République Algérienne Démocratique Et Populaire
Université Mohamed Boudiaf De M'sila
Faculté Des Mathématiques Et De L'informatique
Département De Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Mathématique discrètes

Par

Hadj Doudou Oussama.

Sujet

Arithmétique finie et réciprocité quadratique

Date de soutenance :

Devant le jury :

Mr. **N. MIDOUNE**	Prof. Univ de M'sila	Président
Mr. **D.MIHOUBI**	Prof. Univ de M'sila	Rapporteur
Mr. **L.HABOUB**	Prof. Univ de M'sila	Examinateur

Promotion : 2016 / 2017

Remerciements

*Je remercie mon dieu «**ALLAH**» qui est toujours présent avec moi dans le meilleur et dans la pire.*

*J'adresse mon plus haut respect et ma sincère gratitude, qu'il trouve dans ces quelques mots l'expression de mon profond remerciement, à mon encadreur Mr : **D. Mihoubi** pour son encadrement précieux, son aide, son encouragement continu et ses conseilles afin que je puisse terminer à bien mes travaux.*

*Je tiens à remercier aussi Monsieur **N. MIDOUNE**, d'avoir accepté de présider mon mémoire.*

*Je tiens à remercier aussi Monsieur **L. HABOUB**, pour avoir accepté d'examiner mon mémoire.*

Pour finir mes derniers mots de remerciements vont tout naturellement à ma famille et mes amis.

Merci.

Dédicace

Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect, la reconnaissance, c'est tous simplement que : Je dédie cette thèse de master à :

A Ma tendre Mère ***Hamida****: Tu représente pour moi la source de tendresse et l'exemple de dévouement qui n'a pas cessé de m'encourager. Tu as fait plus qu'une mère puisse faire pour que ses enfants suivent le bon chemin dans leur vie et leurs études.*

A Mon très cher Père ***Ahmed****: Aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement et le respect que j'ai toujours pour vous. Rien au monde ne vaut les efforts fournis jour et nuit pour mon éducation et mon bien être. Ce travail et le fruit de tes sacrifices que tu as consentis pour mon éducation et ma formation le long de ces années.*

A la mémoire de mon petit bébé ***Amire*** *et* ***Ahmed Iyade****, je t'aime énormément.*

A mon cher frères : ***Abdallah*** *et sa femme* ***Khouloud, Lakhdare, Islam, Aymen.***

A ma sœur ***Imane*** *et son mari* ***Ahmed****.*

Pour ma grand-mère ***Zoubida*** *et* ***Zahia****, et mon grand-père* ***Ahmed et lakhdare.***

Pour chaque famille ***Medjahed*** *et* ***Hadj doudou****.*

A mes très chère ***amis****.*

A tous les membres de ma promotion ***2016/2017****.*

A tous mes enseignants depuis mes premières années d'études.

A tous ceux qui me sens chers et que j'ai omis de citer.

Oussama Hadj doudou.

Table des matières

Introduction

La théorie des nombres (ou arithmétique) s'occupe principalement des propriétés des nombres entiers. Bien que son sujet d'étude soit tout à fait élémentaire, les outils qu'elle utilise proviennent de toutes les branches des mathématiques et sont souvent très profonds et assez fréquemment les outils sont en fait créés dans le but de résoudre des problèmes de théorie des nombres. Les exemples les plus frappants sont la théorie des groupes, anneaux et corps. Ces théories ce sont principalement développés sous l'impulsion des problèmes liés à la théorie des nombres.

Dans ce mémoire, nous allons traiter le sujet de arithmétique finie dans l'anneaux $\mathbb{Z}/n\mathbb{Z}$ et le problème de la réciprocité quadratique. De quoi il s'agit ?

Pour résoudre la congruence $\mathbf{ax \equiv b \,(\mathrm{mod}\, n)}$ on multiplie par l'inverse de a, s'il existe, on obtient

$$x \equiv a^{-1}b \,(\mathrm{mod}\, n)$$

on pose $r = a^{-1}b$ on trouve

$$x \equiv r \,(\mathrm{mod}\, n) \Rightarrow x = r + nk,\ k \in \mathbb{Z}$$

le problème est plus délicat si on veut résoudre l'équation du second degré dans l'anneaux fini $\mathbb{Z}/n\mathbb{Z}$.

pour résoudre dans le corps $\mathbb{Z}/p\mathbb{Z}$ une équation du seconde degré $ax^2 + bx + c = 0$. En multipliant les deux membres par a', l'inverse de a dans $\mathbb{Z}/p\mathbb{Z}$, et en posant $a'b = -2r$, ce qui est toujours possible si p est impair. Comme on a $a'c = q$, on est ramené à l'equation :

$$x^2 - 2rx + q = 0$$

En remarquant dans le cas générale que :

$$(x-r)^2 = x^2 - 2rx + r^2$$

tout équation du second degré s'écrit en posant $r^2 - q = a$

$$(x-r)^2 = a \Rightarrow (x-r)^2 \equiv a \,(\text{mod } p)$$

On pose $y = x - r$

$$y^2 \equiv a \,(\text{mod}\, p)$$

donc pour résoudre une équatione de second dégré sur un corps fini, le problème revient donc de trouver les racines carrées de l'élément $a \in \mathbb{Z}/p\mathbb{Z}$. Ces éléments sont appelés les résidues quadratique de l'élément a.

Dans ce mémoire en s'intérèsse à l'étude des méthode de recherche des résidues quadratiques dans un corps fini.tels que : le symbole de Legendre, le symbole de Jacobi et la somme de Gauss.

Ce mémoire est réparti en trois chapitres :

Dans le premier chapitre on donne quelques définitions et notions générale sur les structures algèbriques tels que groupes, anneaux et corps.

Dans le seconde chapitre on s'intérèsse à l'arithmétique sur un anneau fini en faisant en premier lieu un rappel sur les notions suivantes : les nombres premiers, division euclidienne, théorème de bézout et théorème des reste chinois ...etc. Ensuite, on donne quelques propriétés sur l'arithmétique finie dans l'anneaux $\mathbb{Z}/n\mathbb{Z}$ en s'intéressant principalement fonction l'indicatrice d'Euler et théorème de Fermat.

Dans la troisième chapitre, on s 'intérèsse à l'ensemble des carreés dans le corps $\mathbf{F}_p, p$ premier. On introduit le symbole de Legendre et le symbole de Jacobi qui permet de caractériser ces carreés et on développe les principales propriétés de ce symbole. On démontre notamment la loi de réciprocité quadratique due à Gauss. Cette formule admet de nombreuses démonstration. Nous donnerons celle basée sur la sommes de Gauss.

Liste de tableaux

Liste de notation

$a \mid b$: a divise b.

$a \nmid b$: a ne divise pas b.

$\equiv$: Congruence, $a \equiv b \pmod{n}$, a congru b modulo n.

$PGCD$: Plus grand commun diviseur.

$PPCM$: Plus petit commun multiple.

$Card\,(G)$: Cardinal de l'ensemble G.

e : Elément neutre.

G : Groupe.

A : Anneaux

I : Idéal.

H : Sous-groupe

$\left(\frac{a}{p}\right)$: Symbole de legendre

τ : Somme de gauss.

$\Re$: Relation d'équivalence.

$\langle X \rangle$: Sous-groupe engendré par X.

$\varphi\,(n)$: fonction Indicatrice d'Euler.

α : Racine primitive.

$\mathcal{P}$: L'ensemble des nombres premiers.

aR_p : a Résidus quadratique modulo p.

aN_p : a Non-résidus quadratique modulo p.

Chapitre 1

Structures algébriques

Dans ce chapitre, nous nous proposons de donner quelques notions élémentaires sur les structures algébriques suivantes : groupes, anneaux et corps.

1.1 Structures de Groupes

1.1.1 Groupes

Définition 1.1

Soit G un ensemble non vide muni d'une loi de composition interne : une application $g : G \times G \to G$, pour laquelle on note $\forall x, y \in G$, $g(x, y) = x * y$ ou $x + y$, $x - y$, $x \circ y$, ou simplement xy. On dit que $(G, *)$, ou simplement G, est un groupe si :

(i) La loi $*$ est associative : $\forall\ x, y, z \in G, x * (y * z) = (x * y) * z$.

(ii) La loi $*$ possède un élément neutre : $\exists\ e \in G : \forall\ x \in G\ x * e = e * x = x$.

(iii) Tout élément x de G possède un symétrique unique x' :

$$\forall x \in G, \exists x' \in G : x * x' = x' * x = e$$

On désigne ce symétrique par x^{-1} et on l'appelle inverse de x.

Exemples 1.1

1- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sont des groupes.

2- $(\mathbb{R}^*, \cdot), (\mathbb{Q}^*, \cdot)$, ainsi que $(\mathbb{R}_+^*, \cdot), (\mathbb{Q}_+^*, \cdot)$ sont des groupes.

Définition 1.2

Si de plus la loi $*$ est commutative i.e., $\forall x, y \in G\ x * y = y * x$, on dit que le groupe G est commutatif ou abélien.

Exemples 1.2

1- $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ est l'ensemble des entiers modulo n muni de l'opération $\overline{x} \oplus \overline{y} = \overline{x+y}$ est un groupe commutatif.

2- $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \cdot)$ est un groupe commutatif.

Remarque 1.1

Tableau $N°1$ donne les notations de l'élement neutre, symétrique et l'image dans un groupe pour différentes lois.

G	$(G, *)$	$(G, +)$	$(G, \cdot)$
L'élement neutre	e	0	1_G
L'élement symétrique	x'	$-x$ opposé	x^{-1} l'inverse
L'image de $x, y \in G$	$x * y$	$x + y$	$x \cdot y$ *ou* xy

1.1.2 Sous groupe

Définition 1.3

Soit $(G, *)$ un groupe et soit $H \subset G$ une partie non vide de G. On dit que H est un sous-groupe de G si et seulement si les conditions suivantes sont satisfaites :

(i) $e \in H$ (H contient l'élément neutre de G).

(ii) $\forall x, y \in H, x * y \in H$ (stabilité de H pour la loi induite).

(iii) $\forall x \in H$ le symétrique de x pour la loi $*$ est dans H.

Notation 1.1

Si H est un sous groupe de G on note $H \leq G$.

Remarque 1.2

Si G est un groupe d'élément neutre e, il est clair que $\{e\}$ et G sont des sous-groupes de G dits sous groupes triviaux de G.

Exemples 1.3

1- $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C}+)$.

2- $(\{-1,1\},\cdot)$ est un sous-groupe de $(\mathbb{Q}^*,\cdot)$ qui lui même est un sous-groupe de $(\mathbb{R}^*,\cdot)$.

3- Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}, n \in N$.

Théorème 1.2

Soit H un sous-groupe de $\mathbb{Z}$, il existe un entier unique $a \geq 0$ tel que

$$H = a\mathbb{Z}$$

Preuve.

Soit H un sous groupe de G. Deux cas se présentent, H est un sous-groupe trivial de G ou bien H est un sous-groupe propre.

Si H est un sous-groupe trivial. Alors $H = \{0\}$, et on a $H = 0\mathbb{Z}$ ou bien $H = \mathbb{Z}$ et on a $H = 1\mathbb{Z}$.

Supposon que H est un sous-groupe propre i.e. $H \neq \{0\}$ et $H \neq \mathbb{Z}$, alors soit a le plus petit élément de la partie $\{x \in H \ / \ x \geq 0\}$ (ensemble non vide de $\mathbb{N}$ puisque G contient un élément x non nul, donc x ou $-x$ est strictement positif).

Soit $x \in H$, $\exists!\,(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $x = aq + r$ et $0 \leq r < a$, $r = x - aq$, r est donc un élément positif ou nul de G, strictement inférieur à a donc $r = 0$ et $x = aq$, $x \in a\mathbb{Z}$, et par conséquent $H \in a\mathbb{Z}$.

Inversement il est clair que si l'on considère un élément de $a\mathbb{Z}$, il sera aussi élément de H, gràce à la stabilité de la loi $+$ dans le sous-group H. D'ou l'égalité $H = a\mathbb{Z}$. ■

Proposition 1.1

Soit G un groupe et H une partie de G. Alors, H est un sous groupe de G si est seulment si :

(i) $H \neq \emptyset$

(ii) $\forall x, y \in H, x * y^{-1} \in H$.

Preuve.

Comme H est non vide, il existe $h \in H$ et $h * h^{-1} = e \in H$, donc $e \in H$. Pour tout $x \in H$, puisque $e \in H$, on a $e * x^{-1} \in H$, donc $x^{-1} \in H$. Pour tous x et y dans H, puisque $y^{-1} \in H$, on a $x * (y^{-1})^{-1} \in H$, donc $x * y^{-1} \in H$. ■

Remarques 1.3

1- Soit $(G, *)$ un groupe et soit $(H_i)_{i\in I}$ une famille non vide de sous-groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

2- La réunion de deux sous groupes d'un groupe n'est en général pas un sous groupe.

Exemple 1.4

Considérons dans $(R^2, +)$ les deux sous groupes $H_1 = R \times \{0\}$ et $H_2 = \{0\} \times R$ alors :

1- $H_1 \cap H_2 = \{(0, 0)\}$ est un sous groupe de $(R_2, +)$.

2- $H_1 \cup H_2$ n'est pas un sous groupe de $(R_2, +)$, car la condition **1** de la définition du sous groupe n'est pas vérifiée (on a par exemple $(1, 0) \in H_1 \cup H_2$ et $(0, 2) \in H_1 \cup H_2$ mais $(1, 0) + (0, 2) = (1, 2) \notin H_1 \cup H_2$).

Définition 1.4 (Ordre d'un groupe)

Soit $(G, \cdot)$ un groupe si l'ensemble G est fini alors le groupe $(G, \cdot)$ est dit un groupe fini et on note par $ord\,(G)$ d'ordre de G sinon le groupe G est dit d'ordre infini.

Exemples 1.5

1- Le groupe $(S_n, \circ)$ est d'ordre $n!$ c'est le nombre des permutations de n éléments, i.e. les application bijectives d'un ensemble E vers lui même contenant n éléments.

2- Le groupe $(\mathbb{C}, +)$ est d'ordre infini.

1.1.3 Groupe monogène et groupe cyclique

Définition 1.5 (Sous groupe engendré)

Soit X une partie d'un groupe G. On appelle sous-groupe engendré par X et on note $\langle X\rangle$ l'intersection de tous les sous-groupes de G contenant X.

$\langle X\rangle$ est le plus petit sous-groupe de G contenant X.

Si H est un sous-groupe de G et si $H = \langle X\rangle$, on dit que H est engendré par X.

Proposition 1.2

Soit G un groupe dont la loi $\times$ est notée multiplicativement et soit a un élément de G. On a :

$$\langle a\rangle = \{..., a^{-2}, a^{-1}, 1, a, a^2, ...\} = \{a^i \text{ où } i \in \mathbb{Z}\}.$$

Preuve.

($\subset$) On pose $E = \{..., a^{-2}, a^{-1}, 1, a, a^2, ...\}$. Il suffit de montrer que E est un sous-groupe de G.

- Puisque l'on a bien E qui contient a, on a $E \neq \emptyset$.
- $\forall x, y \in E$, $\exists\ n, p \in \mathbb{Z}\ / x = a^n$ et $y = a^p$. On a $xy^{-1} = a^{n-p}$,avec $n - p \in \mathbb{Z}$,donc $xy^{-1} \in E$.

($\supset$) Puisque $\langle a \rangle$ est un sous-groupe qui contient a, $\langle a \rangle$ doit être stable par inverse et composition. Donc $a^{-1} \in \langle a \rangle$ et $\forall n \in \mathbb{Z}$, $a^n \in \langle a \rangle$.

■

Exemple 1.6

$G = (\mathbb{Z}, +)$ et $A = \{3\}$ on a

$$\begin{aligned} \langle \{3\} \rangle &= \langle 3 \rangle = \{\ldots\ldots, -6, -3, 0, 3, 6, \ldots\ldots\} \\ &= \{3k, k \in \mathbb{Z}\} \\ &= 3\mathbb{Z}. \end{aligned}$$

Définition 1.6

Un groupe G est dit **monogène** s'il existe un élément a de G tel que G est engendré par a, i.e., $G = \langle a \rangle$. un tel élément est appelé **générateur** du groupe

Si $G = \langle a \rangle$ et si de plus G est fini, on dit que G est **cyclique** engendré par a.

Exemples 1.7

1- Soient $n \in \mathbb{Z}$ et $S = \{n\}$ un singleton de $\mathbb{Z}$. Alors $\langle n \rangle = n\mathbb{Z}$, donc n engendre $n\mathbb{Z}$, et $n\mathbb{Z}$ est un groupe monogène engendré par n. En particulier, $\mathbb{Z} = \langle 1 \rangle$ est monogène.

2- Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique engendré par $\overline{1}$.

Théorème 1.3

Soit G un groupe fini, soit $x \in G$ et soit n l'ordre de x. Alors

$$n \text{ est le plus petit entier positif telque } x^n = e.$$

Preuve.

Supposons désormais qu'il existe r tel que $x^r = e$. Soit r le plus petit entier naturel vérifiant cette condition. Il est clair que $\{e, x, ..., x^{r-1}\} \subseteq \langle x \rangle$. Si $n \in \mathbb{Z}$, effectuons la division euclidienne dans $\mathbb{Z}$ de n par r il existe $q, s \in \mathbb{Z}$, $0 \leq s \leq r-1$ tels que $n = qr + s$. Donc on montre qu'il existe au moins un entier $k, 1 \leq k \leq m$ tels que $x^k = e$. Soit

$$x^n = x^{qr+s} = x^{qr}x^s = (x^r)^q\, x^s = e^q x^s = x^s \in \left\{e, x, x^2, ..., x^{r-1}\right\}$$

puisque $0 \leq r \leq s-1$, il s'en suit que $\langle x \rangle \subseteq \{e, 1, x, x^2, ..., x^{r-1}\}$ .On a donc $\langle x \rangle = \{e, 1, x, x^2, ..., x^{r-1}\}$ par double inclusion. ■

Corollaire 1.1

Soit $(G, \cdot)$ un groupe fini d'ordre n, alors on a $x^n = 1_G$ pour tout $x \in G$.

Preuve.

Soit m l'ordre de x et soit $k \geq 1$ l'entier tel que $n = mk$, alors

$$x^n = x^{mk} = (x^m)^k = 1^k = 1$$

Ceci achève la preuve. ■

1.1.4 Groupes quotients

Définition 1.7 (Relation d'équivalence sur les groupes)

Soit $\Re$ une relation d'équivalence sur un groupe G. On dit que $\Re$ est compatible à gauche (resp.à droite) avec la loi de G ssi

$$\forall x, y, z \in G,\ x\ \Re\ y \Leftrightarrow zx\ \Re\ zy\ (\text{resp}\ xz\ \Re\ yz)$$

Théorème 1.4

Soient G un groupe et H un sous-groupe de G. Toute relation d'équivalence sur G compatible à gauche (resp.à droite) avec la loi de G est de la forme

$$\forall x, y \in G,\ x\Re_g y \Leftrightarrow x^{-1}y \in H$$
$$\forall x, y \in G,\ x\Re_d y \Leftrightarrow xy^{-1} \in H$$

sont des relations d'équivalence sur G.

Preuve.

Pour tout $x \in G$ on a $x^{-1}x = 1 \in H$ donc $\Re_g$ est réflexive.

Soit $x, y \in G$. Si $x\Re y$ on a

$$\begin{aligned} x\Re y &\Leftrightarrow x^{-1}y \in H \\ &\Leftrightarrow \left(x^{-1}y\right)^{-1} = y^{-1}x \in H \\ &\Leftrightarrow y\Re x. \end{aligned}$$

donc $\Re_g$ est symétrique.

Si $x, y, z \in G$ on a

$$\begin{cases} x\Re y \Leftrightarrow x^{-1}y \in H \\ y\Re z \Leftrightarrow y^{-1}z \in H \end{cases} \begin{aligned} &\Leftrightarrow \left(x^{-1}y\right)\left(y^{-1}z\right) \in H \\ &\Leftrightarrow x^{-1}z \in H \\ &\Leftrightarrow x\Re z \end{aligned}$$

donc $\Re_g$ est transitive.

Le même raisonnement s'applique au cas à droite. ■

Définition 1.8 (Classe modulo un sous groupe)

Soit G un groupe, H un sous groupe et soit x un élélment de G. La classe $\overline{x}_g$ de x modulo $\Re_g$ (resp. modulo $\Re_d$), appelée classe de x modulo H à gauche (resp. classe de x modulo H à droite) l'ensemble

$$xH = \{xh \ / \ h \in H\} \ (resp \ Hx = \{hx \ / \ h \in H\}.$$

L'ensemble de toutes ces classes d'équivalence est noté G/H et on l'appelle l'ensemble des classes à gauche modulo H. Donc on a

$$G/H = \{\overline{g} \ / \ g \in G\} = \{gH \ / \ g \in G\}$$

Proposition 1.3

Soit x un élément de G la classe d'équivalence de x modulo $\Re$ est l'ensemble

$$xH = \{xh \ / \ h \in H\}$$

Preuve.

Soit x un élément de G, les éléments de la forme xh où $h \in H$ sont en relation avec x , car $x^{-1}xh = h \in H$.

Inversement soit y un élément de G en relation avec x. On a $x\Re y$ de sorte que $x^{-1}y \in H$ alors $y \in xH$ ■

Définition 1.9 (Indice de H dans G)

Soient G un groupe et H un sous-groupe de G, on note $[G : H]$ .Le cardinal commun de $(G/H)_g$ (resp. $(G/H)_d$) $\left|(G/H)_g\right| = |(G/H)_d|$ est appelé indice de H dans G.

Théorème 1.5 ***(Théorème de Lagrange)***

Soient G un groupe fini et H un sous-groupe de G on a :

$$|G| = [G : H] \cdot |H|$$

Preuve.

On considère la relation d'équivalence définie sur G selon le sous groupe H. Comme $(G/H)_g$ est une partition de G on a $G = \bigcup_{x \in G} xH$, et comme on a $|H| = |xH| \ \forall x \in G$, alors si G est un groupe fini alors

$$\begin{aligned} |G| &= \left|\bigcup_{x \in G} xH\right| = |x_1H \cup x_2H \cup ... \cup x_kH| \\ &= |x_1H| + |x_2H| + ... |x_kH| \\ &= |H| + |H| + ... + |H| \\ &= k\,|H| \end{aligned}$$

On note par $k = [G : H]$ l'indice de H dans G. et on a donc $|G| = [G : H] \cdot |H|$. ■

Exemples 1.8

1- Si $H = G$, alors $\Re_g$ et $\Re_d$ sont des relations triviales, i.e., $\forall x, y \in G : x\Re_g y$ et $x\Re_d y$ et ainsi $(G/H)g = (G/H)d = \{G\}$.

2- Si $H = \{e\}$, alors deux éléments x et y de G ne sont en relation modulo H à gauche (resp.modulo H à droite) que si $x = y$ et ainsi $(G/H)g = (G/H)d = \{\{x\}/x \in G\}$.

Définition 1.10 (Sous-groupes distingués)

Soient G un groupe et H un sous-groupe de G. Le sous-groupe H est dit distingué si pour tout $g \in G$ on a $Hg = gH$.

Un sous-groupe distingué H de G est appelé aussi un sous-groupe **normal** ou **invariant** du groupe G et on note $H \lhd G$.

Remarques 1.4

1- Si G est un groupe, alors G et $\{e\}$ sont des sous-groupes distingués de G.

2- Si G est un groupe commutatif, alors tout sous-groupe de G est un sous-groupe distingué de G.

3- Si $[G : H] = 2$ alors $(G/H)_g = \{H, xH\}$ et $(G/H)_d = \{H, Hx\}$ et on a bien $(G/H)_g = (G/H)_d$ ce qui montre que $H \lhd G$.

1.1.5 Morphismes de groupes

Définition 1.11

Soient $(G, *)$ et $(G', \circ)$ deux groupes, une application $f : G \to G'$ est dite un **morphisme de groupes** ou **homomorphisme de groupes**, si pour tous $x, y \in G$ on a :

$$f(x * y) = f(x) \circ f(y)$$

Exemple 1.9

L'application

$$\begin{cases} f : & (\mathbb{R}, +) & \to & (\mathbb{R}, \times) \\ & x & \to & \exp(x) \end{cases}$$

est un morphisme du groupe $(\mathbb{R}, +)$ vers $(\mathbb{R}, \times)$. Car pour tous $x, y \in \mathbb{R}$ on a :$f(x + y) = e^{x+y} = e^x \times e^y = f(x) \times f(y)$.

Notation 1.6

- Si de plus f est bijective, f est appelé un **isomorphisme de groupes**.
- Si $G = G'$, on dit que f est un **endomorphisme** de G.
- Si en outre f est une bijection, on dit alors que f est un **automorphisme** de G.

Proposition 1.4

Soit $f : G \to G'$ un morphisme de groupes, alors

1- $f(e_G) = e'_{G'}$.

2- $\forall x \in G \ (f(x))^{-1} = f(x^{-1})$ *où* x^{-1} *est le symétrique de* x .

Preuve.

1- $f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G)$ en multipliant à droite par exemple par $f(e_G)^{-1}$ on obtient :

$$f(e_G) = e'_{G'}$$

2- Soit $x \in G$ alors $x * x^{-1} = e_G$ donc $f(x * x^{-1}) = f(e_G)$ .Cela entraine

$$f(x) \circ f\left(x^{-1}\right) = e'_{G'}$$

en composant à gauche par $(f(x))^{-1}$, nous obtenons

$$f\left(x^{-1}\right) = (f(x))^{-1}$$

■

Définition 1.12

Soit $(G, *)$ un groupe d'élément neutre e_G et soit $(G', *)$ un groupe d'élément neutre $e_{G'}$.

Soit f un morphisme de groupe de G vers G'.

On appelle image de f et on note $\mathbf{Im(f)}$ l'ensemble image de f c'est-à-dire :

$$\mathrm{Im}(\mathbf{f}) = \{y \in G' \ / \ \exists x \in G; y = f(x)\}.$$

On appelle noyau de f et on note $\mathbf{Ker(f)}$ l'image réciproque de $\{e_{G'}\}$ c'est-à-dire :

$$\ker(\mathbf{f}) = \{x \in G \ / \ f(x) = e_{G'}\} = f^{-1}(\{e_{G'}\}).$$

Exemple 1.10

Soit $f : \mathbb{Z} \to \mathbb{Z}$ définie par $f(k) = 3k$. C'est un morphisme du groupe $(\mathbb{Z}, +)$, dans le groupe $(\mathbb{Z}, +)$. Pour $k, k' \in \mathbb{Z}$, on a :

$$f(k + k') = 3(k + k') = 3k + 3k' = f(k) + f(k')$$

L'image de f est

$$\mathrm{Im}(f) = \{f(k) \setminus k \in \mathbb{Z}\} = \{3k \setminus k \in \mathbb{Z}\} = 3\mathbb{Z}$$

Le noyau de f est

$$\ker(f) = \{k \in \mathbb{Z} \setminus f(k) = 0\} = \{k \in \mathbb{Z} \setminus 3k = 0\} = \{k = 0\} = \{0\}$$

Théorème 1.7 ***(Première théoreme d'isomorphisme)***

Soit $f : G \to G'$ un homomorphisme de groupes. Alors, les groupes $G/\ker(f)$ et $\mathrm{Im}(f)$ sont isomorphes et on note $G/\ker f \simeq \mathrm{Im}\, f$.

Preuve.

Considérons

$$\begin{array}{rccc} \overline{f}: & G/Ker(f) & \to & f(G) \\ & \overline{x} & \to & \overline{f}(\overline{x}) = f(x). \end{array}$$

$\overline{f}$ est une application bien définie et on a aussi $\mathrm{Im}\,\overline{f} = \mathrm{Im}\, f$. D'autre part, $\overline{f}$ est un homomorphisme de groupes. En effet,

$$\overline{f}(\overline{x}\overline{x'}) = \overline{f}\left(\overline{xx'}\right) = f(xx') = f(x) f(x)'.$$

$\overline{f}$ est injectif car si

$$x \in G : \overline{f}(\overline{x}) = e', \text{alors } f(x) = e' \text{d'où } x \in \ker f, i.e., \overline{x} = \overline{e}$$

et aussi $\overline{f}$ est par définition surjectif. Ainsi $G/\ker f \simeq \mathrm{Im}\, f$ ■

1.2 Structures de Anneaux

1.2.1 Anneaux

Définition 1.13

Soit A un ensemble muni de deux lois de composition internes " $+$ " et " $\cdot$ " On dit que $(A, +, \cdot)$, ou simplement que A est un anneaux si :

(i) $(A, +)$ est un groupe commutatif.

(ii) La loi " $\cdot$ " est associative :

$$\forall a, b, c \in A : a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) La loi " $\cdot$ " est distributive par rapport à " $+$ " :

$$\forall a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c \text{ et } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Remarques 1.5

1- Si de plus la loi $\cdot$ est commutative, on dit que l'anneaux $(A, +, \cdot)$ (ou simplement A) est anneaux commutatif.

2- Si un anneaux $(A, +, \cdot)$ possède un élément neutre pour la loi " $\cdot$ ", on dit que l'anneaux A est unitaire. Dans ce cas, on note 1_A cet élément et on l'appelle unité de A.

Exemples 1.11

1- $(\mathbb{Z}, +, \times)$ est un anneaux commutatif unitaire.

2- De même $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ sont des anneaux commutatifs unitaires.

Définition 1.14 (Diviseur de zéros)

Soit A un anneaux et soit $x \in A$ avec $x \neq 0$, alors x est un diviseur de zéro s'il existe $y \in A$ tell que

$$x \cdot y = y \cdot x = 0$$

Définition 1.15 (Anneau intègre)

On appelle anneaux intègre tout anneaux distinct de l'anneaux nul et qui n'a pas de

diviseurs de zéros. Dans un anneaux intègre $(A, +, \times)$, on a :

$$\forall (a, b) \in A^2, a \times b = 0_A \Rightarrow a = 0_A \text{ ou } b = 0_A.$$

Exemples 1.12

1- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des anneaux intègres.

2- $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier, est un anneaux intègre.

Définition 1.16

Soit $(A, +, \times)$ un anneaux unitaire. On dit qu'un élément est inversible si et seulement si il admet un symétrique par rapport à la loi $\times$ c'est-à-dire :

$$x \in A \text{ et } x \text{ inversible} \Rightarrow \exists x' \in A \ / \ x \times x' = x' \times x = 1.$$

On note $U(A)$ l'ensemble des éléments inversibles de A (qui sont appelés aussi les unités de A).

Exemple 1.13

Les élément inversibles de $\mathbb{Z}$ sont $U(\mathbb{Z}) = \{-1, 1\}$.

1.2.2 Sous-anneaux

Définition 1.17

Soit $(A, +, \cdot)$ un anneaux et B une partie de A. On dit que B est un sous-anneaux de l'anneaux $(A, +, \cdot)$ si :

(i) $1_A \in B$.

(ii) $\forall a, b \in B, a - b \in B$.

(iii) $\forall a, b \in B, a \cdot b \in B$.

Exemples 1.14

1- $(\mathbb{Z}, \times)$ est un sous-anneaux de $(\mathbb{Q}, \times)$.

2- $(\mathbb{R}, +)$ est un sous-anneaux de $(\mathbb{C}, +)$.

3- Soit A un anneaux , A est un sous-anneaux de A mais $\{0\}$ n'est pas un sous anneaux de A si $A \neq \{0\}$.

1.2.3 Idéal d'un anneaux

Définition 1.18

Soit $(A, +, \cdot)$ un anneaux et I une partie de A. On dit que I est un idéal à gauche (resp. idéal à droite) de l'anneaux A si :

1) $\forall x, y \in I,\ x - y \in I$.

2) $\forall x \in I, y \in A, x \cdot y \in I$ et $y \cdot x \in I$.

Exemples 1.15

1- Les parties $\{0\}$ et A sont des idéaux de A.

2- Les ideaux de $(\mathbb{Z}, +, \times)$ sont les parties $n\mathbb{Z} = \{nx \ / \ x \in \mathbb{Z},\ n \in \mathbb{N}\}$.

Remarque 1.6

Tout idéal est un sous anneaux, mais la réciproque est en genérale fausse.

Exemple 1.16

Soit $A = (\mathbb{Q}, +, \times)$ et $I = (\mathbb{Z}, +, \times)$, I est un sous anneaux de A mais n'est pas un idéal de A.

1.2.4 Anneaux quotient

Définition 1.19

Considérons un anneaux commutatif A et I un idéal de A. Puisque $(A, +)$ est un groupe abélien et que I est un sous-groupe de A, on peut associer a I la relation d'équivalence $\Re$ sur A définie pour tous $x, y \in A$ par la condition

$$x \Re y \Leftrightarrow x - y \in I.$$

L'ensemble quotient A/I, muni de la loi de composition définie pour tous $x, y \in A$ par

$$(x + I) + (y + I) = (x + y) + I.$$

est un groupe abélien, d'élément neutre I i.e. la classe de 0. On va définir une seconde loi de composition sur A/I, appelée multiplication, de sorte que A/I soit, avec l'addition

précedente, muni d'une structure d'anneaux commutatif. Soient $x+I$ et $y+I$ des éléments de A/I. On définit la multiplication par la formule :

$$(x+I)(y+I) = xy + I$$

Pour que cette définition ait un sens, il convient de vérifier qu'elle ne dépend pas des représentants x et y de $x+I$ et de $y+I$. Soient x' et y' dans A tels que $x+I = x'+I$ et $y+I = y'+I$. Il existe r et t dans I tels que $x = x'+r$ et $y = y'+t$. On a

$$xy = x'y' + (x't + ry' + rt)$$

Puisque r et t sont dans I, il en est de même de $x't+ry'+rt$, par suite, $xy-x'y'$ appartient a I, d'où notre assertion.

Théorème 1.8

L'ensemble A/I muni de l'addition et la multiplication définies par les formules précedentes est un anneaux commutatif. On l'appelle l'anneaux quotient de A par I.

Preuve.

Soit x, y, z des élément de A alors on va montré que la loi définie sur l'ensemble quotient A/I est associative

$$\begin{aligned}
(x+I)((y+I)(z+I)) &= (x+I)(yz+I) \\
&= x(yz)+I \\
&= (xy)z+I \\
&= (xy+I)(z+I) \\
&= ((x+I)(y+I))(z+I)
\end{aligned}$$

Il reste a vérifier que la multiplication est distributive par rapport a l'addition. Soient x, y, z des éléments de A. On a les égalites

$$\begin{aligned}
(x+I)((y+I)+(z+I)) &= (x+I)((y+z)+I) \\
&= x(y+z)+I
\end{aligned}$$

$$
\begin{aligned}
&= xy + xz + I \\
&= (xy + I) + (xz + I) \\
&= (x + I)(y + I) + (x + I)(z + I)
\end{aligned}
$$

La deuxième égalité de la définition de la distributivité se vérifie de la même façon. ■

Remarque 1.7

l'anneaux A/I est trivial si et seulement si $I = A$.

Exemple 1.17

Soit $A = \mathbb{Z}$ et $I = n\mathbb{Z}$, on a $\mathbb{Z}/n\mathbb{Z}$ est un anneaux commutatif

On définit les deux application suivantes

$$
\begin{array}{rccc}
\oplus: & A/I \times A/I & \to & A/I \\
& (\overline{a}, \overline{b}) & \to & \overline{a} \oplus \overline{b} = \overline{a+b}
\end{array}
\qquad
\begin{array}{rccc}
\otimes: & A/I \times A/I & \to & A/I \\
& (\overline{a}, \overline{b}) & \to & \overline{a} \otimes \overline{b} = \overline{a \times b}
\end{array}
$$

Pour $\overline{a} = a + n\mathbb{Z}$ et $\overline{b} = b + n\mathbb{Z}$ on a

$$
\begin{aligned}
\overline{a} \oplus \overline{b} &= a + n\mathbb{Z} + b + n\mathbb{Z} \\
&= (a + b) + n\mathbb{Z}
\end{aligned}
$$

de même

$$
\begin{aligned}
\overline{a} \otimes \overline{b} &= (a + n\mathbb{Z})(b + n\mathbb{Z}) \\
&= ab + an\mathbb{Z} + bn\mathbb{Z} + n\mathbb{Z}n\mathbb{Z} \\
&= ab + n\mathbb{Z}
\end{aligned}
$$

1.2.5 Morphisme d'anneaux

Définition 1.20

Soit $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux (unitaires et non triviaux). On dit qu'une application f de A dans B est un morphisme d'anneaux (ou homomorphisme d'anneaux) si :

(i) $f(x + y) = f(x) + f(y)$ pour tout (x, y) élément de A^2.

(ii) $f(x.y) = f(x) \cdot f(y)$ pour tout (x, y) élément de A^2.

(iii) $f(1_A) = 1_B$.

Exemple 1.18

Si I est un idéal bilatère d'un anneaux A, l'application canonique $\pi : A \to A/I$ est un morphisme d'anneaux. On l'appelle le morphisme canonique.

Théorème 1.9 ***(Premier théoreme d'isomorphisme)***

Si $f : A \to B$ est un homomorphisme d'anneaux, alors les anneaux $A/\ker f$ et $\operatorname{Im} f$ sont isomorphes.

Preuve.

Soit $\overline{f} : A/\ker f \to \operatorname{Im} f$ définie par $\overline{f}(\overline{x}) = f(x)$. On sait que $\overline{f}$ est un isomorphisme de groupes (le premier théorème d'isomorphisme pour les groupes). D'autre part, on a

$$\overline{f}(\overline{1_A}) = f(1_A) = 1_B$$

et

$$\forall \overline{x}, \overline{y} \in A/\ker f : \overline{f}(\overline{x}\ \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$$

et ainsi f est un isomorphisme d'anneaux ■

1.3 Structures de Corps

1.3.1 Corps

Définition 1.21

Soit $(\Bbbk, +, \cdot)$ un anneau commutatif (unitaire et non trivial). On dit que $(\Bbbk, +, \cdot)$ est un corps (commutatif) si :

(i) $\Bbbk \neq \{0_A\}$.

(ii) Tout élément non nul de $\Bbbk$ est inversible.

Exemples 1.19

1- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ .sont des corps

2- $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier.

Théorème 1.10

L'anneaux $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Preuve.

Si n n'est pas premier, alors $n = ab$ avec $(a,\ b \neq \pm 1)$ et donc ni a ni b sont multiples de n. Ceci montre que dans $\mathbb{Z}/n\mathbb{Z}$ on a $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$, mais $\overline{a}\overline{b} = \overline{ab} = \overline{n} = 0$, donc $\mathbb{Z}/n\mathbb{Z}$ ne peut pas être un corps.donc il faut que n soit premier.

Inversement, si n est premier, montrons que tout élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z} - \left\{\overline{0}\right\}$ possède un inverse.On a a et n sont premiers entre eux, donc d'aprés Bézout il existe $u,\ v \in \mathbb{Z}$ tels que $au + nv = 1$ et donc $au = 1 \,(\mathrm{mod}\, n)$ et par suite dans $\mathbb{Z}/n\mathbb{Z}$ on a $\overline{au} = \overline{1}$. ■

1.3.2 Sous corps

Définition 1.22

Soit $(\Bbbk, +, \cdot)$ un corps et $\Bbbk'$ un sous-anneaux de $(\Bbbk, +, \cdot)$ on dit qu'une partie $\Bbbk'$ est un sous-corps du corps de $(\Bbbk, +, \cdot)$ si $(\Bbbk', +, \cdot)$ est un corps.

Exemples 1.20

1- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$.

2- $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$.

1.3.3 Morphisme de corps

Définition 1.23

On appelle morphisme du corps $(\Bbbk, +, \cdot)$ vers le corps $(\Bbbk', +, \cdot)$ toute application f de $\Bbbk$ vers $\Bbbk'$ telle que :

1- $\forall (x; y) \in \Bbbk^2, f(x + y) = f(x) + f(y)$.

2- $\forall (x; y) \in \Bbbk^2, f(x \cdot y) = f(x) \cdot f(y)$.

3- $f(1_{\Bbbk}) = 1_{\Bbbk'}$.

1.3.4 Corp finis

Définition 1.24

On appelle corps finis tout corps possedant un nombre fini d'éléments dit corps de Galois (Galois field).

Remarque 1.8

Le plus petit corps de Galois est $\mathbf{F}_2 = \left\{\overline{0}, \overline{1}\right\}$ muni de l'addition $(+)$ et de la multiplications $(\times)$ modulo 2.

$\overline{0}$ élément neutre de l'addition $(+)$.

$\overline{1}$ élément neutre de multiplication $(\times)$.

Exemples 1.21

1- Soit $\mathbf{F}_2 = \mathbb{Z}/2\mathbb{Z} = \left(\left\{\overline{0}, \overline{1}\right\}, +, \times\right)$, la table d'addition et multiplication de $\mathbb{Z}/2\mathbb{Z}$ sont :

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

2- Soit $\mathbf{F}_3 = \mathbb{Z}/3\mathbb{Z} = \left(\left\{\overline{0}, \overline{1}, \overline{2}\right\}, +, \times\right)$, la table d'addition et multiplication de $\mathbb{Z}/3\mathbb{Z}$ sont :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

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

Chapitre 2

Arithmétique finie

Dans ce chapitre on considère l'arithmétique sur l'anneaux quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ et plus particulièrement sur le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles par rapport à la multipliacation. Ce groupe se révélera trés important dans les applications pour le chapitre suivant, et plus particulièrement sur $\mathbb{Z}_p$ avec p premier. Dans ce paragraphe on donne quelques algorithmes pour le calcul du $PGCD$ de deux entiers ainsi que l'algorithme d'Euclide.

2.1 Arithmétique dans $\mathbb{Z}$

Dans le premier partie dans ce chapiter on donne quelques notions et propriétés sur l'arithmétique dans $\mathbb{Z}$, tels que nombre premier, division euclidienne, l'algorithme d'Euclide et l'algorithme d'Euclide étendu, théorème des reste chinois,....etc.

2.1.1 Division euclidienne

Définition 2.1

Soit $a, b \in \mathbb{Z}$. On dit que a est divisible par b s'il existe $q \in \mathbb{Z}$ tel que $a = qb$. Dans ce cas, on dit aussi que a est un multiple de b et b est un diviseur de a. On écrite $a \mid b$.

Théorème 2.1 ***(Division euclidienne)***

Soit a et b deux éléments de $\mathbb{Z}$, avec $b \neq 0$. Il existe un couple unique $(q, r) \in \mathbb{Z}^2$ vérifiant

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

On dit que q est le quotient et r le reste de la division euclidienne de a par b.

Preuve.

Existence, Soit L'ensemble $A = \{a - bk \ / \ k \in \mathbb{Z}\} \cap \mathbb{N}$ Vérifons que A n'est pas vide. Tel est le cas si $a \geq 0$, car alors a est dans A (on prend $k = 0$). Supposons $a < 0$. Si $b \geq 1$, on constate que $a(1 - b) \in A$ (prendre $k = a$) et si $b \leq -1$, alors $a(1 + b) \in A$ (prendre $k = -a$). D'aprés la propriété fondamentale satisfaite par $\mathbb{N}$, l'ensemble A possède donc un plus petit élément r. Parce que r appartient a A, on a $r \geq 0$ et il existe $q \in \mathbb{Z}$ tel que l'on ait $a - bq = r$. Il reste à vérifer que l'on a $r < |b|$. Supposons le contraire. On obtient

$$0 \leq r - |b| = a - bq - b = a - b(q + \xi) \in A \text{ avec } \xi = \pm 1$$

mais on a $0 \leq r - |b| < r$, ce qui contredit le fait que r est le plus petit élément de A.

Unicité. Supposons $a = bq_1 + r_1 = bq_2 + r_2$, avec $0 \leq r_1 < |b|$ et $0 \leq r_2 < |b|$. Si $q_1 \neq q_2$, supposons $q_1 - q_2 \geq 1$ par exemple, on écrit

$$b \leq b(q_1 - q_2) = r_2 - r_1 \leq r_2.$$

ce qui contredit l'hypothèse que $r_2 < b$.

On en déduit $q_1 = q_2$, et il s'en suit que $r_1 = r_2$. ■

Exemple 2.1

1- Division euclidienne de 17 par 5 :

$$17 = 5 \times 3 + 2 \text{ donc } q = 3 \text{ et } r = 2$$

2- Division euclidienne de -17 par 5 :

$$-17 = 5 \times (-4) + 3 \text{ donc } q = -4 \text{ et } r = 3$$

2.1.2 Quelque propriétés sur $\mathbb{Z}$

Définition 2.2 (Nombres premiers)

On appelle nombre premier, tout entier qui possède exactement 4 diviseurs dans $\mathbb{Z}$. les

seuls diviseurs sont les diviseurs triviaux ± 1 et $\pm p$. On noté $\mathcal{P}$ l'ensemble des nombres premiers.

Exemple 2.2

3 et -3 les deux sont des nombres premiers dans $\mathbb{Z}$.

Définition 2.3 (Décomposition en facteurs premiers)

Tout entier $n > 1$ se décompose d'une et d'une seule manière en un produit de nombres premiers. Autrement dit, pour tout entier $n > 1$, il existe des nombres premiers deux à deux distincts $p_1, p_2, ..., p_k$ et des entiers strictement positifs $\alpha_{1,}\alpha_{2,}, ..., \alpha_{k,}$, uniquement déterminés à l'ordre prés, tels que

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$$

Exemple 2.3

Pour $n = 120$, le nombre 120 se décompose en produit de nombre premiers c'est à dire

$$120 = 2^3 \times 3 \times 5$$

Définition 2.4 (PGCD)

Le plus grand commun diviseur (PGCD) de deux nombres a et b est un nombres d qui divise a et b et tel que tout diviseur commun de a et b divise aussi d en quelques sortes on a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Définition 2.5 (PPCM)

Le plus petit commun multiple (PPCM) de deux nombres a et b est un nombres m qui est un multiple de a et b et tel que tout multiple commun de a et b est multiple de m en quelques sortes on a $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Proposition 2.1

Soit p un nombre premier et soit $a \in \mathbb{Z}$. Alors ou bien p et a sont premiers entre eux, ou bien p divise a.

Preuve.

Soit $d = PGCD\,(a, p)$. Puisque d divise p et p est premier, d est égal à 1 ou à p.

Si $d = 1$, p et a sont premiers entre eux et on note $PGCD\,(a, p) = 1$.

Si $d = p$, p divise a. ■

Remarque 2.1

Si $a, b \in \mathbb{Z}$ on peut définir le sous-ensemble suivant de $\mathbb{Z}$

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv \ / \ u, v \in \mathbb{Z}\}$$

Proposition 2.2

Soit a et b deux entiers non nuls alors il existe deux entiers d et m tels que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. De plus l'entier d est le $PGCD$ de a et b, et m est le $PPCM$ de a et b. Enfin on a l'égalité $ab = \pm md$.

Preuve.

Soit $d \in \mathbb{Z}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, montrons que d est un $PGCD$ de a et b. Tout d'abord $a = a \cdot 1 + b \cdot 0$ est un multiple de d donc d divise a (et aussi b par le même raisonnement, on peut aussi écrire $d = au + bv$ pour certains entiers u, v par conséquent tout entier d' diviseur commun de a et b divise au, av et donc leur somme c'est à dire d.

Soit $m \in \mathbb{Z}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, montrons que m est un $PPCM$ de a et b. Tout d'abord $m \in a\mathbb{Z}$ donc m est un multiple de a (et aussi de b par le même raisonnement), si m' est un multiple de a et b alors $m' \in a\mathbb{Z}$ et $m' \in b\mathbb{Z}$ et donc $m' \in m\mathbb{Z}$ c'est à dire que m' est un multiple de m.

On sait donc que $a = a'd$ et $b = b'd$ donc $r = a'b'd$ est un multiple de a et b est donc divisible par m, donc md est divise $rd = ab$. Par ailleures, d'aprés la première partie du proposition, il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$ donc $md = aum + bvm$, mais ab divise am et bm donc md et on peut conclure $md = \pm ab$.

Si $PGCD\,(a, b) = 1$ on dit que a et b sont premiers entre eux. ■

Exemple 2.4

Soit $a = 120$ et $b = 32$ alors

$$d = PGCD\,(120, 32) = 8 \text{ et } m = PPCM\ \ (120, 32) = 480$$

donc

$$120 \times 32 = 3840 \text{ et } 480 \times 8 = 3840 \Rightarrow ab = md$$

Théorème 2.2 ***(Bézout)***

Soit $d = PGCD(a, b)$ alors il existe deux entiers u et v tels que :

$$au + bv = d$$

En particulier deux entiers a et b sont premiers entre eux si et seulement si'il existe u, v entiers tels que $au + bv = 1$.

Preuve.

La première partie de l'énoncé est une conséquence directe de la proposition précédente. Pout la deuxiéme partie, notons que si $PGCD(a, b) = 1$ alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Inversement si de tels u, v existent, alors un diviseur d de a et b diviserait $au + bv$ et donc 1 ce qui donne bien que a et b sont premiers entre eux. ■

Lemme 2.1 ***(Lemme de Gauss)***

Si $a \mid bc$ et si a est premier avec c, alors $a \mid b$.

Preuve.

Ils existent $u, v \in \mathbb{Z}$ tels que $au + cv = 1$, on multiplie par b, ce qui donne $bau + bvc = b$. On a $a \mid bc$ c'est à dire $bc = ak$, $k \in \mathbb{Z}$ alors on a

$$bau + bvc = b \Leftrightarrow bau + akv = b \Leftrightarrow a(bu + kv) = b \Leftrightarrow ak' = b \Leftrightarrow a \mid b.$$

Ce qui achève la preuve. ■

Lemme 2.2 ***(Eulide)***

Soit p un nombre premier et $a, b \in \mathbb{Z}$. Si p divise ab alors p divise a ou p divise b.

Preuve.

Si p ne divise pas a, alors a et p sont premiers entre eux, car les seuls diviseures de p sont 1 et lui même. D'aprés le lemme de Gauss, p doit alors diviser b. De même, si p ne divise b, il doit diviser a. ■

2.1.3 L'algorithme d'Euclide

L'algorithme d'Euclide est une méthode efficace pour déterminer le $PGCD$ de deux entiers

$$PGCD\,(a,b) = PGCD\,(b,r)$$

si $a = bq + r$ pour des entiers a, b, q et r. La démonstration de cette propriété est immédiate.

L'algorithme fonctionne alors ainsi. Supposons donnés deux entiers a et b positifs tels que $a > b$. On effectue la division euclidienne de a par b :

$$a = bq_0 + r_0$$

et d'aprés la propriété précédente, on est ramené à calculer le $PGCD$ des entiers b et r_0. Deux cas se présentent alors : si $r_0 = 0$, le $PGCD$ cherché est b. Sinon, on effectue la division euclidienne de b par r_0 :

$$b = r_0q_1 + r_1$$

et le $PGCD$ cherché vaut celui de r_0 et r_1. Si $r_1 = 0$, on a fini. Sinon, on continue.....

Les r_i forment une suite d'entiers positifs ou nuls strictement décroissante (d'aprés les propriétés de la division euclidienne). Cette suite ne peut pas être infinie, ce qui montre que l'algorithme doit s'arrêter. La description de cet algorithme prouve qu'il s'arrête automatiquement avec un reste nul. À ce moment, le précédent reste fournit le $PGCD$ cherché.

Soit a et b deux entiers positifs, on pose $r_0 = a$ et $r_1 = b$, et tant que $r_i > 0$ on effectues les divisions euclidiennes successives suivantes

$$\begin{aligned}
\text{de } a \text{ par } b &: r_0 = r_1q_1 + r_2, \text{ avec } 0 \leq r_2 < r_1.\\
\text{de } b \text{ par } r_1 &: r_1 = r_2q_2 + r_3, \text{ avec } 0 \leq r_3 < r_2.\\
&\vdots\\
&\vdots\\
\text{de } r_{n-2} \text{ par } r_{n-1} &: r_{n-2} = r_{n-1}q_{n-1} + r_n, \text{ avec } 0 \leq r_n < r_{n-1}.\\
\text{de } r_{n-1} \text{ par } r_n &: r_{n-1} = r_nq_n + r_{n+1}, \text{ avec } 0 \leq r_{n+1} \leq r_n \text{ et } r_{n+1} = 0.
\end{aligned}$$

Proposition 2.3

On a $PGCD\,(a,b) = r_n$, i.e. le PGCD de a et b et le dernier reste non nul dans cette série de divisions euclidiennes.

Preuve.

La suite des restes : $r_0, r_1, r_2, ..., r_n$ est une suite strictement décroissante dans $\mathbb{N}$ car $r_0 > r_1 > r_2 > ... > r_n$. Cette suite est donc finie. Il existe alors n tel que $r_{n+1} = 0$.

Montrons que $PGCD\,(a,b) = PGCD\,(b,r_0)$

Soit $D = PGCD\,(a,b)$ et $d = PGCD\,(b,r_0)$. D divise a et b donc D divise $a - bq_0 = r_0$, donc D divise b et r_0 donc : $D \leq d$, d divise b et r_0 donc d divise $bq_0 + r_0 = a$, donc d divise a et b donc : $d \leq D$

On déduit de ces deux inégalités que $D = d$: $PGCD\,(a,b) = PGCD\,(b,r_0)$.

De proche en proche, on en déduit que :

$$PGCD\,(a,b) = PGCD\,(b,r_0) = PGCD\,(r_0,r_1) = ... = PGCD\,(r_{n-1},r_n) = r_n$$

or r_n divise r_{n-1}, donc $PGCD\,(r_{n-1},r_n) = r_n$ car $r_{n+1} = 0$. ■

Exemple 2.5

Prenons $a = 59$ et $b = 27$. Alors

$$\begin{aligned} 59 &= 27 \times 2 + 5 \\ 27 &= 5 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Alors $PGCD\,(a,b) = 1$. Par suite, a et b sont premiers entre eux.

2.1.4 Algorithme d'Euclide étendu

A chaque étape de l'algorithme d'Euclide on a l'égalité de la forme

$$r_{k-2} = r_{k-1}q_{k-1} + r_k$$

L'algorithme d'Euclide étendu permet de déterminer $d = PGCD(a,b)$ ainsi que les deux

entiers u et v vérifiant

$$d = au + bv$$

Reprenons la suite des divisions euclidiennes et à chaque étape $k \geq 0$, calculons deux entiers u_k et v_k tels que

$$r_k = au_k + bv_k$$

Un coup d'oeil de la suite des divisions euclidiennes montre que $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ et $v_1 = 1$.
De la relation $(r_{k-1} = r_k q_k + r_{k+1})$, qu'on écrit

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k \\ &= au_{k-1} + bv_{k-1} - q_k \left(au_k + bv_k\right) \\ &= a\left(u_{k-1} - q_k u_k\right) + b\left(v_{k-1} - q_k v_k\right) \\ &= au_{k+1} + bv_{k+1} \end{aligned}$$

on déduit que pour $k \geq 1$, on a

$$\begin{cases} u_{k+1} = u_{k-1} - u_k q_k \\ v_{k+1} = v_{k-1} - v_k q_k \end{cases}$$

Si $d = r_n$ est le dernier reste non nul, on a $u = u_n$ et $v = v_n$.
D'où **l'algorithme d'Euclide étendu** :
Soit deux entiers positifs a et b. Pour déterminer $d = PGCD(a, b)$, ainsi que deux entiers u et v tels que $d = au + bv$, on écrit

$$\begin{cases} r_0 = a \\ u_0 = 1 \\ v_0 = 0 \end{cases}, \quad \begin{cases} r_1 = b \\ u_1 = 0 \\ v_1 = 1 \end{cases} \quad \text{et } \forall k \geq 1 \begin{cases} r_{k+1} = r_{k-1} - r_k q_k \\ u_{k+1} = u_{k-1} - u_k q_k \\ v_{k+1} = v_{k-1} - v_k q_k \end{cases}$$

jusqu'à obtenir un reste nul.

$$\begin{cases} d = r_n \\ u = u_n \\ v = v_n \end{cases}$$

Exemple 2.6

D'aprés l'exemple 2.4, on a

$$\begin{aligned}
1 &= 5 - 2 \times 2 \\
1 &= 5 - (27 - 5 \times 5) \times 2 \\
1 &= 5 - 27\,(2) + 5 \times 10 \\
1 &= 5\,(1 + 10) - 27\,(2) \\
1 &= 5\,(11) - 27\,(2) \\
1 &= (59 - 27 \times 2)\,(11) - 27\,(2) \\
1 &= 59\,(11) - 27\,(22) - 27\,(2) \\
1 &= 59 \times 11 + 27\,(-22 - 2) \\
1 &= 59 \times 11 + 27 \times (-24)
\end{aligned}$$

2.2 Arithmétique sur $\mathbb{Z}/n\mathbb{Z}$

Dans ce partie on donne quelques notions sur les congruences, théorème des reste chinois ainsi que fonction l'indicatrice d'Euler et le petit théoreme de Fermat,...,etc.

2.2.1 Congruences

Définition 2.6

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a et b sont congrus modulo n si l'entier n divise $a - b$, c-à-dire il existe un entier $k \in \mathbb{Z}$ tel que $a = b + kn$. On note

$$a \equiv b \bmod n \text{ ou } a \equiv b[n] \text{ ou } a \equiv_n b$$

Le fait que a et b sont congrus modulo n. Cette relation s'appelle relation de congruence modulo n.

Exemple 2.7

1- $7 \equiv 1 \bmod 6$ car $7 - 1 = 1 \times 6$ est divisible par 6.

2- $31 \equiv 11 \bmod 4$ car $31 - 11 = 20 = 5 \times 4$.

Proposition 2.4

La relation $\equiv_n$ est une relation d'équivalence sur $\mathbb{Z}$.

Preuve.

La relation est réflexive, car nous avons $a = a + 0 \times n$ pout tout $a \in \mathbb{Z}$ donc $a \equiv a \bmod n$.

La relation est symétrique, car si $a = b + kn$ alors $b = a + (-k)\, n$ donc $b \equiv a \bmod n$.

La relation est transitive, car si $a = b + kn$ et $b = c + gn$ alors $a = (c + gn) + kn = c + (g + k)\, n$ alors $a \equiv c \bmod n$. ■

Proposition 2.5

Si $a \equiv b \pmod n$ et $c \equiv d \pmod n$ alors

$$a + c \equiv b + d \pmod n \text{ et } ac \equiv bd \pmod n .$$

Preuve.

On a $a \equiv b \pmod n$ et $c \equiv d \pmod n$ c'est à dire $a = nk + b$ et $c = nj + d$, alors on obtient $a + c = nk + b + nj + d = b + d + n\,(k + j)$ alors $a + c \equiv b + d \pmod n$.

$ac = (b + kn)\,(d + nj) = bd + bnj + knd + kjnn = bd + n\,(bj + kd + kjn)$

et par suite $ac \equiv bd \pmod n$. ■

2.2.2 Classe de congruence inversibles

Définition 2.7 (Classe de congruence)

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. La classe de $a \bmod n$ est l'ensemble

$$\begin{aligned}
\overline{a} &= \{b \in \mathbb{Z} \mid a \equiv b \bmod n\} \\
&= \{b \in \mathbb{Z} \mid b \equiv a \bmod n\} \\
&= \{b \in \mathbb{Z} \mid n \backslash b - a\} \\
&= \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : b - a = kn\} \\
&= \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}
\end{aligned}$$

Exemple 2.8

Dans $\mathbb{Z}/4\mathbb{Z}$, on a

$\overline{1} = \{..., \ 1 - 3 \times 4 = -11, \ 1 - 2 \times 4 = -7, \ 1 - 1 \times 4 = -3, ...1, \ 1 + 1 \times 4 = 5, \ 1 + 2 \times 4 = 9, ...\}$

Définition 2.8 (Sommes et produit de classes)

On considère deux éléments $\overline{a}$ et $\overline{b}$ de $\mathbb{Z}/n\mathbb{Z}$. on définit la somme et le produit de $\overline{a}$ et $\overline{b}$ par

$$\begin{aligned} \overline{a} \oplus \overline{b} &= \overline{a+b} \\ \overline{a} \odot \overline{b} &= \overline{a \cdot b} \text{ qu'ou note plus simplement } \overline{ab} \end{aligned}$$

Exemple 2.9

Dans $\mathbb{Z}/6\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\right\}$, on a $\overline{5} + \overline{3} = \overline{5+3} = \overline{8} = \overline{2}$ et $\overline{2} \cdot \overline{5} = \overline{2 \cdot 5} = \overline{10} = \overline{4}$.

Définition 2.9

Soit $n \geq 2$ un entier, une classe de congruence $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible s'il existe une classe $\overline{b}$ telle que $\overline{a}\ \overline{b} = \overline{1}$. On note $(\mathbb{Z}/n\mathbb{Z})^{\times}$ l'ensemble des classes inversibles modulo n.

Exemple 2.10

Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\overline{3} \otimes \overline{3} = \overline{3 \times 3} = \overline{9} = \overline{1}$ car le reste de la division euclidienne de 9 par 4 est 1. Ainsi $\overline{3}$ est inversible et son inverse est lui-même : $\overline{3} \in (\mathbb{Z}/4\mathbb{Z})^{\times}$.

Théorème 2.3

Soit a un entier. Alors, $\overline{a}$ est inversible si et seulement si a et n sont premiers entre eux. Et par suite le groupe des classes inversibles modulo est :

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\overline{a} \mid 1 \leq a \leq n \text{ et } PGCD\,(a, n) = 1\}$$

Preuve. Supposons $\overline{a}$ inversible. Il existe alors $b \in \mathbb{Z}$ tel que $\overline{a}\overline{b} = \overline{1}$. Par suite, on a la congruence $ab \equiv 1 \bmod n$, autrement dit, il existe $c \in \mathbb{Z}$ tel que $ab + nc = 1$, ce qui prouve que a et n sont premiers entre eux.
Inversement, d'aprés le théorème de Bézout, s'il existe des entiers u et v tels que l'on ait $au + nv = 1$, on obtient $\overline{au} = \overline{1}$, ce qui signifie que $\overline{a}$ est inversible. ■

2.2.3 Systèmes de congruences. Théorème des restes chinois

Un système de congruences est un système de la forme

$$\begin{cases} x \equiv a_1 \,(\mathrm{mod}\, n_1) \\ x \equiv a_2 \,(\mathrm{mod}\, n_2) \\ \qquad \vdots \\ x \equiv a_k \,(\mathrm{mod}\, n_k) \end{cases}$$

Lemme 2.3 ***(Lemme de chinois)***

Soient $n_1, n_2 \in \mathbb{N}$, $n_1 \geq 2, n_2 \geq 2$, $PGCD\,(n_1, n_2) = 1$. *Soient* $u_1, u_2 \in \mathbb{Z}$ *tels que* $u_1 n_1 + u_2 n_2 = 1$. *Soient* $a_1, a_2 \in \mathbb{Z}$ *et* $a \in \mathbb{Z}$ *tels que* $a \equiv a_1 u_2 n_2 + a_2 u_1 n_1 \,(\mathrm{mod}\, n_1 n_2)$, *alors pour tout* $x \in \mathbb{Z}$ *on a :*

$$\begin{cases} x \equiv a_1 \,(\mathrm{mod}\, n_1) \\ x \equiv a_2 \,(\mathrm{mod}\, n_2) \end{cases} \Rightarrow x \equiv a \,(\mathrm{mod}\, n_1 n_2)$$

Remarque 2.2

On peut réinterpréter le lemme en disant que la solution générale $x \in \mathbb{Z}$ du système de congruences est donnée par :

$$x = a + k n_1 n_2$$

Preuve.

Soient $u_1, u_2, n_1, n_2, a_1, a_2, a$ vérifiant les hypothèse de lemme. Soit $x \in \mathbb{Z}$.
supposons que $x \equiv a \,(\mathrm{mod}\, n_1 n_2)$, $\exists k \in \mathbb{Z}$ tels que $x = a + k n_1 n_2$ alors

$$\begin{aligned} x &\equiv a \,(\mathrm{mod}\, n_1) \text{ et } a \equiv a_1 u_2 n_2 \,(\mathrm{mod}\, n_1) \\ a &\equiv a_1 \,(1 - u_1 n_1) \,(\mathrm{mod}\, n_1) \\ a &\equiv a_1 \,(\mathrm{mod}\, n_1) \end{aligned}$$

Donc $x \equiv a_1 \,(\mathrm{mod}\, n_1)$
on a de même $x \equiv a_2 \,(\mathrm{mod}\, n_2)$
Supposons maintenant que $x \equiv a_1 \,(\mathrm{mod}\, n_1)$ et $x \equiv a_2 \,(\mathrm{mod}\, n_2)$, $x - a$ est divisble par n_1 et par n_2, puisque les deux entier n_1 et n_2 sont premiers entre eux, il en résulte que $n_1 n_2$ divise $x - a$, c'est à dire $x \equiv a \,(\mathrm{mod}\, n_1 n_2)$. ■

Théorème 2.4 ***(Théoreme de chinois)***

Soient $p, q \in \mathbb{N}$ *tell que* $p \geq 2$ *et* $q \geq 2$ *et* $PGCD\,(p, q) = 1$. *Alors l'application définie*

par

$$\begin{array}{rccc}(\phi): & \mathbb{Z}/pq\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}\\ & \overline{x}_{pq} & \to & (\overline{x}_p,\overline{x}_q)\end{array}$$

est un isomorphisme d'anneaux.

Preuve.

Soient $x, y \in \mathbb{Z}$.

$$\begin{aligned}\phi\left(\overline{x}_{pq}+\overline{y}_{pq}\right) &= \phi\left(\overline{x+y}_{pq}\right)\\ &= \left(\overline{x+y}_p+\overline{x+y}_q\right)\\ &= \left(\overline{x}_p+\overline{y}_p,\overline{x}_q+\overline{y}_q\right)\\ &= \left(\overline{x}_p+\overline{x}_q\right)+\left(\overline{y}_p+\overline{y}_q\right)\\ &= \phi\left(\overline{x}_{pq}\right)+\phi\left(\overline{y}_{pq}\right)\end{aligned}$$

De même, on montre que $\phi\left(\overline{xy}_{pq}\right)=\phi\left(\overline{x}_{pq}\right)\times\phi\left(\overline{y}_{pq}\right)$.

Montrons maintenant que ϕ est surjective :

Soit $y_1, y_2 \in \mathbb{Z}$ et $x \in \mathbb{Z}$.

$$\phi\left(\overline{x}_{pq}\right)=\left(\overline{y_1}_p,\overline{y_2}_q\right) \text{ signifie } \overline{x}_p=\overline{y_1}_p, \overline{x}_q=\overline{y_2}_q$$

alors x est vérifie le système

$$\begin{cases} x\equiv y_1 \pmod p\\ x\equiv y_2 \pmod q\end{cases}$$

p et q étant premiers entre eux, on sait qu'il existe une solution de système (d'aprés le lemme de chinois) ϕ est surjective.

Montrons que ϕ est injective :

Soient $x, y \in \mathbb{Z}$.

$$\phi\left(\overline{x}_{pq}\right)=\phi\left(\overline{y}_{pq}\right) \text{ signifie } \overline{x}_{pq}=\overline{y}_{pq}, \text{ c'est à dire : } \begin{cases} x\equiv y \pmod p\\ x\equiv y \pmod q\end{cases}$$

$x-y$ est donc divisible par p et par q donc par pq car $PGCD(p,q)=1$, donc $x\equiv y \pmod{pq}$ c'est à dire $\overline{x}_{pq}=\overline{y}_{pq}$, donc ϕ est injective. Alors $\mathbb{Z}/pq\mathbb{Z}$ est bien isomorphe à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$. ■

Exemple 2.11

Soit le système

$$\begin{cases} x \equiv 2 \,(\mathrm{mod}\, 3) \\ x \equiv 3 \,(\mathrm{mod}\, 5) \\ x \equiv 2 \,(\mathrm{mod}\, 7) \end{cases}$$

On a $(3,5) = (5,7) = (3,7) = 1$ donc le système précédent admet un seul solution modulo $(3 \times 5 \times 7 = 105)$ d'aprés théoreme des reste chinois, et pour trouver la solution on remarque

$$x \equiv 2 \,(\mathrm{mod}\, 3) \Rightarrow x = 2 + 3k,\ k \in \mathbb{Z}$$

Alors

$$2 + 3k \equiv 3 \,(\mathrm{mod}\, 5) \Rightarrow 3k \equiv 1 \,(\mathrm{mod}\, 5)$$

on trouve l'inverse de 3 dans $\mathbb{Z}/5\mathbb{Z}$, $k = 3^{-1} = 2 \in \mathbb{Z}/5\mathbb{Z}$ et on obtient

$$k \equiv 2 \,(\mathrm{mod}\, 5) \Rightarrow k = 2 + 5t \ t \in \mathbb{Z}$$

donc

$$x = 8 + 15t$$

alors

$$8 + 15t \equiv 2 \,(\mathrm{mod}\, 7) \Rightarrow 15t \equiv -6 \,(\mathrm{mod}\, 7)$$

$$\Rightarrow 5t \equiv -2 \,(\mathrm{mod}\, 7) \Rightarrow t \equiv 1 \,(\mathrm{mod}\, 7) \Rightarrow t = 1 + 7m, m \in \mathbb{Z}$$

donc

$$x = 23 + 105m \Rightarrow x \equiv 23 \,(\mathrm{mod}\, 105)$$

2.2.4 Indicatrice d'Euler

Définition 2.10 (Fonction indicatrice d'Euler)

Pour tout $n \geq 1$, l'entier $\varphi(n)$ est le nombre des entiers compris entre 1 et n, et premiers avec n. Autrement dit, $\varphi(n)$ est le nombre des entiers a pour lesquels on a :

$$\varphi(n) = card\left((\mathbb{Z}/p\mathbb{Z})^{\times}\right)$$

ou bien

$$\varphi(n) = card\{a : 1 \leq a \leq n-1 \text{ et } PGCD(a,n) = 1\}$$

Exemples 2.12

1- $\varphi(8) = 4$ car parmi les nombres de 1 à 8, seuls les quatre nombres $1, 3, 5$ et 7 sont premiers avec 8.

2- $\varphi(1) = 1$ car 1 est premier avec lui-même, et $\varphi(2) = 1$.

3- La table de premières valeurs de l'indicatrice d'Euler pour $1 \leq n \leq 12$

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Théorème 2.5

Soit φ l'indicatrice d'Euler, Si m et n sont deux entiers positifs premiers entre eux, alors

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Preuve.

On a d'aprés la fonction d'indicatrice d'Euler $card(\mathbb{Z}/n\mathbb{Z})^{\times} = \varphi(n)$ pour entier $n > 0$.

On a donc d'aprés le théorème de restes chinois on a

$$card(\mathbb{Z}/mn\mathbb{Z})^{\times} = \varphi(mn) = card(\mathbb{Z}/n\mathbb{Z})^{\times} \times card(\mathbb{Z}/m\mathbb{Z})^{\times} = \varphi(m)\varphi(n)$$

■

Exemple 2.13

Soit $n = 6$. On a

$$\varphi(6) = \varphi(3)\varphi(2) = 2 \times 1 = 2$$

Corollaire 2.1

Soit n un entier positif, le groupe $(\mathbb{Z}/n\mathbb{Z})^{\times}$ est d'ordre $\varphi(n)$, où φ désigne l'indicatrice d'Euler.

Preuve.

Chaque élément de $\mathbb{Z}/n\mathbb{Z}$ est la classe d'un entier unique $a \in \mathbb{Z}$ tell que $1 \leq a \leq n$.

Comme $\varphi(n) = Card\{a \ / \ 1 \leq a \leq n \text{ et } PGCD(a,n) = 1\}$, la classe $\overline{a}$ d'un entier $a(\mathrm{mod}\, n)$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $PGCD(a,n) = 1$. Donc

$$\begin{aligned} \varphi(n) &= Card\{\overline{a} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} \text{ tels que } 1 \leq a \leq n\} \\ \varphi(n) &= Card\,(\mathbb{Z}/n\mathbb{Z})^{\times} \end{aligned}$$

■

2.2.5 Théorème d'Euler et petit théorème de Fermat

Théorème 2.6 ***(Euler)***

Soit $n \in \mathbb{N}$, $n > 1$. Soit $a \in \mathbb{Z}$ tel que $PGCD\,(a,n) = 1$. Alors :

$$a^{\varphi(n)} \equiv 1\,(\mathrm{mod}\, n)$$

Preuve.

Si a est premier avec n, alors $\overline{a}$ appartient à $(\mathbb{Z}/n\mathbb{Z})^{\times}$ qui est un groupe d'ordre $\varphi(n)$. Soit $g = \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. On a

$$Card\,(\mathbb{Z}/n\mathbb{Z})^{\times} = \varphi(n)$$

Par le théorème de Lagrange, on a $g^{\varphi(n)} = 1$. Ce qui implique que :

$$\overline{a}^{\varphi(n)} = \overline{1} \text{ et donc } a^{\varphi(n)} \equiv 1\,(\mathrm{mod}\, n)$$

■

Remarques 2.3

1- Comme lorsque p est premier, et $\varphi(p) = p - 1$ alors le corollaire de ce théoreme est le plus petit théorme de Fermat.

2- Pour tout nombre premier p et tout entier $r \geq 1$, on a

$$\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$$

3- Si $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ et $k \geq 1$, p_i premiers distincts, $n_i \geq 1$, $i = 1, 2, ..., k$, alors on a :

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p}\right)$$

Exemples 2.14

1- Soit $a = 4$ et $\mathbb{Z}/9\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\right\}$ alors $\varphi(9) = 6$ et donc $4^6 = 4096 \equiv 1 \pmod 9$.

2- Soit $a = 5$ et $\mathbb{Z}/7\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\right\}$ donc $\varphi(7) = 7 - 1 = 6$ et donc $5^6 = 15625 \equiv 1 \pmod 7$.

3- Soit $\varphi(60) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16$.

Corollaire 2.2 ***(petit théorème de Fermat)***

Soit p un nombre premier. Pour tout entier a non divisible par p, on a

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

En particulier, pour tout entier a, on a

$$a^p \equiv a \pmod p$$

Preuve.

Soit $a \in \mathbb{Z}$. On sait d'après la (**proposition 2.1**) qu'ou bien a est multiple de p ou bien a est premier avec p. Soit $\overline{a}$ la classe de a modulo p.

Si a est multiple de p, a^p est aussi multiple de p, on a donc

$$a^p \equiv a \equiv 0 (\mathrm{mod}\, p)$$

Si $PGCD(a, p) = 1$, alors $a \in (\mathbb{Z}/p\mathbb{Z})^*$ d'après le (**définition 2.10**).

Or $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre $p - 1$ donc $\overline{a}^{p-1} = \overline{1}$, ceci s'écrit $a^{p-1} \equiv 1 \pmod p$, il en résulte $a^p \equiv a \pmod p$. ■

Exemples 2.15

1- Soit $a = 2$ et $p = 7$, alors $2^{7-1} = 2^6 = 64 \equiv 1 \pmod 7$.

2- Soit $a = 3$ et $p = 5$, alors $3^{5-1} = 3^4 = 81 \equiv 1 \pmod 5$.

Chapitre 3

Réciprocité quadratique

Dans ce chapitre, on s 'interesse à l'ensemble des carreés dans le corps $\mathbf{F}_p, p$ premier. On introduit le symbole de Legendre et le symbole de Jacobi qui permet de caractériser ces carreés et on développe les principales propriétés de ce symbole. On démontre notamment la loi de réciprocité quadratique due à Gauss. Cette formule admet de nombreuses démonstration. Nous donnerons celle basée sur les sommes de Gauss.

3.1 La congruence $x^2 \equiv a \pmod{n}$

Dans cette partie, on va étudier la congruence

$$x^2 \equiv a \pmod{n}$$

On considère qu'ils existent trois types de problèmes. D'abord, il faut voir quand la solution existe, ensuite, combien y'a t'ils ? et enfin comment les trouver ?
Nous montrons qu'on peut réduire la congruence de la forme $x^2 \equiv a \pmod{n}$ à une même forme avec $(a, n) = 1$.
Supposons que $PGCD(a, n) > 1$.et soit p un nombre premier qui divise $PGCD(a, n)$, telle que $p \mid a$ et $p \mid n$. On suppose que x est une solution de $x^2 \equiv a \pmod{n}$. On a $p \mid x^2$ et pour cette raison $p \mid x$ on écrit $x = py$, alors la forme $x^2 \equiv a \pmod{n}$ est équivalente avec :

$$p^2y^2 \equiv a \pmod{n}$$

On divise par p pour obtenir

$$py^2 \equiv a/p \,(\mathrm{mod}\, n/p)$$

On distingue trois cas :
Si $p^2 \mid n$ et $p^2 \mid a$,alors, $py^2 \equiv a/p \,(\mathrm{mod}\, n/p)$ est équivalente à la congruence.

$$y^2 \equiv a/p^2 (\mathrm{mod}\, n/p^2)$$

pour chaque solution y_0 de cette congruence (s'il existe). il existe p une incongruente solution modulo n de la congruence originale $x^2 \equiv a \,(\mathrm{mod}\, n)$ il existe $x \equiv py_0 (\mathrm{mod}\, n/p)$, si $(a/p^2, n/p^2) > 1)$ on répète toute les étapes.
Si $p^2 \mid n$ mai $p^2 \nmid a$, alors $py^2 \equiv a/p \,(\mathrm{mod}\, n/p)$ est une contradiction.pour que

$$x^2 \equiv a \,(\mathrm{mod}\, n)$$

n'a pas des solutions dans ce cas.
Si $p^2 \nmid n$,et $(p, n/p) = 1$, et pour qu'il existe un nombre c, telle que $cp \equiv 1 (\mathrm{mod}\, n/p)$ la formule $py^2 \equiv a/p \,(\mathrm{mod}\, n/p)$ est équivalente de cette congruence $y^2 \equiv ca/p (\mathrm{mod}\, n/p)$ aucune solution y_0 de cette congruence admet une unique solution $x \equiv py_0 (\mathrm{mod}\, n)$ de

$$x^2 \equiv a \,(\mathrm{mod}\, n) \text{ si } (ca/p, n/p) > 1.$$

on peut répéter toute la procedure
on note que si p^2/a, alors $ca/p = cp.a/p^2 \equiv 1.a/p^2 \equiv a/p^2 (\mathrm{mod}\, n/p)$.
i.e, $py^2 \equiv a/p \,(\mathrm{mod}\, n/p)$ est équivalente de la congruence $y^2 \equiv a/p^2 (\mathrm{mod}\, n/p)$ dans ce cas.

Exemples 3.1

1- On a la congruence suivante

$$x^2 \equiv 36 \,(\mathrm{mod}\, 45)$$

On a $PGCD\,(45, 36) = 9$ donc on va écrit $x = 3y$ alors la congruence $x^2 \equiv 36 \,(\mathrm{mod}\, 45)$

équivalente a

$$\begin{aligned}(3y)^2 &\equiv 36\,(\mathrm{mod}\,45) \Rightarrow 9y^2 \equiv 36\,(\mathrm{mod}\,45)\\ &\Rightarrow y^2 \equiv 4\,(\mathrm{mod}\,5) \Rightarrow y^2 = 4 + 5k,\ k \in \mathbb{Z}\end{aligned}$$

Pour $k = 0$ on obtient

$$y^2 = 4 \Rightarrow y = \pm 2.$$

alors la solution particulier est

$$y \equiv \pm 2\,(\mathrm{mod}\,5) \Rightarrow x = \pm 6\,(\mathrm{mod}\,15)$$

i.e.l'ensembles des solution la congruence $x^2 \equiv 36\,(\mathrm{mod}\,45)$ est 6, 9, 21, 24, 36, et 39.

2- On a la congruence suivantes

$$x^2 \equiv 15\,(\mathrm{mod}\,45)$$

On a $PGCD\,(45, 15) = 15$ et on a $3 < 15$ donc $x = 3y$ alor $9 \mid 45$ mais $9 \nmid 15$ alors il n'admet pas solutions

3- On a la congruence suivantes

$$x^2 \equiv 15\,(\mathrm{mod}\,21)$$

On a $PGCD\,(21, 15) = 3$ on écrit $x = 3y$ et on a $9 \nmid 21$ et $PGCD\,(3, 7) = 1$, alors il existe c tels que $3c \equiv 1\,(\mathrm{mod}\,7)$ alor $c = 5$ donc on obtient

$$9y^2 \equiv 15\,(\mathrm{mod}\,21) \Rightarrow 3y^2 \equiv 5\,(\mathrm{mod}\,7)$$

On multiplie cette congruence $3y^2 \equiv 5\,(\mathrm{mod}\,7)$ par 5 on obtient

$$y^2 \equiv 4\,(\mathrm{mod}\,7) \Rightarrow y = \pm 2$$

alors on trouve

$$x \equiv \pm 6\,(\mathrm{mod}\,21)$$

3.2 Résidus quadratique et non-résidus dans $\mathbb{Z}/p\mathbb{Z}$

Définition 3.1

Soit p un nombres premier et a un entier tel que p ne devise pas a .Alors a est appelé un **résidu quadratique modulo p** si l'équation $x^2 \equiv a(\text{mod } p)$ posséde une solution .Dans le cas contraire a appelé un **non résidu quadratique modulo p.**

Autrement dit , soit $x \in \mathbb{Z}/n\mathbb{Z}$, on dit que x est un **carré** (ou un **résidu quadratique**) si il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x = y^2$, dans ce cas on dit que y est une racine **carré de x**.

Notation 3.1

Si a résidu quadratique modulo p on note aR_p, et si a non-résidu quadratique modulo p on note aN_p.

Exemples 3.2

1- La table des carrés dans $\mathbb{Z}/7\mathbb{Z}$. Les carrés sont $0, 1, 2, 4$.

x mod 7	0	1	2	3	4	5	6
x^2 mod 7	0	1	4	2	2	4	1

2- La table des carrés dans $\mathbb{Z}/10\mathbb{Z}$. les carrés sont $0, 1, 4, 5, 6, 9$.

x mod 10	0	1	2	3	4	5	6	7	8	9
x^2 mod 10	0	1	4	9	6	5	6	9	4	1

Théorème 3.2

p un nombre premier impaire alors : $\mathbf{F}_p^*$ contient $\frac{p-1}{2}$ et carré (résidu quadratique) et $\frac{p-1}{2}$ non carré (non-résidu quadratique), $\mathbf{F}_p$ contient $\frac{p+1}{2}$ carré.

Preuve. On pose

$$\begin{array}{rccc} \varphi: & \mathbf{F}_p^* & \rightarrow & \mathbf{F}_p^* \\ & x & \rightarrow & x^2 \end{array}$$

morphisme de groupes.

$$\ker\varphi = \left\{x \in \mathbf{F}_p^* \backslash x^2 = 1\right\} = \left\{x \in \mathbf{F}_p^* \backslash\, (x-1)\,(x+1) = 0\right\} = \{-1, +1\}$$

D'où $Card\ \{\ker\varphi\} = 2$ et comme φ morphisme de groupes, alors d'après le 1^{er} théorème

d'isomorphisme il vient $Card\left\{\mathbf{F}_p^*\right\} = Card\left\{\ker\varphi\right\} \times Card\left\{\operatorname{Im}\varphi\right\}$ alors

$$Card\left\{\operatorname{Im}\varphi\right\} = \frac{Card\left\{\mathbf{F}_p^*\right\}}{Card\left\{\ker\varphi\right\}} = \frac{p-1}{2}$$

Alors $\mathbf{F}_p^*$ contient $\frac{p-1}{2}$ carrés (résidus quadratique) et $\frac{p-1}{2}$ non carrés (non-résidus quadratique).

Les carrés de $\mathbf{F}_p$ sont donc un nombre de $\frac{p-1}{2}+1 = \frac{p+1}{2}$ puis que compter 0. ■

Exemple 3.3

Soit $p = 7$ un nombre premier impaire, alors dans $(\mathbb{Z}/7\mathbb{Z})^*$ les résidus quadratiques sont $\{1,\ 2,\ 4\}$, et les non-résidus quadratiques sont $\{3,\ 5,\ 6\}$.

Alors $Card\left\{a \in \mathbb{Z}_7^* \ :\ aR_7\right\} = Card\left\{a \in \mathbb{Z}_7^* \ :\ aN_7\right\} = \frac{7-1}{2} = 3$.

3.3 Critére d'Euler

Théorème 3.3 *(**Critére d'Euler**)*

Soit p un nombre premier impair, et a un entier tel que p ne divise pas a. Alors

(i) *a est un résidu quadratique modulo p si et seulement si*

$$a^{\frac{p-1}{2}} \equiv 1 \,(\operatorname{mod} p)$$

(ii) *a est un non-résidu quadratique modulo p si et seulement si*

$$a^{\frac{p-1}{2}} \equiv -1 \,(\operatorname{mod} p)$$

Preuve.

D'aprés la théoreme de Fermat, on a

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 \,(\operatorname{mod} p)$$

Donc $a^{\frac{p-1}{2}}$ est une solution de la congruence $x^2 \equiv 1(\operatorname{mod}\ p)$ et donc et comme $a^{p-1} \equiv 1(\operatorname{mod}\ p)$ pour tout a premier à p, nous avons

$$a^{\frac{p-1}{2}} \equiv \pm 1 \,(\operatorname{mod}\ p)$$

L'équation $x^{\frac{(p-1)}{2}} \equiv 1(\text{mod } p)$ a exactement $\frac{p-1}{2}$ solutions modulo p. Comme il ya $\frac{p-1}{2}$ résidus quadratique modulo p, les solutions de l'équation précédente sont exactement les résidu quadratique. Ainsi pour un non-résidu quadratique a, on a

$$a^{\frac{p-1}{2}} \equiv -1 \,(\text{mod}\, p)$$

De tout ceci, nous pouvons conclure que le théorème est vérifié. ■

Exemple 3.4

1- Soit $a = 5$ et $p = 23$ alors on obtient $5^{\frac{23-1}{2}} = 5^{11}$. Alors :

$$5^{11} \equiv -1 \,(\text{mod}\, 23)$$

2- Soit $a = 2$ et $p = 13$ alors on obtient $3^{\frac{13-1}{2}} = 3^6$. Alors

$$3^6 \equiv 729 \,(\text{mod}\, 13) \equiv 1 \,(\text{mod}\, 13)$$

3.4 Symbole de Legendre

Définition 3.2

Soit $a \in \mathbb{Z}$ On déffinit le symbole de Legendre noté $\left(\frac{a}{p}\right)$ par

$$\left(\frac{a}{p}\right) = \begin{cases} +1 \text{ si } a \text{ est un carré (résidu quadratque) modulo p} \\ -1 \text{ si } a \text{ n'est pas un carré (n'est pas résidu quadratque) modulo p} \\ 0 \text{ si } p \text{ devise } a \end{cases}$$

Remarque 3.1

$\left(\frac{1}{p}\right) = 1$, car 1 est le carré de lui-même.

Exemple 3.5

Soit p un nombre premier, $\left(\frac{a}{p}\right)$ pour $p < 70$ et $a = 2, 3, 5$.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67
$\left(\frac{2}{p}\right)$	-1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	-1	-1	-1
$\left(\frac{3}{p}\right)$	0	-1	-1	1	1	-1	-1	1	-1	-1	1	-1	-1	1	-1	1	1	-1
$\left(\frac{5}{p}\right)$	-1	0	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	-1	1	1	-1

Remarque 3.2

Soit p un nombre quelconque alors on a :

$$\left(\frac{a}{p}\right) = 1 \not\Rightarrow a \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z}$$

Exemple 3.6

Soit $a = 2$ et $p = 9$ alors on a $\frac{2}{9} = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = (-1)(-1) = 1$.Mais Dans $\mathbb{Z}/9\mathbb{Z}$ les carrés sont $0, 1, 4$ et 7.Donc 2 n'est pas un carré dans $\mathbb{Z}/9\mathbb{Z}$.

Remarque 3.3 Soit p un nombre premier impair. Parmi les entiers compris entre 1 et $p-1$, il y en a exactement la moitié qui sont des résidus quadratiques modulo p. On a donc la formule

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = \sum_{k=1}^{p-1}(-1)^k = 0$$

Notation 3.4 (Critére d'Euler)

Soient p un nombre premier impaire et a un entier. On a

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Proposition 3.1

Soit p un nombre premier et $a, b \in \mathbb{Z}$, $PGCD(a, p) = PGCD(b, p) = 1$ alors :

(i) ***(Modularité)*** *Si $a \equiv b \pmod{p}$ alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) ***(Multiplicativité)*** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) $\left(\frac{a^2}{p}\right) = 1$.

(iv) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Preuve.

(i) Si $a \equiv b \,(\mathrm{mod}\, p)$ alors $x^2 \equiv a \,(\mathrm{mod}\, p)$ admet a solution si et seulement si $x^2 \equiv b \,(\mathrm{mod}\, p)$ admet a solution alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) En utilisant le critére d'Euler on a :$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \,(\mathrm{mod}\ p)$ et $\left(\frac{b}{p}\right) = b^{\frac{p-1}{2}} \,(\mathrm{mod}\ p)$ alors :

$$\begin{aligned}\left(\frac{ab}{p}\right) &= (ab)^{\frac{p-1}{2}} \,(\mathrm{mod}\ p) \\ &= a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \,(\mathrm{mod}\ p) \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\end{aligned}$$

(iii) On a $\left(\frac{a}{p}\right) = \pm 1$ donc d'aprés **(ii)** on obtient :

$$\begin{aligned}\left(\frac{a^2}{p}\right) &= \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) \\ &= \pm 1 \cdot \pm 1 \\ &= 1.\end{aligned}$$

(iv) On a $\left(\frac{a^2}{p}\right) = 1$ donc d'aprés **(ii)** et **(iii)** on obtient

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)$$

■

3.4.1 La loi complémentaire

Caractère quadratique de -1

Proposition 3.2

Soit p un nombre premier impaire.Alor on a :

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \ si\ p \ \equiv 1 \,(\ \mathrm{mod}\, 4) \\ -1 \ si\ p \ \equiv 3 \,(\ \mathrm{mod}\, 4) \end{cases}$$

De façon équivalente on a :$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Preuve.

Observons que

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si p } \equiv 1 \,(\mod 4) \\ -1 \text{ si p } \equiv 3 \,(\mod 4) \end{cases}$$

D'autre part en appliquant le critére d'Euler on a

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \,(\mod\ p)\,.$$

Si $p \equiv 1 \,(\mod 4)$ alor $p = 4k+1, k \in \mathbb{Z}$ donc, $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$ alors $\left(\frac{-1}{p}\right) = 1$.
Si $p \equiv 3 \,(\mod 4)$ alor $p = 4k+3, k \in \mathbb{Z}$ donc, $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$ alors $\left(\frac{-1}{p}\right) = -1$.
Donc le résultas suit immédiatement car chacun des termes de la congruence et ± 1. ■

Caractère quadratique de 2

Proposition 3.3

Soit p un nombre premier impaire. Alors on a :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \ si\ p \equiv \pm 1 \,(\mod 8) \\ -1 \ si\ p \equiv \pm 3 \,(\mod 8) \end{cases}$$

Preuve.

D'aprés le critére de Euler, 2 est un racine carrés modulo p si et seulement si

$$2^{\frac{p-1}{2}} \equiv 1 \,(\mod\ p)$$

Alors en utilisant l'expression $(-1)^{\frac{p-1}{4}}$ pour $\frac{p-1}{2}$ pair et $(-1)^{\frac{p+1}{4}}$ pour $\frac{p-1}{2}$ impaire on obtient

$$\begin{aligned}
p &= 8k+1 \Rightarrow 2^{\frac{(8k+1)^2-1}{8}} \equiv (-1)^{\frac{64k^2+16k}{8}} \equiv (-1)^{8k^2+2k} \equiv (-1)^{2l} \equiv 1 \,(\mod\ p)\,. \\
p &= 8k-1 \Rightarrow 2^{\frac{(8k-1)^2-1}{8}} \equiv (-1)^{\frac{64k^2-16k}{8}} \equiv (-1)^{8k^2-2k} \equiv (-1)^{2l} \equiv 1 \,(\mod\ p)\,. \\
p &= 8k+3 \Rightarrow 2^{\frac{(8k+3)^2-1}{8}} \equiv (-1)^{\frac{64k^2+48k+8}{8}} \equiv (-1)^{8k^2+6k+1} \equiv (-1)^{2l+1} \equiv -1 \,(\mod\ p)\,. \\
p &= 8k-3 \Rightarrow 2^{\frac{(8k-3)^2-1}{8}} \equiv (-1)^{\frac{64k^2-48k+8}{8}} \equiv (-1)^{8k^2-6k+1} \equiv (-1)^{2l+1} \equiv -1 \,(\mod\ p)\,.
\end{aligned}$$

tels que si $p = 8k \pm 1$, on a $l = 4k^2 \pm k$ et si $p = 8k \pm 3$ on a $l = 4k^2 \pm 3k$. ■

3.4.2 La loi de réciprocité quadratique

Proposition 3.4

Soient p et q deux nombres premiers impairs, on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Remarque 3.4

On peut énoncer la proposotion de réciprocité quadratique de la façon suivante :

Soient p et q deux nombres premiers impairs, on a :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1 \,(\mod 4) \text{ ou } q \equiv 1 \,(\mod 4) \\ -1 \text{si } p \equiv q \equiv 3 \,(\mod 4) \end{cases}$$

Preuve.

Pour p,q nombre premier impair, alors $\frac{p-1}{2}\frac{q-1}{2}$ est un nombre pair si et seulement si p ou q s'écrit sous la forme $4k+1$, alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$$

Si $p \equiv q \equiv 3 \,(\mod 4)$ alors $\frac{p-1}{2}\frac{q-1}{2}$ est un nombre impair i,e.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$$

■

Corollaire 3.1

Soient p et q deux nombres premiers impairs, on a :

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) \; si \; p \equiv 1 \,(\mod 4) \; ou \; q \equiv 1 \,(\mod 4) \\ -\left(\frac{q}{p}\right) \; si \; p \equiv q \equiv 3 \,(\mod 4) \end{cases}$$

Preuve.

Si $p \equiv 1 \,(\mod 4)$ ou $q \equiv 1 \,(\mod 4)$ alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ D'aprés la (**Remarque 3.4**)

donc

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = \left(\frac{q}{p}\right)$$

On a $\left(\frac{q}{p}\right)^2 = 1$ alors $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
Si $p \equiv q \equiv 3\,(\mod 4)$ alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ D'aprés la (**Remarque 3.4**) donc

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = -\left(\frac{q}{p}\right)$$

On a $\left(\frac{q}{p}\right)^2 = 1$ alors $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ ■

3.4.3 Exemple

On va de nouveau utiliser les règles énoncées ci-dessus pour calculer $\left(\frac{541}{2011}\right)$.

$$\begin{aligned}
\left(\frac{541}{2011}\right) &= \left(\frac{2011}{541}\right) \text{ réciprocité } 541 \equiv 1\,(4)\,. \\
&= \left(\frac{388}{541}\right) \text{ modularité } 2011 \equiv 388\,(541)\,. \\
&= \left(\frac{2}{541}\right)^2\left(\frac{97}{541}\right) \text{ multiplicativité } 388 = 2^2 \times 97. \\
&= \left(\frac{97}{541}\right) \\
&= \left(\frac{541}{97}\right) \text{ réciprocité } 541 \equiv 1\,(4)\,. \\
&= \left(\frac{56}{97}\right) \text{ modularité } 541 \equiv 56\,(97)\,. \\
&= \left(\frac{2}{97}\right)^3\left(\frac{7}{97}\right) \text{ multiplicativité } 56 = 2^3 \times 7. \\
&= \left(\frac{2}{97}\right)^3\left(\frac{97}{7}\right) \text{ réciprocité } 97 \equiv 1\,(4)\,. \\
&= \left(\frac{-1}{7}\right)\left(\frac{2}{97}\right)^3 \text{ modularité } 97 \equiv -1\,(7)\,. \\
&= (-1)\,(1)^3 \text{ la loi complémentaire } \left(\frac{-1}{7}\right) = -1 \text{ et } \left(\frac{2}{97}\right) = 1 \\
&= -1
\end{aligned}$$

3.5 Symbole de Jacobi

Définition 3.3

Soit n un entier positif impair dont la composition en facteurs premiers est $n = p_1^{\alpha_1} p_2^{\alpha_2} .....p_k^{\alpha_k}$.
Le symbole de jacobi $\left(\frac{m}{n}\right)$ est définie par :

$$\begin{aligned}\left(\frac{m}{n}\right) &= \left(\frac{m}{p_1}\right)^{\alpha_1}\left(\frac{m}{p_2}\right)^{\alpha_2}..... \left(\frac{m}{p_k}\right)^{\alpha_k} \\ &= \prod_{i=0}^{k}\left(\frac{m}{p_i}\right).\end{aligned}$$

Proposition 3.5

Soient m, n, a, b quatre entiers avec $m, n > 1$ impairs.On a

$$\begin{aligned}\left(\frac{a}{m}\right)\left(\frac{b}{m}\right) &= \left(\frac{ab}{m}\right). \\ \left(\frac{a}{m}\right)\left(\frac{a}{n}\right) &= \left(\frac{a}{mn}\right).\end{aligned}$$

Preuve. La preuve de ces égalités réside en les propriétés du symbole de Legendre et la définition du symbole de Jacobi. On écrit les décomposition $m = m_1 m_2 ... m_s$ et $n = n_1 n_2 ... n_r$ en produit de nombres premiers. On a alors :

$$\begin{aligned}\left(\frac{ab}{m}\right) &= \prod_{i=1}^{k}\left(\frac{ab}{m_i}\right) = \prod_{i=1}^{k}\left(\frac{a}{m_i}\right)\left(\frac{b}{m_i}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) \\ \left(\frac{a}{mn}\right) &= \prod_{i=1}^{s}\prod_{j=1}^{r}\left(\frac{a}{m_i}\right)\left(\frac{a}{n_j}\right) = \prod_{i=1}^{s}\left(\frac{a}{m_i}\right)\prod_{j=1}^{r}\left(\frac{a}{n_j}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)\end{aligned}$$

■

Lemme 3.1

Soit $a, b \in \mathbb{Z}$ deux éléments positive impairs on a :

1- $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2$.

2- $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{(ab)^2-1}{8} \pmod 2$.

Preuve.

1- Pour $a - 1 \equiv 0 \pmod 4$ et $b - 1 \equiv 0 \pmod 4$ on a :

$$\begin{aligned}(a-1)(b-1) &\equiv 0\,(\text{mod } 4)\\ ab-a-b+1 &\equiv 0\,(\text{mod } 4)\\ ab-1 &\equiv (a-1)+(b-1)\,(\text{mod } 4)\\ \frac{ab-1}{2} &\equiv \frac{(a-1)}{2}+\frac{(b-1)}{2}\,(\text{mod } 2)\end{aligned}$$

2- On a $a^2-1\equiv 0\,(\text{mod}\,4)$ et $b^2-1\equiv 0\,(\text{mod}\,4)$. Alors

$$\begin{aligned}\left(a^2-1\right)\left(b^2-1\right) &\equiv 0\,(\text{mod}\,16)\\ a^2b^2-a^2-b^2+1 &\equiv 0\,(\text{mod}\,4)\\ a^2b^2-1 &\equiv \left(a^2-1\right)+\left(a^2-1\right)\,(\text{mod}\,16)\\ \frac{(ab)^2-1}{8} &\equiv \frac{(a^2-1)}{8}+\frac{(b^2-1)}{8}\,(\text{mod}\,2)\end{aligned}$$

■

3.5.1 La loi complémentaire

Caractére quadratique de -1

Proposition 3.6

Pour m impair on a :

$$\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}=\begin{cases}1\ si\ m\ \equiv 1\,(\ \text{mod}\,4)\\ -1\ si\ m\ \equiv 3\,(\ \text{mod}\,4)\end{cases}$$

Preuve.

Si m est un nombre impair alors on pose $m=p_1p_2$:

$$\begin{aligned}\left(\frac{-1}{m}\right) &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\\ \left(\frac{-1}{m}\right) &= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\\ \left(\frac{-1}{m}\right) &= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}}\end{aligned}$$

$$\begin{aligned}\left(\frac{-1}{m}\right) &= (-1)^{\frac{p_1p_2-1}{2}} \text{ D'aprés (\textbf{lemme 3.1})}\\ \left(\frac{-1}{m}\right) &= (-1)^{\frac{m-1}{2}} \pmod 2\end{aligned}$$

■

Caractére quadratique de 2

Proposition 3.7

Pour m impair on a :

$$\left(\frac{2}{m}\right) = \begin{cases} 1 \text{ si } m \equiv \pm 1 \pmod 8 \\ -1 \text{ si } m = \pm 3 \pmod 8 \end{cases}$$

Preuve.

Si m est un nombre impair alors on pose $m = p_1p_2$:

$$\begin{aligned}\left(\frac{2}{m}\right) &= \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\\ \left(\frac{2}{m}\right) &= (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\\ \left(\frac{2}{m}\right) &= (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}}\\ \left(\frac{2}{m}\right) &= (-1)^{\frac{(p_1p_2)^2-1}{8}} \text{ D'aprés (\textbf{lemme 3.1})}\\ \left(\frac{2}{m}\right) &= (-1)^{\frac{m^2-1}{8}} \pmod 2\end{aligned}$$

■

3.5.2 La loi de réciprocité quadratique

Théorème 3.5 ***(La loi de réciprocité quadratique)***

Soient m et $M \geq 3$ des entiers naturels impairs. On a :

$$\left(\frac{M}{m}\right)\left(\frac{m}{M}\right) = (-1)^{\frac{(M-1)(m-1)}{4}}.$$

Preuve.

Ecrivons les décompositions $m = m_1 m_2 ... m_l$ et $M = M_1 M_2 ... M_r$ en produit de nombres premiers.

$$\left(\frac{M}{m}\right)\left(\frac{m}{M}\right) = \prod_{i=1}^{r}\prod_{j=1}^{l}\left(\frac{M_i}{m_j}\right)\left(\frac{m_j}{M_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{l}(-1)^{\frac{(M_i-1)\left(m_j-1\right)}{4}} = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{l}\frac{(M_i-1)\left(m_j-1\right)}{4}}$$

Dans ce cas en va montrer

$$(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{l}\frac{(M_i-1)\left(m_j-1\right)}{4}} = (-1)^{\frac{(M-1)(m-1)}{4}}$$

i.e,

$$(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{l}\frac{(M_i-1)\left(m_j-1\right)}{4}} \equiv (-1)^{\frac{(M-1)(m-1)}{4}} \pmod 2$$

On a

$$\sum_{i=1}^{r}\sum_{j=1}^{l}\frac{(M_i-1)(m_j-1)}{4} = \left(\sum_{i=1}^{r}\frac{(M_i-1)}{2}\right)\left(\sum_{j=1}^{l}\frac{(m_j-1)}{2}\right)$$

Daprés (lemme 3.2) on obtient

$$\begin{aligned}\left(\sum_{i=1}^{r}\frac{(M_i-1)}{2}\right) &\equiv \frac{\prod_{i=1}^{r}M_i - 1}{2} \pmod 2 \equiv \frac{M-1}{2} \pmod 2\\ \left(\sum_{j=1}^{l}\frac{(m_j-1)}{2}\right) &\equiv \frac{\prod_{j=1}^{l}m_j - 1}{2} \pmod 2 \equiv \frac{m-1}{2} \pmod 2\end{aligned}$$

Donc

$$\sum_{i=1}^{r}\sum_{j=1}^{l}\frac{(M_i-1)(m_j-1)}{4} \equiv \frac{M-1}{2}\frac{m-1}{2} \pmod 2$$

■

3.5.3 Exemple

On va de nouveau utiliser les règles énoncées ci-dessus pour calculer $\left(\frac{68}{233}\right)$.

$$\begin{aligned}\left(\frac{68}{233}\right) &= \left(\frac{233}{68}\right) \text{ car } 233 \equiv 1 \bmod 4\\ &= \left(\frac{29}{68}\right) \text{ car } 233 \equiv 29 \bmod 68\end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{68}{29}\right) \text{ car } 29 \equiv 1 \bmod 4 \\
&= \left(\frac{10}{29}\right) \text{ car } 68 \equiv 10 \bmod 29 \\
&= \left(\frac{2}{29}\right)\left(\frac{5}{29}\right) \text{ car } 10 = 2 \times 5 \\
&= -\left(\frac{5}{29}\right) \text{ car } 29 \equiv -3 \bmod 8 \\
&= -\left(\frac{29}{5}\right) \text{ car } 5 \equiv 1 \bmod 4 \\
&= -\left(\frac{4}{5}\right) \text{ car } 29 \equiv 4 \bmod 5 \\
&= -1 \text{ car } PGCD\,(5,4) = 1
\end{aligned}
$$

3.6 Sommes de Gauss

Les sommes de Gauss sont trés importantes en arithmétique. Nous allons les utiliser pour donner une démonstartion de la loi de réciprocité quadratique. Nous les utiliserons également pour calculer le nombre de solution modulo p d'une équation quadratique. Dans cette section, nous introduisons ces sommes et donnons quelques formules utiles pour démontrés la loi de réciprocité quadratique.

Définition 3.4

Soient p et q deux nombres premiers impairs distincts, et α une racine primitive $p-ième$ de l'unité dans une extension de $\mathbf{F_q}$.

On appelle alors Somme de Gauss dans $\mathbf{F_q}$ sur la forme suivante :

$$\tau\,(a) = \sum_{x \in \mathbf{F}_p} \left(\frac{x}{p}\right) \alpha^{ax}$$

Théorème 3.6

Soient $\Bbbk$ un corps de caractéristique q, soit p un nombre premier impaire, $p \neq q$. Alors La somme de Gauss τ vérifie les identités suivantes :

(i) *Pour tout $a \in \mathbf{F_p^*}$*

$$\tau\,(a) = \left(\frac{a}{p}\right) \tau\,(1)$$

(ii) $\tau(1)^2 = \left(\frac{-1}{p}\right) p$

(iii) *Si q est nombre premier impaire, pour tout $a \in \mathbf{F}_\mathbf{p}^*$, on a*

$$\tau(\alpha)^{q-1} = \left(\frac{a}{p}\right)$$

Preuve.

(i) L'application $x \to ax$ est une bijection de $\mathbf{F}_\mathbf{p}^*$ sur $\mathbf{F}_\mathbf{p}^*$. On a donc

$$\begin{aligned}\tau(\alpha) &= \sum_{y \in \mathbf{F}_p^*} \left(\frac{a^{-1}y}{p}\right) \alpha^y \\ &= \sum_{y \in \mathbf{F}_p^*} \left(\frac{a^{-1}}{p}\right)\left(\frac{y}{p}\right) \alpha^y \\ &= \left(\frac{a^{-1}}{p}\right) \tau(1)\end{aligned}$$

Or $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$ car $\left(\frac{a}{p}\right) \in \{-1, 1\}$. D'où $\tau(a) = \left(\frac{a}{p}\right)\tau(1)$.

(ii) Pour simplifier, nous noterons $\tau = \tau(1)$. En utilisant **Multiplicativité de symbole de Legendre,** on a

$$\tau^2 = \left(\sum_{x \in \mathbf{F}_p^*} \left(\frac{x}{p}\right) \alpha^x\right)\left(\sum_{y \in \mathbf{F}_p^*} \left(\frac{x}{p}\right) \alpha^y\right) = \sum_{x,y \in \mathbf{F}_p^*} \left(\frac{xy}{p}\right) \alpha^{x+y}$$

Si on effectue le changment de variable $t = x^{-1}y$, on a $y = xt$ et donc $xy = x^2 t$.

D'où

$$\left(\frac{xy}{p}\right) = \left(\frac{x^2 t}{p}\right) = \left(\frac{x^2}{p}\right)\left(\frac{t}{p}\right) = \left(\frac{t}{p}\right)$$

Donc

$$\tau^2 = \sum_{x,t \in \mathbf{F}_p^*} \left(\frac{t}{p}\right) \alpha^{x(1+t)} = \sum_{t \in \mathbf{F}_p^*} \left(\frac{t}{p}\right)\left(\sum_{x \in \mathbf{F}_p^*} \alpha^{x(1+t)}\right)$$

Si $1 + t \equiv 0 \pmod{p}$, alors $\alpha^{x(1+t)} = 1$ donc

$$\sum_{x \in \mathbf{F}_p^*} \alpha^{x(1+t)} = p - 1$$

Si $1 + t \neq 0 \pmod{p}$, alors l'application $x \to x(1+t)$ est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$,

d'où

$$\sum_{x\in\mathbf{F}_p^*}\alpha^{x(1+t)}=\alpha+\alpha^2+...+\alpha^{p-1}=-1$$

Ainsi

$$\tau^2=\left(\frac{-1}{p}\right)(p-1)-\sum_{t\in\mathbf{F}_p^*,t\neq-1}\left(\frac{t}{p}\right)=\left(\frac{-1}{p}\right)p-\sum_{t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right)$$

D'aprés (**Remarque 3.3**) on obtient

$$\tau^2=\left(\frac{-1}{p}\right)p$$

(iii) Remarquons que $\left(\frac{a}{p}\right)^{q-1}=1$, donc d'aprés **(i)**, il suffit de prouver le résultas pour $a=1$. En notant $\tau=\tau(1)$, comme la caractéristique de $\sum_p(\Bbbk)$ est égale à q, on a

$$\tau^q=\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)^q\alpha^{qx}$$

Or comme q est impair, on a

$$\left(\frac{x}{p}\right)^q=\left(\frac{x}{p}\right)$$

d'où

$$\tau^q=\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)^q\alpha^{qx}=\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\alpha^{qx}=\left(\frac{q}{p}\right)\sum_{x\in\mathbf{F}_p^*}\left(\frac{qx}{p}\right)\alpha^{qx}$$

L'application $x\to qx$, est une bijection de $\mathbf{F}_p^*$ sur $\mathbf{F}_p^*$, d'où

$$\tau^q=\left(\frac{q}{p}\right)\sum_{x\in\mathbf{F}_p^*}\left(\frac{x}{p}\right)\alpha^x=\left(\frac{q}{p}\right)\tau$$

Or d'aprés (ii), $\tau\neq0$, alors

$$\tau^{q-1}=\left(\frac{q}{p}\right)$$

■

3.6.1 La loi de réciprocité quadratique

Théorème 3.7 ***(Gauss)***

Soient p et q deux nombres premiers impairs distincts. On a

$$\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$$

Preuve.

D'aprés critère d'Euler et le (**théorème 3.6**), on obtient les égalités suivantes

$$\left(\frac{p}{q}\right) = p^{\frac{(q-1)}{2}} = \left(\left(\frac{-1}{p}\right)\tau^2\right)^{\frac{(q-1)}{2}}$$

$$\left(\frac{-1}{p}\tau^2\right)^{\frac{(q-1)}{2}} = (-1)^{\frac{(q-1)(p-1)}{4}}\,\tau^{q-1}$$

$$(-1)^{\frac{(q-1)(p-1)}{4}}\,\tau^{q-1} = (-1)^{\frac{(q-1)(p-1)}{4}}\left(\frac{q}{p}\right)$$

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(q-1)(p-1)}{4}}\left(\frac{q}{p}\right)$$

ce qui termine la démonstration de la Loi de réciprocité quadratique. ■

3.6.2 Exemple

Vérifons que l'on a $\left(\frac{1956}{2311}\right) = 1$.

En utilisant la loi de réciprocité, on obtient

$$\begin{aligned}
\left(\frac{1956}{2311}\right) &= \left(\frac{3}{2311}\right)\left(\frac{5}{2311}\right)\left(\frac{131}{2311}\right)\\
\left(\frac{3}{2311}\right) &= \left(\frac{2311}{3}\right)(-1)^{1155\times 1} = -\left(\frac{1}{3}\right) = -1 \text{ car } 2311 \equiv 1\,(\text{mod } 3)\\
\left(\frac{5}{2311}\right) &= \left(\frac{2311}{5}\right)(-1)^{1155\times 2} = \left(\frac{1}{5}\right) = 1 \text{ car } 2311 \equiv 1\,(\text{mod } 5)\\
\left(\frac{131}{2311}\right) &= \left(\frac{2311}{131}\right)(-1)^{1155\times 65} = -\left(\frac{84}{131}\right) \text{ car } 2311 \equiv 84\,(\text{mod } 131)\\
-\left(\frac{84}{131}\right) &= -\left(\frac{4}{131}\right)\left(\frac{3}{131}\right)\left(\frac{7}{131}\right)\\
&= -\left(\frac{3}{131}\right)\left(\frac{7}{131}\right)\\
&= -\left(\frac{131}{3}\right)(-1)^{65\times 1}\left(\frac{131}{7}\right)(-1)^{65\times 3}\\
&= -\left(\frac{2}{3}\right)\left(\frac{5}{7}\right) = -(-1)\left(\frac{7}{5}\right)(-1)^{3\times 2} = \left(\frac{2}{5}\right)\\
&= -1
\end{aligned}$$

Donc

$$\left(\frac{1956}{2311}\right) = (-1)\,(1)\,(-1) = 1$$

Conclusion

La loi de réciprocité quadratique comme nous l'avons vu peut prendre différentes formes toutes aussi intéressantes et pleines d'intéret.
Nous avons pu voir comment à partir d'une loi de réciprocité pour résoudre le problème d'existence de carré modulo un nombre premier, c'est à dire le problème de résolution d'équation du type

$$ax^2 + bx + c = 0$$

cette équation est équivalente à la congruence comme sous la forme

$$y^2 \equiv a \,(\mathrm{mod}\, p)$$

dans $\mathbf{F}_p$. Cette la loi admet pleusieurs démonstartions, mais dans ce mémoire en s'est basé sur la loi de réciprocité de Legendre, Jacobi et Gauss.

Bibliographie

[1] **A.FONTAINE**, *Groupe des permutations d'un ensemble fini.Application,* 24 *avril* 2013.

[2] **A.CRUPTOS**, *Les résidus quadratiques.*

[3] **AKITA**, *Loi de réciprocité quadratique,ENS Rennes,* $2013-2014$.

[4] **A.KRAUS**, *Universit e Pierre et Marie Curie , Cours de cryptographie* $MM067-2012/13$.

[5] **B.DESCHAMPS**, *Arithmétique des entiers Université d'Eleuthéria-Polites Cours de Licence,* 2014/2015.

[6] **C.MOUROUGANE**, *Théorie Des Groupes Et Géometrie, Université De Rennes 1, Version Du* 6 *Avril* 2010.

[7] **D.SCHAUB**, *Élements de La Théorie des Groupes, Université D'angers,*1997/1998.

[8] **D.GUIN** *et* ***T.HAUSBERGER***, *Algébre Tome* 1, *Groupe,Corps et Théorie de Galois.*

[9] **D.MERCIER**, *Congruences dans* $\mathbb{Z}$, *Anneaux* $\mathbb{Z}/n\mathbb{Z}$, 11 *avril* 2003.

[10] **D.DUMMIT** *et* ***R.FOOTE***,*Absract Algebra, Third Edition.*

[11] **D.ROBINSON**, *Absract Algebra, An Introduction With Application, Second Edition.*

[12] **E.FRICIANE**, *Arithmétique et combinatoire cours et exercices, Master Main (Mathématique Générales,* 1^{er} *année),* 2011/2012.

[13] **F.DUMAS**, *Algébre : Groupes et Anneaux* 1, *Université Blaise Pascal* 2007.

[14] **F.GOODMAN**, *Algebra Abstract And Concrete, Edition* 2.5, *Univesity Of Lowa.*

[15] **J.JACQUES***et* ***P.BOYER***, *Algébre pour La licennce* 3 *éme année, Groupe, Anneaux, Corps.*

[16] **J.DURBIN**,*Modern Algebra An Introduction,Sixth Edition, The University Of Texas at Austin.*

[17] **L.JAISINGH**, *et* ***F.YRES***, *Abstract Algebra, second Edition.*

[18] **M.COSSEC** *et* ***L.THÉODON***, *Sommes de Gauss Université de Rennes* 1 *TER supervisé par Christophe Mourougane Mardi,* 27*st Avril* 2009.

[19] **N.EMMY**, *chapiter* 05*, l'anneaux des entier* $\mathbb{Z}$.

[20] **R.DANCHIN et autres**, *Cours arithmétique et groupes.*

[21] **R.BÈDARD et C.PICHET**. *Notes du groupe de travail sur les fonctions L en théorie des nombres.*

[22] **T.JUDSON et F.STEPHEN**, *Abstract Algebra, Theory and Application, Austin state University, August 27, 2010 .*

[23] **W.GILBERT et W.NICHOLSON**, *Modern Algebra With Applications, Second Edition.*

[24] **Y.SCHWAR**, *Groupes Finis, Groupes et Algébres Lie, Représentation, Deuxiéme Édition.*

Résumé :

Dans ce mémoire, nous étudions l'arithmétique finie dans l'anneau $\boldsymbol{Zn/Z}$ et la loi de réciprocité quadratique où $\boldsymbol{n}$ est un nombre premier, et en utilisé cette la loi pour résoudre la congruence sous la forme $\boldsymbol{x^2 \equiv a(mod\ p)}$ et $\boldsymbol{PGCD(a,n) = 1,}$ s'il existe, où n'existe pas, solution dans la congruence, on dit que résidu quadratique et non-résidu quadratique. Cette la loi admet plusieurs démonstration en utilise dans ce mémoire preuve de Gauss, et symbole de Legendre et Jacobi.

Mots clés :

L'arithmétique finie، l'anneau $\boldsymbol{Z/nZ}$، la loi de réciprocité quadratique، nombre premier impaire، congruence، résidu quadratique et non-résidu quadratique، Gauss، symbole Legendre et Jacobi.

الملخص :

ندرس في هذه المذكرة الحسابات المنتهية في الحلقة $\boldsymbol{Zn/Z}$ و قانون التعاكس الثنائي حيث $\boldsymbol{n}$ عدد أولي فردي، و هذا القانون نستعمله في حل للتطابق من الشكل $\boldsymbol{x^2 \equiv a(mod\ p)}$ و كان $\boldsymbol{PGCD(a،n) = 1}$، إن وجود أو عدم وجود حل لهذا التطابق فهذا ما يسمى بالبواقي التربيعية و الغير التربيعية. إن قانون التعاكس الثنائي لديه الكثير من البراهين استعملنا في هذه المذكرة برهان جاوس، و رمزي ليجندر و جاكوبي لإيجاد هذه الحلول.

الكلمات المفتاحية :

الحسابات المنتهية، الحلقة $\boldsymbol{Zn/Z}$، قانون التعاكس الثنائي، عدد أولي فردي، حل للتطابق، البواقي التربيعية و الغير التربيعية، جاوس، رمزي لجندر و جاكوبي.

Abstract :

In this memory، we study the finite arithmetic in the $\boldsymbol{Z/nZ}$ ring and the quadratic reciprocity law where $\boldsymbol{n}$ is a odd prime number، and using this law to solve the congruence in the form $\boldsymbol{x^2 \equiv a(mod\ p)}$ and $\boldsymbol{PGCD(a,n) = 1}$، if there is or does not exist, solution in the congruence we say that quadratic residue and quadratic non-residue. This law admits many demonstration uses in this memory proof of Gauss، symbol Legendre and Jacobi.

Key words :

finite arithmetic, $\boldsymbol{Z/nZ}$ ring, quadratic reciprocity law, odd prime number, congruence, quadratic residue and quadratic non-residue, Gauss، symbol Legendre and Jacobi.