un élément primitif modulo 17 .

Remarque 5.26. Si n n'est pas premier, le Théorème précédent n'est plus valable. En effet, par exemple si $n = 8$, $\mathbb{U}_8 = \{1, 3, 5, 7\}$ et $\phi(8) = 4$. Modulo 8 on a, $3^2 = 9 \equiv 1$, $5^2 = 25 \equiv 1$, $7^2 = 49 \equiv 1$. Par suite il n'y a pas d'élément d'ordre 4 modulo 8.

Théorème 5.27. *Soit p un nombre premier et $\alpha \in \mathbb{U}_p$ un élément primitif modulo p, l'application :*

$$\begin{array}{ccc} f : \{0, 1, \ldots, p-2\} & \longrightarrow & \mathbb{U}_p \\ k & \longmapsto & \alpha^k \text{ modulo } p \end{array}$$

est une bijection. L'application réciproque est appelée **le logarithme discret de base** α. *On note $k = Dlog_\alpha(x)$.*
Si $x \in \mathbb{Z}$, non divisible par p, $Dlog_\alpha(x) = Dlog_\alpha(r)$, où r est le reste de la division euclidienne de x par p.
On a donc $\forall x \in \mathbb{Z}$ et $k \in \{0, 1, \ldots, p-2\}$

$$k = Dlog_\alpha(x) \Leftrightarrow \alpha^k = x \text{ modulo } p$$

de plus, $Dlog_\alpha(xy) = Dlog_\alpha(x) + Dlog_\alpha(y)$ modulo $p-1$.

Preuve. Puisque $\text{card}(\mathbb{U}_p) = p-1$, il suffit de montrer que f est injective. Soient $m \geq n \in \{0, 1, \ldots, p-2\}$ tels que $\alpha^m = \alpha^n$. Alors $\alpha^{m-n} \equiv 1$ modulo p. Comme α est d'ordre $p-1$, on a $p-1 \mid m-n$ et puisque $0 \leq n \leq m \leq p-2$, on a $m-n = 0$. ■

Exemple 5.28. On reprend l'exemple 5.25. On a 3 est un élément primitif modulo 17 et $3^7 \equiv 11$ modulo 17. Donc $\text{Dlog}_{\bar{3}}(11) = 7$ modulo 17.

5.4 Applications de l'arithmétique à la cryptographie

L'arithmétique a plusieurs applications dans le domaine de la sécurité de l'information.

1. Mots de passe. Pour certains nombres premiers très grands, le calcul du logarithme discret est très difficile. La seule méthode pour calculer le logarithme discret d'un entier y, est la méhode qui consiste à tester tous les nombres entiers naturels $k \leq p-2$. Ce calcul peut prendre un temps énorme même avec le plus rapide des ordinateurs.
Par opposition le calcul de la puissance $f(k) = \alpha^k$ modulo p, où α est un élément primitif modulo p, est facile, mais la fonction inverse est difficile à déterminer. On dit que f est une fonction à sens unique.
Ce type de fonction est utilisé en cryptographie, particulièrement pour ouvrir des sessions (compte, e-mail, etc..) avec des mots de passe et les échanges de clés.

Un utilisateur 'A' décide de créer un compte. Il compose son login (identifiant : nom ou email) et compose aussi un mot de passe x qu'il est le seul à connaitre. Le serveur calcule

$y = f(x)$, où f est une fonction à sens unique et associe y au login. Si 'A' compose le login et son mot de passe x, le serveur calcule $f(x)$. Comme $f(x) = y$, la session s'ouvre. Si une autre personne tape un mot de passe $x' \neq x$, on a $f(x') \neq y$, la session ne s'ouvre pas.
Même si une personne arrive à connaître y, il lui sera très difficile de trouver x, car f est une fonction à sens unique.

2. Echange de clés. (Protocole de Diffie-Hellman) Deux personnes A et B décident de créer un nombre N qui servira comme clé secrète à des échanges de communications secrètes. Chacune de ces personnes dispose d'une clé secrète, n pour A et m pour B.
A envoie α^n à B, B calcule $(\alpha^n)^m = \alpha^{nm}$.
B envoie α^m à A, A calcule $(\alpha^m)^n = \alpha^{nm}$.
Donc A et B disposent tous les deux d'un nombre commun $N = \alpha^{nm}$ qui sera la clé secrète. Connaissant N, A ne peut connaitre la clé secrète de B, car il doit déterminer le logarithme discret de N, le même problème se pose pour B.
En fait le calculs précédents se font de manière automatique par les serveurs de courrier éléctronique, ou de téléphonie etc...

3. Cryptosystème RSA Une personne A choisit deux grands entiers naturels premiers p et q (plus de 100 chiffres chacun) et calcule leur produit $n = p.q$. Puis elle choisit un entier e premier avec $\phi(n) = (p-1).(q-1)$. Enfin, elle publie sur le web, sa clef publique : (RSA, n, e). Puis calcule d tel que $ed \equiv 1$ modulo $(p-1)(q-1)$. Elle ne publie pas d c'est sa clé secrète.
Une personne B veut envoyer un message à A. Il doit utiliser le système RSA avec les deux entiers n et e (prenons par exemple $n = 5141 = 53.97$ et $e = 7$, premier avec $52 \cdot 96 = 4992$). Il transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet $A = 1$, $B = 2$, $C = 3$..... Par exemple le message 'SALUT' devient $x = (0019, 0001, 0012, 0021, 0020) = (x_1, x_2, x_3, x_4, x_5)$. La personne B crypte le message de la façon suivante en calculant les x_i^7, modulo n : $19^7 \equiv 928, 1^7 \equiv 1, 12^7 \equiv 4179, 21^7 \equiv 883, 20^7 \equiv 4102$, le message devient :$y = (0928, 0001, 4179, 0883, 4102) = (y_1, y_2, y_3, y_4, y_5)$. Il envoie ce message à A.
La personne A decrypte le message reçu en calculant les y_i^d modulo n. En effet,

$$y_i^d = (x_i^e)^d = x_i^{ed} = x_i^{k\phi(n)+1} = (x_i^{\phi(n)})^k.x_i \text{ modulo } n$$

Or $x_i^{\phi(n)} \equiv 1$, modulo n. Donc $y_i^d \equiv x_i$ modulo n. Elle retrouve alors le message envoyé.

Supposons qu'une personne malveillante C a pu intercepter le message crypté. Elle pourra décrypter le message si elle connait le nombre d. Pour cela, elle doit connaître $(p-1)(q-1)$ donc connaître p et q que seul A connaît. Pour cela C doit pouvoir factoriser n. Mais si p et q sont deux nombres premiers très grands avec plusieurs centaines de chiffres, cette factorisation est pratiquement impossible même avec le plus rapide des ordinateurs actuels. Donc C ne pourra pas "pirater" le message.