# Arithmetique

Par Lorenzo

24 November 2024

## Contents


**1 Structures algébriques** **1**
- 1.1 Lois de compositions internes . . . 1
- 1.2 Groupes . . . 1
- 1.3 Anneaux et Corps . . . 3

**2 Arithmétique des entiers** **4**
- 2.1 Rappels sur $\mathbb{N}$ et $\mathbb{Z}$ . . . 4
- 2.2 Arithmétique élémentaire dans $\mathbb{Z}$ . . . 5
- 2.3 Division euclidienne . . . 7
- 2.4 PGCD, PPCM . . . 7

**3 Arithmétique avancée dans $\mathbb{Z}$** **8**
- 3.1 Bézout, Gauss . . . 8
- 3.2 Unicité de la décomposition en facteurs premiers . . . 9
- 3.3 Résolution des équations diophantiennes . . . 9

**4 Arithmétique modulaire : $(\mathbb{Z}/n\mathbb{Z})$** **10**
- 4.1 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ . . . 11
- 4.2 Restes chinois (aka le restau chinois) . . . 12

**5 Polynômes et Fractions rationnelles** **12**


# 1 Structures algébriques

## 1.1 Lois de compositions internes

**Définition 1.1.** *Soit $E$ un ensemble. On appelle* ***loi de composition interne*** *(l.c.i) sur $E$ une opération binaire.*

*On parle d'application $E \times E \to E$*

**Définition 1.2.** *Soit $*$ une l.c.i sur $E$. On dit que $*$ est*

***associative*** *si* $\forall x, y, z \in E,\ x * (y * z) = (x * y) * z$

***commutative*** *si* $\forall x, y \in E,\ x * y = x * y$

***identitaire*** *(a un* ***élement neutre*** *$e \in E$) si* $\forall x \in E, x * e = e * x = x$

## 1.2 Groupes

**Définition 1.3.** *Soit $G$ un ensemble et $*$ une l.c.i sur $G$. On dit que $(G, *)$ est un* ***groupe*** *lorsque les axiomes suivants sont vérifiés.*

- *$*$ est associative*
- *$*$ admet un élement neutre $e \in G$*
- *$\forall x \in G, \exists x' \in G$ tel que $x * x' = x' * x = e$ (on dit que x' est l'élement inverse ou symétrique de $x$ pour $*$)*

**Remarques 1.1.** *Si de plus $*$ est commutative, alors le groupe est dit* ***abélien*** *(ou commutatif).*

**Example 1.1.** *Si $X$ est un ensemble, notons $Bij(X)$, l'ensemble des application de $X$ dans $X$ admettant une application réciproque*

$$\forall\, f\colon X \to X,\ \exists\, g\colon X \to X,\ g \circ f = f \circ g = \mathrm{Id}_X : \begin{cases} X & \to X \\ x & \mapsto x \end{cases}$$

*Ainsi $(Bij(X), \circ)$ est un groupe.*

**Proposition 1.1.**

*Si $(G, *)$ est un groupe alors*

***(a)*** *L'élement neutre de $G$ est unique*

***(b)*** *Chaque $x \in G$ admet un unique élement inverse*

***(c)*** *Si $x, y, z \in G$ tel que $x * y = z * y$ alors $x * y$ (indépendament de l'ordre)*

**Démonstration 1.1.**

***(a)*** *Soient e, e' des élements neutres de G par *,* $e * e' = e' * e = e = e'$

***(b)*** *Soient x', x" des élements inverse de $x \in G$,*
$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$

***(c)*** *Posons* $x^{-1} * (x * y) = x^{-1} * (x * z) \implies (x^{-1} * x) * y = (x^{-1} * x) * z \implies e * y = e * z \implies y = z$

□

**Remarques 1.2.** *Lorsqu'il n'y a pas d'ambiguïtés, l'inverse d'un élement $x$ sera noté $x^{-1}$. Notons que $(x^{-1})^{-1} = x$*

**Définition 1.4.** *Soit (G, *) un groupe. Soit $H \subset G$, on dit que $H$ est un* ***sous-groupe*** *de $G$ lorsque les condtions suivantes sont vérifiées.*

- *$\forall x, y \in H,\ x * y \in H$. On dit que $H$ est stable par $*$*

- *Muni de $*$, $H$ est un groupe*

**Proposition 1.2.**

*Soit $(G, *)$ un groupe et $H \subset G$. Les conditions suivantes sont équivalentes.*

***(a)*** *$H$ est un sous groupe de $G$*

***(b)*** *$H \neq \emptyset$, $H$ est stable par $*$ et par passage au symétrique ($\forall x \in H,\ x^{-1} \in H$)*

***(b)*** *$H \neq \emptyset$ et $\forall x, y \in H,\ x * y^{-1} \in H$*

**Démonstration 1.2.**

• *Démontrons que* $(a) \implies (b)$.

◇ *$H$ est un sous groupe donc doit admettre un élement neutre ($e_H$) donc $H \neq \emptyset$. Montrons que $e_H = e_G$, on a $e_H * e_H = e_H = e_G + e_H = e_G$.*

◇ *La stabilité par * fait partie de la définition de sous groupe.*

◇ *Soit $x \in H$, soit s' son symétrique dans H. x' est aussi un symétrique dans G. Dans G par unicité du symétrique $x^{-1} = x' \in H$.*

• *Démontrons que* $(b) \implies (c)$.

◇ *Soient $x, y \in H$. Alors $y^{-1} \in H$ et encore par $x * x^{-1} \in H$.*

• *Démontrons que* $(c) \implies (a)$.

◇ *l'associativité est montré par $\forall x, y, z \in H, x, y, z \in G, x * (y * z) = (x * y) * z$*

◇ *l'élement neutre par $\exists x \in H, e = x * x^{-1} \in G$, ainsi $\forall x \in H, x \in G$*

◇ *l'élement inverse par $x \in H$, prenons $y = e$, ainsi $x^{-1} * e = x^{-1}$, ici $x^{-1}$ est le symétrique de x dans H.*

◇ *la stabilité par * dans H par $x, y \in H$, posons $z = y^{-1}$, ainsi $x * y = x * z^{-1} \in H$.*

> *Finalement par implication circulaire nous avons démontré que*
> $(a) \iff (b) \iff (c)$

□

**Définition 1.5.** *Soient $(G, *)$ et $(H, \square)$ deux groupes.*

*On appelle **morphisme de groupes** toute application $f : G \to H$ vérifiant*

$$\forall x, y \in G, f(x * y) = f(x) \square f(y)$$

**Proposition 1.3.**

*Si $f : G \to H$ est un morphisme de groupe, alors $f(e_G) = e_H$*

**Démonstration 1.3.**

$f(e_G) = f(e_G * e_G) = f(e_G) \square f(e_G)$
$f(e_G) = f(e_G) \square e_H$
$f(e_G) \square f(e_G) = f(e_G) \square e_H \implies f(e_G) = e_H$

$\square$

**Proposition 1.4.**

*Si $f : G \to H$ est un morphisme de groupe, alors $\forall x \in G, f(x^{-1}) = f(x)^{-1}$*

**Démonstration 1.4.**

$f(x^{-1}) = f(x^{-1})\square f(x)\square f(x)^{-1} = f(x^{-1} * x)\square f(x)^{-1} = f(x)^{-1}$

$\square$

## 1.3 Anneaux et Corps

**Définition 1.6.** *Un **anneau** est $(A, +, \times)$ où $A$ est un ensemble, + et x sont deux l.c.i sur $A$ vérifiant les axiomes suivants*

- *$(A, +)$ est un groupe abélien (on note $0_A$ sont élément neutre)*
- *$\times$ est associative*
- *$\times$ est distributive sur +*

**Remarques 1.3.** *On dit que $(A, +, \times)$ est un anneau commutatif si, de plus $\times$ est commutative.*

*Un élément $x \in A$ est dit inversible dans $A$ lorsqu'il adment un symétrique pour $\times$.*

**Proposition 1.5.**

*Soit $(A, +, \times)$ un anneau alors*
*$\forall x \in A,\ 0_A \times x = 0_A$*

**Démonstration 1.5.**

$$\begin{aligned} 0_A \times x &= (0_A + 0_A) \times x \\ &= 0_A \times x + 0_A \times x \implies 0_A = 0_A \times x \text{ (par soustraction de } 0_A \times x) \end{aligned}$$

$\square$

**Proposition 1.6.**

*Soient $x, y, z \in A$, Si $x \times z = y \times z$ et $z$ est inversible alors $x = y$*

**Démonstration 1.6.**

$$\begin{aligned} x \times z = y \times z &\implies (x \times z) \times z^{-1} = (y \times z) \times z^{-1} \\ &\implies x \times (z \times z^{-1}) = y \times (z \times z^{-1}) \\ &\implies x \times 1_A = y \times 1_A \\ &\implies x = y \end{aligned}$$

$\square$

**Définition 1.7.** *Un **corps** est la donnée d'un triplet $(\Bbbk, +, \times)$ où $\Bbbk$ est un ensemble, + et $\times$ sont deux l.c.i sur $\Bbbk$ vérifiant les axiomes suivants:*

- *$(\Bbbk, +, \times)$ est un anneau commutatif*
- *$(\Bbbk^*, \times)$ est un groupe abélien (de neutre noté $1_\Bbbk$).*

**Remarques 1.4.** *De manière équivalente, un corps est un anneau commutatif avec un élément neutre pour $\times$ où tout élément non-nul est inversible.*

# 2 Arithmétique des entiers

## 2.1 Rappels sur $\mathbb{N}$ et $\mathbb{Z}$

**Théorème 2.1.** *(propriétés de + et × sur $\mathbb{N}$)*

***(a)*** *+ et × sont associative et commutative sur $\mathbb{N}$*

***(b)*** *0 est élement neutre pour + tandis que 1 est neutre pour ×*

***(c)*** *Il y a une distributivité de × sur +*

***(d)*** $\forall x, y, m \in \mathbb{N},\ x + m = y + m \implies x = y$

**Théorème 2.2.** *(propriétés de ≤ sur $\mathbb{N}$)*

***1)*** *(relation d'ordre total)* $\forall m, n, p \in \mathbb{N}$

***(a)*** $n \leq n$

***(b)*** $m \leq n \wedge n \leq m \iff m = n$

***(c)*** $m \leq n \wedge n \leq p \implies m \leq p$

***(d)*** $m \leq n \vee n \leq m$

***2)*** *Les opérations + et × sont compatibles avec la relation d'ordre*
$\forall n, m, p \in \mathbb{N},\ n \leq m \implies (n + p \leq m + p) \wedge (n \times p \leq m \times p)$

***3)*** $\forall n \in \mathbb{N},\ 0 \leq n$

***4)*** $\forall n, m \in \mathbb{N}, \forall p \in \mathbb{N}^*,\ n \leq m \implies n \times p \leq m \times p$

**Théorème 2.3.**

***1.*** *Toute partie finie de $\mathbb{N}$ admet un plus grand élément.*

***2.*** *Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.*

***3.*** *Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.*

***4.*** *$\mathbb{N}$ n'admet pas de plus grand élément.*

**Théorème 2.4.** *(propriétés de + et × sur $\mathbb{Z}$)*

***(a)*** *+ et × sont associative et commutative sur $\mathbb{Z}$*

***(b)*** *0 est élement neutre pour + tandis que 1 est neutre pour ×*

***(c)*** *Il y a une distributivité de × sur +*

***(d)*** *Tout $m \in \mathbb{Z}$ admet un symétrique (élément inverse), $-m \in \mathbb{Z}$ pour +*

**Théorème 2.5.** *(propriétés de ≤ sur $\mathbb{Z}$)*

***1)*** *≤ est une relation d'ordre totale sur $\mathbb{Z}$.*

***2)*** *Soient $n, m, p \in \mathbb{Z}$*

***(a)*** $n \leq m \iff n + p \leq m + p$

***(b)*** $\forall p \in \mathbb{Z}_+^*, n \leq m \iff np \leq mp$

***(c)*** $\forall p \in \mathbb{Z}_-^*, n \leq m \iff mp \leq np$

***(d)*** $\forall p \in \mathbb{Z}^*, m = n \iff mp = np$

## 2.2 Arithmétique élémentaire dans $\mathbb{Z}$

**Définition 2.1.** *Soient $x$ et $y$ dans $\mathbb{Z}$. On dit que $x$ divise $y$ s'il existe $k \in \mathbb{Z}$ tel que $y = kx$. La notation associée est $x \mid y$. $x$ est un diviseur de $y$ ou $y$ est un multiple de $x$*

**Remarques 2.1.**

- *tout entier relatif divise 0.*
- *0 divise uniquement 0.*
- *si $x$ est un diviseur de $y$ alors (-$x$) est un diviseur de $y$*
- *1 et -1 sont les diviseurs de tout entier relatifs.*
- *les diviseurs de 1 et -1 sont 1 et -1*
- $\forall x, y \in \mathbb{N}^*,\ x \mid y \implies x \leq y$

**Définition 2.2.** *On dit que $p \in \mathbb{N},\ p \geq 2$ est un nombre premier si les seuls diviseurs positifs de $p$ sont 1 et $p$.*

**Remarques 2.2.** *Une autre définition est tout nombre qui a exactement 2 diviseurs.*

**Remarques 2.3.** *Pour vérifier qu'un nombre est premier, on peut regarde pour chaque $\forall k \in \mathbb{N}, k \leq \sqrt{p}$ si $k$ divise $p$.*

**Définition 2.3.** *Soit $n \in \mathbb{Z}^*$, on appelle décomposition en facteurs premiers de $n$ une écriture de la forme*

$$n = c\prod_{i=1}^{k} p_i = c(p_1 \times ... \times p_k)$$

*où $c \in \{\pm 1\}, k \in \mathbb{N}, p_1, ..., p_k$ sont premiers*

**Proposition 2.1.**

*Tout $n \in \mathbb{Z}^*$ admet une décomposition en facteurs premier.*

**Démonstration 2.1.**

*Il suffit de le démontrer pour $n \in \mathbb{N}^*$ et $c = 1$ et pour les négatifs on se ramène à $\mathbb{N}^*$ en posant $c = -1$*

*Démonstration par récurrence forte.*

***Initialisation:*** *$n = 1$, on pose $c = 1, k = 0$, c'est un produit vide.*

***Initialisation:*** *Soit $n \in \mathbb{N}^*, \forall d \leq n$, on ait une telle décomposition. Si $n$ + 1 est premier, on pose $k = 1 \quad P_1 = n + 1$. Si $n$ + 1 n'est pas premier il admet un diviseur $d \in [2, n]$. Par hypothèse de récurrence $d = c \times p_1 \times ... \times p_k$. De même $d' = \dfrac{n+1}{d} \in [2; n]$ $d' = p'_1 \times ... \times p'_k$.*

*Donc $n + 1 = d \times d' = p_1 \times ... \times p_k \times p'_1 \times ... \times p'_k$*

□

**Corollaire 2.1.** *Tout entier $n \geq 2$ admet au moins un diviseur premier*

**Proposition 2.2.**

*L'ensemble des nombre premiers est infini.*

**Démonstration 2.2.**

*Supposons (par l'absurde) qu'il y ait un nombre fini de nombres premiers* $p_1, ..., p_m$
*On pose* $N = p_1 \times ... \times p_m + 1$
*Alors N admet un diviseur premier* $p_i(i \in [i; m])$ *i.e.* $N = p_i N' \implies N = \prod p_j + 1 \implies p_i N' - p_i \prod_{i \neg j} p_j = 1 \implies p_i(N' - multi_{j \neg i} p_j) = 1$

□

## 2.3 Division euclidienne

**Théorème 2.6.** *Soient* $a \in \mathbb{Z}, b \in \mathbb{N}*$.
*Alors il existe un unique couple* $(q, r) \in \mathbb{Z} \times \mathbb{N}, a = bq + r$ *avec* $b > r \geq 0$

**Démonstration 2.3.**

***Existence:*** *Pour* $a \in \mathbb{N}$, *raisonnement par récurrence.*
***Initialisation:*** $a = 0$: *On pose* $q = 0$ *et* $r = 0 \implies 0 = b \times 0 + 0$
***Hérédité:*** *Si* $a = bq + r$ *avec* $(b > r \geq 0)$
*Alors* $a+1 = bq+(r+1)$, *C'est une division euclidienne lorsque* $r+1 < b \implies r < l-1$
*Lorsque* $r = b - 1$
$a + 1 = bq + ((b - 1) + 1) = bq + b = b(q + 1) + 0$, *C'est une division euclidienne.*
*Si* $a < 0$ *alors* $(-a) > 0$ *Donc* $\exists (q, r) \in \mathbb{Z} \times \mathbb{N}, -a = bq + r \implies a = b \times (-q) + (-r)$ *avec* $(b > r \geq 0)$
*Si r = 0, c'est une division euclidienne.*
*Sinon* $-b < -r < 0 \implies 0 < -r + b < b$
*Donc* $a = b \times (-q) + (-r+b) - b = b \times (-q-1) + (-r+b)$ *C'est un division euclidienne.*
***Unicité:*** *Si* $a = bq + r$ *et* $a = bq' + r'$ *avec* $b > r, r' \geq 0$
*Par soustraction:* $0 = b(q - q') + r - r' \implies r' - r = b(q - q')$
$b - 1 \geq r' - r \geq -b - 1$ *Donc* $r' - r = 0 \implies r = r'$
*Ainsi* $bq + r = bq' + r' \implies bq = bq' \implies q = q'$

□

## 2.4 PGCD, PPCM

**Définition 2.4.** *le **pgcd** de deux nombres* $a, b \in \mathbb{Z}^*$ *est le plus grand diviseur commun à a et b. Il est noté* $PGCD(a, b)$ *(ou encore* $a \wedge b$*)*
*On dit que a et b sont **premiers entre eux** si PGCD(a, b) = 1.*
*Le **ppcm** de deux nombres* $a, b \in \mathbb{Z}^*$ *est le plus petit multiple strictement positif commun à a et b. Il est noté PPCM(a, b) (ou encore* $a \vee b$*)*

**Proposition 2.3.**

$\forall a, b \in \mathbb{Z}^*, PGCD(a, b) \times PPCM(a, b) = |ab|$

**Démonstration 2.4.**

*Si on remplace a et b par leurs valeurs absolues:* $||a||b|| = |ab|$
*Les multiples et les diviseurs de |a| et de a sont les mêmes.*

*Donc $PGCD(a, b) = PGCD(|a|, |b|)$ et $PPCM(a, b) = PPCM(|a|, |b|)$*
*Ainsi il suffit de montrer le résultat pour $a, b \in \mathbb{N}^*$*
*On pose $d = PGCD(a, b)$*
$\exists a', b' \in \mathbb{N}^*, a = da'$ *et* $b = db'$
$\frac{ab}{d} = \frac{da'b}{d} = a'b$ $\frac{ab}{d} = \frac{adb'}{d} = ab'$

□

**Méthode 2.1.**

*L'algorithme d'Euclide:*
*Le PGCD peut se calculer avec l'algorithme d'Euclide:*

***1.*** *(Eventuellement) remplacer $a$ et $b$ par $|a|$ et $|b|$*

***2.*** *De manière récursive:*

***2.1*** *Calculer la division euclidienne de $a$ par $b$: $a = bq + r$*

***2.2*** *Si $r \neq 0$: recommencer en remplcaçant (a, b) par (b, r) Sinon sortir de la récursion*

***3.*** *Le pgcd est le dernier reste non-nul calculé.*

**Proposition 2.4.**

*Si $d$ est un diviseur commun à $a$ et $b$ alors $d \mid PGCD(a, b)$*

**Corollaire 2.2.** *Le PGCD est aussi le plus grand diviseur commun au sens de la divisibilité.*

# 3 Arithmétique avancée dans $\mathbb{Z}$

## 3.1 Bézout, Gauss

**Proposition 3.1** (Bézout)**.**

*Soient $a, b \in \mathbb{Z}^*$. Il existe $u, v \in \mathbb{Z}$ tels que*
$au + bv = PGCD(a, b)$

**Méthode 3.1.**

*Pour trouver une relation de Bezout, il suffit de remonter l'algorithme d'Euclide. Que l'on appelle **l'algorithme d'Euclide étendu**.*

1. *Faire l'algorithme d'Euclide*

2. *Réecrire le reste avec les autres valeurs*

**Lemme 3.1.** *Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ avec $n \in \mathbb{Z}$*

**Démonstration 3.1.**

- *$n\mathbb{Z}$ sous groupe de $(\mathbb{Z}, +)$ (cf TD1)*

- *Soit $H$ un sous groupe de $(\mathbb{Z}, +)$ alors $0 \in H$*

- *Si $H = \{0\}$ alors $H = 0\mathbb{Z}$*
- *Sinon il existe un $x$ non nuls dans $H$, alors $(-x) \in H$ "A completer"*

$\square$

**Corollaire 3.1.** *Soient $a, b \in \mathbb{Z}$ alors $a\mathbb{Z} + b\mathbb{Z} = \{au + bv | u, v \in \mathbb{Z}\} = \delta\mathbb{Z}$ où $\delta = \mathrm{PGCD}(a, b)$*

**Démonstration 3.2.**

*Soient $u, v \in \mathbb{Z}$ et $c = au + bv$. Comme $\delta a$ et $\delta b$ alors $\delta c$.*

*Réciproquement, soit $c \in \delta\mathbb{Z}$, il existe un c' dans $\mathbb{Z}$ tel que $c = \delta c'$. Par Bézout, il existe $u', v' \in \mathbb{Z}$ tels que $au' + bv' = \delta$, en multipliant par c' on a $au'c' + bv'c' = \delta c' = c$. Il suffit alors de poser $u = u'c'$ et $v = v'c'$.*

*On dit alors que le sous groupe* ***engendré par*** *a et b coïncide avec le sous groupe engendré par leurs PGCD.*

$\square$

**Proposition 3.2** (Gauss)**.**

*Soient $n, a, b \in \mathbb{Z}^*$ tels que $n | ab$ et $\mathrm{PGCD}(n, a) = 1$. Alors $n | b$.*

**Démonstration 3.3.**

*Par Bezout, il existe $u$ et $v$ tels que $nu + av = 1$. Donc $nub + abv = b$. De $ab = nk$ (pour un $k \in \mathbb{Z}$), on déduit $n(ub + kv) = b$. Donc $n | b$.*

$\square$

## 3.2 Unicité de la décomposition en facteurs premiers

**Lemme 3.2.**

1. *Soient $a, b, c \in \mathbb{Z}^*$*

$$\left.\begin{array}{l}\mathrm{PGCD}(c, a) = 1\\ \mathrm{PGCD}(c, b) = 1\end{array}\right\} \Longrightarrow \mathrm{PGCD}(c, ab) = 1$$

2. *Soient $p$ un nombre premier et $a, b \in \mathbb{Z}^*$*

   (a) *On a $\mathrm{PGCD(a, p)} = 1$ ou $p | a$*

   (b) *On a $[p | ab \implies (p | a ou p | b)]$*

**Démonstration 3.4.**

*À faire*

$\square$

**Proposition 3.3.**

*Une décomposition en facteurs premier est unique à l'ordre des facteurs près.*

**Démonstration 3.5.**

*À faire*

$\square$

### 3.3 Résolution des équations diophantiennes

Soient $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$.

On cherche à résoudre l'équation suivante d'inconnues entères u, v

$$au + bv = c$$

**Méthode 3.2.**

1. *Posant* $\delta = \mathrm{PGCD(a, b)}$, *on a* $a = \delta a'$, $b = \delta b'$ *et* $c = \delta c'$ *avec* $a', b', c' \in \mathbb{Z}$ *on a donc*

$$a'u + b'v = c'$$

   *Soit* $d = \mathrm{PGCD(a', b')}$ *alors* $d\delta$ *est un diviseur commun à* $a = \delta a'$ *et* $b = \delta b'$. *Par maximalité du diviseur commun* $\delta$, *on a* $d = 1$. *Donc a' et b' sont premier entre eux.*

2. *Bézout nous fournit une solution à l'équation* $a'u + b'v = 1$, *qu'il suffit de multiplier par c' pour avoir une solution particulière* $(u_0, v_0)$.

3. *Soit* $(u, v) \in \mathbb{Z}^2$ *une solution.* $a'u + b'v = c'$ *et* $a'u_0 + b'v_0 = c'$ *donc* $a'(u - u_0) + b'(v - v_0) = 0$. *On a* $\mathrm{PGCD(a', b')} = 1$ *donc, d'après Gauss,* $a'|(v - v_0)$. *Donc* $\exists k \in \mathbb{Z}$ *tel que* $v - v_0 = ka' \implies v = v_0 + ka'$ *donc* $u = u_0 - b'k$.

4. *L'ensemble des solutions est donc contenu dans* $\{u_0 - b'k, v_0 + a'k \mid k \in \mathbb{Z}\}$

# 4 Arithmétique modulaire : $(\mathbb{Z}/n\mathbb{Z})$

**Définition 4.1.** *Soient* $a, b \in \mathbb{Z}$. *On dit que a et b sont* ***congrus modulo*** $n$ *si* $a - b \in n\mathbb{Z}$.

*On note alors* $a \equiv b[n]$ *ou encore* $a \equiv b \mod n$.

**Proposition 4.1.**

1. *On a* $a \equiv b[n] \iff \exists k \in \mathbb{Z}, a = b + kn$.

   *On note* $\overline{b} := \{b + nk \mid k \in \mathbb{Z}\} = \{a \in \mathbb{Z} \mid a \equiv b[n]\}$. *On l'appelle la* ***classe de congruence****.*

2. *Supposons que* $a = nq + r$ *soit la division euclidienne de a par n. Alors* $\overline{a} = \overline{r}$.

3. *Il y a exactement n classes de congruence distinctes : les* $\overline{r}$, *pour* $r \in \{0, 1, ..., n-1\}$. *Elles sont disjointes 2 à 2.*

**Définition 4.2.** *On note* $\mathbb{Z}/n\mathbb{Z}$ *l'ensemble des classes de congruences.*

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ *est un ensemble fini à n élements.*

**Démonstration 4.1.**

*À faire*

□

**Remarques 4.1.** *La congruence est un relation d'équivalence ainsi les classes congruences sont les classes d'équivalences pour la relation de congruence.*

*Ainsi* $\mathbb{Z}/n\mathbb{Z}$ *se réinterprète comme* $\mathbb{Z}/R$ *avec* $xRy \iff x \equiv y[n]$

## 4.1 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

**Proposition 4.2.**

*Soient* $a, a', b, b' \in \mathbb{Z}$ *tels que* $a \equiv a'[n]$ *et* $b \equiv b'[n]$ *Alors* $a + b \equiv a' + b'[n]$

**Démonstration 4.2.**

$(a - a') = kn$ *et* $(b - b') = k'n$ *avec* $k, k' \in \mathbb{Z}$

$(a + b) - (a' + b') = a - a' + b - b' = kn + k'n = (k + k')n$

$$\boxed{\text{Donc } a + b \equiv a' + b'[n]}$$

□

**Définition 4.3.** *Soient* $a, b \in \mathbb{Z}$. *On pose dans* $\mathbb{Z}/n\mathbb{Z}$ : $\overline{a} + \overline{b} = \overline{a + b}$ *et* $\overline{a} \times \overline{b} = \overline{a \times b}$

**Proposition 4.3.**

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *est un anneau commutatif unitaire.*
$\overline{0}$ *est l'élement neutre pour l'addition et* $\overline{1}$ *est l'élement neutre pour la multiplication.*

**Démonstration 4.3.**

*À faire*

□

**Example 4.1.** *On peut faire des tables d'addition et de multiplication dans* $\mathbb{Z}/n\mathbb{Z}$. *Par exemple la table de multiplication de* $\mathbb{Z}/3\mathbb{Z}$

| $\times$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{1}$ |

**Lemme 4.1.** *Soient* $a$ *et* $b$ *dans* $\mathbb{Z}$ *tels que* $a \equiv b[n]$.
*Pour tout* $p \in \mathbb{N}^*, a^p \equiv b^p[n]$

**Démonstration 4.4.**

*À faire*

□

**Remarques 4.2.** *En revanche on n'a pas* $p \equiv q[n] \implies a^p \equiv a^q[n]$

**Théorème 4.1.** $\{\mathbb{Z}/n\mathbb{Z}, +, \times\}$ *est un corps si et seulement si* $n$ *est premier.*

**Démonstration 4.5.**

*À faire*

□

## 4.2 Restes chinois (aka le restau chinois)

**Théorème 4.2** (des restes chinois)**.**

*Soient $n_1, n_2, ..., n_k \in \mathbb{N}^*$, tels que $\forall i \in \mathbb{N}^*, n_i \geq 2$ et deux à deux premiers entre eux. Alors pour tous $a_1, ..., a_k \in \mathbb{Z}$, il existe $x \in \mathbb{Z}$, unique modulo $n := \prod n_i$, tel que*

$$\forall i \in [\![1, k]\!], x \equiv a_i mod n_i$$

*Plus formellement, on a une application bijective,*

$$\varphi := \begin{cases} \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \times ... \times (\mathbb{Z}/n_k\mathbb{Z}) \\ x \mod n \mapsto (x \mod n_1, ..., x \mod n_k) \end{cases}$$

**Démonstration 4.6.**

*À faire*

□

**Remarques 4.3.** *$\varphi$ est un isomorphisme d'anneau. (respecte l'addition et la multiplication).*

**Méthode 4.1.**

*À faire*

# 5 Polynômes et Fractions rationnelles

**Définition 5.1.** *Un **polynôme à coefficient dans** $\Bbbk$: une suite $A = (a_n)_{n\in\mathbb{N}}$ telle que $\exists N \in \mathbb{N}, \forall n > N, a_n = 0$.*

*On écrira souvent $A = a_0 + a_1X + a_2X^2 + ... + a_NX^N = \Sigma_{i=0}^{N} a_iX^i = \Sigma_{i\in\mathbb{N}} a_iX^i = \Sigma a_iX^i$*

*$\Bbbk[X]$ = {polynômes à coefficients dans $\Bbbk$}*

***polynôme nul** : tous les coefficients sont nuls.*

***polynôme constant** : $\forall i > 0, a_i = 0$ ($A = cX^0 = c$ où $c \in \Bbbk$)*

***monôme** : polynôme de la forme*

Symbole de Kronecker $\delta_{i,j} = 1$ si i = j sinon 0

**Propriétés 5.1.**

**Démonstration 5.1.**

*Soient $A = \sum(a_iX^i)$ et $B = \sum(b_iX^i)$*
*$C = A + B$ avec $c_i = a_i + b_i$*
*Si $i > max(degA, degB)$ alors*

□