UNIVERSITE MOHAMED BOUDIAF M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du diplôme de **Licence**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Spécialité : Mathématiques Appliquées

Par

1- Selikh Bilel

2-Bouaied Younes

3-Saadi Belgacem

Sujet

Le théorème des restes chinois et quelques applications

Dirigé par :

Mr. Ladjelat lahcene

Promotion: 2014/2015

Remerciements

Je tiens à remercier ALLAH qui me donne la force de faire ce modeste travail.

Je tiens à exprimer toute mes respecte à mes parents, mes frères et mes soeurs qui m'ont toujours encouragé.

Je tiens à remercier mon encadreur **Ladjelat LahceneQui me donne des orientations et les conseil sur cet ouvre.**

Nous remerciements vents à tous les professeurs de départements de Mathématique.

Je ne saurais aussi oublier mes amis et mes collègues en loin et proche , ainsi tous ceux qui ont participé de loin ou de prés et qui nous ont aidé l'élaboration de ce mémoire.

الإهداء

* أهدي هذا العمل المتواضع :

* إلى من اشتاق إلى رؤيتنا شفيعنا يوم القيامة رسول الله **محمد**

* إلى كل من يحب الله ورسوله.

* إلى من سقتني من نهر حنانها حتى الثمالة,إلى من تربيت في حجرها إلى التي تربعت على عرش قلبي واستحوذت على كل حبي,إلى أحلى أم إلى سيدة النساء :"أمي **أمينة بشيري**"

* إلى من حرم نفسه وأعطاني إلى من لامس الجمر,ومشى على الشوك لأعيش في رغد,إلى فخري وتاج رأسي إلى الغالي على قلبي إلى :"أبي**عامر**"

* إلى كل إخوتي.

* إلى كل إخوتي في الله بالجامعة " إخوتي في الكلية إخوتي في الإقامة ".
* إلى كل أحبابي,وخاصة ابناء– **بوسعادة**–

* إلى كل من أعانني حتى وصلت إلى ما أنا فيه .
* إلى كل أخ مسلم إلى كل من أعرفه ,ومن لاأعرفه.

سليخ بلال

الإهداء

* أهدي هذا العمل المتواضع :

* إلى من اشتاق إلى رؤيتنا شفيعنا يوم القيامة رسول الله **محمد**

* إلى كل من يحب الله ورسوله.

* إلى من سقتني من نهر حنانها حتى الثمالة,إلى من تربيت في حجرها إلى التي تربعت على عرش قلبي واستحوذت على كل حبي,إلى أحلى أم إلى سيدة النساء :"أمي **محفوظة ولد ونوغي**"

* إلى من حرم نفسه وأعطاني إلى من لامس الجمر,ومشى على الشوك لأعيش في رغد,إلى فخري وتاج رأسي إلى الغالي على قلبي إلى :"أبي **لعريبي**"

* إلى كل إخوتي.

* إلى كل إخوتي في الله بالجامعة " إخوتي في الكلية إخوتي في الإقامة ".
* إلى كل أحبابي,وخاصة ابناء– **سيدي عيسى**–

* إلى كل من أعانني حتى وصلت إلى ما أنا فيه .
* إلى كل أخ مسلم إلى كل من أعرفه ,ومن لاأعرفه.

بوعياد يونس

الإهداء

* أهدي هذا العمل المتواضع :

* إلى من اشتاق إلى رؤيتنا شفيعنا يوم القيامة رسول الله **محمد**

* إلى كل من يحب الله ورسوله.

* إلى من سقتني من نهر حنانها حتى الثمالة,إلى من تربيت في حجرها إلى التي تربعت على عرش قلبي واستحوذت على كل حبي,إلى أحلى أم إلى سيدة النساء :"أمي **خيرة سعود**"

* إلى من حرم نفسه وأعطاني إلى من لامس الجمر,ومشى على الشوك لأعيش في رغد,إلى فخري وتاج رأسي إلى الغالي على قلبي إلى :"أبي **أحمد**"

* إلى كل إخوتي.

* إلى كل إخوتي في الله بالجامعة " إخوتي في الكلية إخوتي في الإقامة ".
* إلى كل أحبابي,وخاصة ابناء– **بوسعادة**–

* إلى كل من أعانني حتى وصلت إلى ما أنا فيه .
* إلى كل أخ مسلم إلى كل من أعرفه ,ومن لاأعرفه.

سعدي بلقاسم

Histoire de le théorème des restes chinois:

On racontre que, dans la chine ancienne, les régiments compataient 1000 soldats. Pour si un régiment était au complet, on faisait aligner les hommes par rangs de 7, puis de 11 et enfin de 13.

Si, dans les trois cas , il manquait 1 homme pour que le dernière rang soit rempli, on en déduisait que le régiment était au complet.

Cette méthode s'appuie sur le bien nommé théorème des restes chinois dont l'étude fait l'objet de ce mémoire.

Introduction:

Dans ce travail, on s'intéresse au théorème des restes chinois dans un anneau commutatif quelconque (pas nécessairement $\mathbb{Z}$) et ainsi quelques applications.

Dans le premier chapitre, on cite quelques notions préliminaires concernant les anneaux, les idéaux, les anneaux quotient, et les idéaux premiers et maximaux.

Dans le deuxième chapitre, on étudie l'homomrphismes , l'isomorphismes , les idéaux étrangers et le théorème des restes chinois.

Finalement, dans le troisième chapitre ,on a appliqué le théorème à la congruence et l'interpolation de Lagrange.

Table des matiéres

Chapitre 01 : Notions préliminaires sur les anneaux

1.1. Rappels sur les groupe····4
1.1.1 Structure de groupe····4
1.1.2 Sous groupe····5
1.2. Les anneaux····5
1.3. Les idéaux····7
1.4. Anneaux quotient····10
1.4.1 Idéaux premiers ····10
1.4.2 Idéaux maximaux····11

Chapitre 02 : Théorème des restes chinois

2.1. Théorème d'isomorphisme d'anneau····13
2.2. Idéaux étrangers ····14
2.3. Le théorème des restes chinois···· 17

Chapitre 03 : Quelques applications

3.1. La congruence····20
3.1.1 Anneau z/nz····22
3.2. L'interpolation de lagrange····26

Chapitre 01:

Notions Préliminaires Sur Les Anneaux

1.1) Rappels sur Les groupes:

1.1.1) Structure de groupe

Définition 1.1.1.1:
un groupe est un ensemble G muni d'une loi interne

$$G \times G \to G,\ (x, y) \longmapsto xy = x.y$$

1) *qui est associative :* $\forall x, y, z \in G, x(yz) = (xy)z$,
2) *admet un élément neutre e:* $\forall x \in G, xe = ex = x$,
3) *et tout élément x du groupe G admet un inverse (ou symétrique) y :*
$\forall x \in G,\ \exists y \in G,\ \ xy = yx = e$,

cet élément est alors unique, on le noté x^{-1}.

En outre le groupe G est dit commutatif s'il vérifie également la condition suivante : $\forall\ x, y \in G, \quad xy = yx.$

Remarque 1.1.1.2: On prend souvent une notation additive pour la loi d'un groupe commutatif , la loi s'écrira alors

$$(x, y) \longmapsto x + y,$$

l'élément neutre sera noté 0 et le symétrique d'un élément x sera noté $-x$.

Exemple :
L'ensemble $\mathbb{Z}$ muni de l'addition est un groupe commutatif .
il est de même pour $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ muni de l'addition.

.

1.1.2) Sous-groupes

Definition 1.1.2.1:
si G est un groupe, un sous-groupe de G est une partie H de G vérifiant les trois conditions suivantes :

$SG1)$ $e \in H$,
$SG2)$ $\forall x, y \in H, xy \in H$,
$SG3)$ $\forall x \in H, x^{-1} \in H$.

alors H est un groupe pour la loi induite

$$H \times H \to H, (h_1, h_2) \longmapsto h_1 h_2$$

Exemple :
si G est un groupe, G et $\{e\}$ sont des sous-groupes de G.

Exemple :
Si $(H_i)_{i \in I}$ est une famille des sous-groupes d'un groupe G, alors l'intersection $\cap_{i \in I} H_i$ est un sous-groupe de G. En particulier, si X est une partie de G, l'intersection des sous-groupes de G contenant X, est un sous-groupe de G. C'est le plus petit sous-groupe de G contenant X, on l'appelle le sous-groupe de G engendré par X. On notera $\langle X \rangle$ le sous-groupe engendré par X

1.2) Les Anneaux:

Définition 1.2.1:
Soit A une ensemble muni de deux lois de composition interne notées" $+$ " et " $\cdot$ ".On dit que A est un anneau si
1) $(A, +)$ est un groupe abélien
2) La loi " $\cdot$ " est associative
3) $\forall a, b, c \in A$, on a : $a.(b + c) = a.b + a.c$ et $(a + b).c = a.c + b.c$
Si de plus la loi " $\cdot$ " est commutative, A est dit commutatif et si $(A, \cdot)$ possède un élément neutre (noté 1), A est dit unitaire.
Si de plus $(A \backslash \{0\}, \cdot)$ est un groupe abelien A est dit un corps.

Exemples :
1) $(\mathbb{Z}, +, \cdot)$ est un anneau.
2) $(\mathbb{Q}, +, \cdot)$est un corps.
3) $(\mathbb{R}, +, \cdot)$ est un corps.

Définitions 1.2.2:

Soit A un anneau et $a \in A$.
On dit que a est inversible si il existe $b \in A$ tel que $ab = 1$.
On dit que a est diviseur de 0 si $a \neq 0$ et il existe $b \neq 0$ tel que $ab = 0$.

Proposition 1.2.3: *Soit A un anneau non nul. L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour la multiplication de A.*

Démonstration :
- $A^\times \neq \phi$ car $1 \in A^\times$
- soient $x, y \in A^\times$,alors $xy^{-1}yx^{-1} = 1$, alors $xy^{-1} \in A^\times$.

Donc $A^\times$ est un groupe pour la multiplication.
L'ensemble $A^\times$, muni de la multiplication, s'appelle le groupe multiplicatif de l'anneau A ou encore le groupe des éléments inversibles de l'anneau A.

Exemple :
$\mathbb{Z}^\times = \{1, -1\}, \mathbb{Q}^\times = \mathbb{Q} - \{0\}, \mathbb{R}^\times = \mathbb{R} - \{0\}$ et $\mathbb{C}^\times = \mathbb{C} - \{0\}$.

Remarque 1.2.4:
1 est toujours un élément inversible .
D'autre part il est aisé de voir que si a est diviseur de 0 alors il n'est pas inversible.
On note $A^\times$ l'ensemble des éléments inversibles.

Définition 1.2.5:

On dit qu'un anneau A est intégre ou est un anneau d'intégrité s'il est non nul, commutatif et s'il ne posséde pas de diviseurs de zéro.
Autrement dit l'anneau A est intégre si la relation $ab = 0$ implique $a = 0$ ou $b = 0$.

Définition 1.2.6:

Soit A un anneau et $B \subset A$. On dit que B est un sous-anneau si
1) $1 \in B$
2) $\forall a, b \in B, a - b \in B$
3) $\forall a, b \in B, a.b \in B$

Définition (morphisme d'anneaux) 1.2.7:

Soient A et B des anneaux et $f : A \longrightarrow B$ une application.
On dit que f est un morphisme d'anneaux si :

1) $\forall a, b \in A, f(a+b) = f(a) + f(b)$

2) $\forall a, b \in A, f(a.b) = f(a).f(b)$

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

Si de plus f est bijective alors on dit que f est un isomorphisme.

1.3) Idéaux:

Définition 1.3.1:

Soient A un anneau et $I \subset A$. On dit que I est un idéal de A si :
1) $(I, +)$ *est un sous-groupe de* $(A, +)$
2) $\forall a \in A, \forall x \in I, \quad ax \in I, \ xa \in I$

Proposition 1.3.2: *Soit A un anneau commutatif et I une partie non vide de A.*
Alors I est un idéal de A si et seulement si $\forall x, y \in I$ et $\forall a \in A$,

$$x + ay \in I.$$

Démonstration :

$\Rightarrow$) : évident

$\Leftarrow$) :

- Pour $a = -1$, on a pour tout $x, y \in I, x - y \in I$. Donc, $(I, +)$ est sous-groupe de A.
- Pour $x = 0$, on a pour tout $a \in A$ et tout $y \in I$, $ay \in I$.

Ainsi I est un idéal de I.

Remarque 1.3.3:

$\{0\}$ et A sont des idéaux de A
Si I est un idéal différent de A, on dira que c'est un idéal propre.

Définition 1.3.4: (idéal engendré)

Soient A un anneau commutatif et S une partie non vide de A.Il existe des idéaux de A contenant S (par exemple A lui-méme). L'intersection de tous ces idéaux est un idéal de A contenant S et c'est le plus petit, au sens de l'inclusion.On l'appelle l'idéal engendré par S. On le note $< S >$. Un idéal engendré par une partie S finie est dit de type fini.

Plus généralement, soit S une partie non vide de A. On a :
$< S >= \{x/\exists r \in \mathbb{N}, \exists a_1, ...a_r \in S, \exists x_1, ..., x_r \in A$
avec $x = a_1x_1 + ... + a_rx_r\}$.

Proposition 1.3.5:

Soient A et B des anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux. On a :

1) *$f(A)$ est un anneau.*
2) *Si J est un idéal de B, $f^{-1}(J)$ est un idéal de A en particulier* $\ker(f)$ *est un idéal de A.*
3) *Si I est un idéal de A alors $f(I)$ est un idéal de $f(A)$, donc de B si f est surjective.*
4) *Si A est un corps alors f est injective ou $f = 0$.*

Opérations sur les idéaux 1.3.6:
(a) Soient I, J deux idéaux de de A. Leur somme

$$I + J = \{x + y \quad | \quad x \in I, y \in J\}$$

est le plus petit idéal de A contenant I et J.

La somme d'une famille d'idéaux $(I_\alpha)_{\alpha \in I}$ est formée par toutes les sommes finies

$$\sum_{\alpha \in \Gamma} I_\alpha = \{\sum_{\alpha \in \Gamma} x_\alpha, x_\alpha \in I_\alpha\}$$

où $x_\alpha = 0$ sauf un nombre fini de $\alpha \in \Gamma$.
(b) L'intersection ensembliste

$$\bigcap_{\alpha \in \Gamma} \mathbf{I}_\alpha$$

d'une famille d'idéaux $(I_\alpha)_{\alpha \in \Gamma}$ est toujours un idéal de A.
(c) Le produit

$$I_1 \cdot I_2 \cdot .... \cdot I_n$$

d'un nombre fini d'idéaux est l'idéal engendré par :

$$\{x_1 \cdot x_2 \cdot ... \cdot x_n \mid x_1 \in I_1, x_2 \in I_2, ..., x_n \in I_n\}$$

En particulier, l'idéal I^n est engendré par :

$$\{x_1 \cdot x_2 \cdot ... \cdot x_n \mid x_1, x_2 \in I, ..., x_n \in I\}$$

Exemple :
Si $A = \mathbb{Z}, I = (m), J = (n)$, alors
$I + J = (p\,\gcd(m, n)),\ \ I \cap J = (ppcm(m, n)),\ \ I.J = (mn)$.

1.4) Anneau quotient :

Soit A un anneau et I un idéal de A. Le groupe $(A,+)$ étant abélien et I étant un sous-groupe de A, on peut regarder le quotient $(A/I,+)$ qui est un groupe abélien.

Définition et proposition :
Soit A un anneau et I un idéal, on appelle anneau quotient A sur I l'ensemble A/I muni des lois "$+$ "et "$\cdot$" héritées de A.

Ceci est un anneau et la surjection canonique de A dans A/I est un morphisme d'anneaux.

1.4.1)Idéaux premiers :

Définition 1.4.1.1: *un idéal I d'un anneau A est premier si seulement si l'anneau quotient A/I est intègre.*

Exemple :
dans $\mathbb{Z}$, l'idéal $(a) = a\mathbb{Z}$ est premier si seulement si $a = 0$ ou a est premier

.

Proposition 1.4.1.2 : *Les assertions suivantes sont équivalentes :*
(i) I est un idéal premier de A ,
(ii) $I \neq A$ et $\forall (a,b) \in A \times A$ on a : $a.b \in I \Rightarrow a \in I$ ou $b \in I$.

Démonstration :
$(i) \Rightarrow (ii)$: soit I un idéal premier de A. A/I est différent de $\{\overline{0}\}$ donc $I \neq A$. Si $a.b \in I$ alors $\overline{a}.\overline{b} = \overline{0}$ dans A/I soit $\overline{a}$ ou $\overline{b}$ est nul car A/I est intègre donc a ou b appartient à I.
$(ii) \Rightarrow (i)$: comme $I \neq A$, $A/I \neq \{\overline{0}\}$. D'autre part :
$\overline{a}.\overline{b} = \overline{0} \Leftrightarrow a.b \in I \Rightarrow a$ ou b appartient à $I \Leftrightarrow \overline{a}$ ou $\overline{b}$ est nul et donc A/I est intègre.

1.4.2)Idéaux maximaux:

Définition 1.4.2.1 *: un idéal I d'un anneau A est maximal si seulement si l'anneau quotient A/I est un corps.*

On a donc l'implication : I idéal maximal $\Rightarrow$ I idéal premier.
La proposition suivante donne une caractérisation des idéaux maximaux d'un anneau :

Proposition 1.4.2.2: *Les assertions suivantes sont équivalentes :*
(i) I est un idéal maximal de A ,
(ii) $I \neq A$ et si J est un idéal de A distinct de A tel que $I \subset J$, alors $J = I$ (autrement dit I est maximal pour l'inclusion parmi les idéaux propres de A).

Démonstration :
$(i) \Rightarrow (ii)$: soit I un idéal maximal de A, A/I est différent de $\{\overline{0}\}$ donc $I \neq A$. Soit J un idéal de A distinct de A tel que $I \subset J$. Si I est distinct de J considérons $x \in J - I$. On a $\overline{x} \neq \overline{0}$ donc $\overline{x}$ est inversible (car A/I est un corps) : il existe $y \in A$ tel que $\overline{x}.\overline{y} = \overline{1}$ donc il existe $z \in I$ tel que $x.y = 1 + z$ soit $1 = x.y - z$ d'où $1 \in J$ et on aurait $J = A$ contrairement à l'hypothèse. Donc $J = I$.
$(ii) \Rightarrow (i)$: si $\overline{x}$ appartenant à $A/I - \{\overline{0}\}$ on a $x \notin I$. L'idéal $I + (x)$ engendré par I et x contient strictement I donc il est égal à A par hypothèses. Par conséquent il existe $z \in I$ et $y \in A$ tels que $1 = z + x.y$ d'où $\overline{1} = \overline{x}.\overline{y}$ et $\overline{x}$ est inversible dans A/I. Comme A/I est non nul car $A \neq I$ c'est donc un corps et I est un idéal maximal de A.

Chapitre 02:

Théorème des Restes Chinois

2.1)Théorème d'isomorphisme d'anneau:

Théorème 2.1.1:
Soient $f : A \to B$ un morphisme d'anneaux, π le morphisme canonique de A sur $A/\ker(f)$ et j l'injection canonique de $f(A)$ dans B.Alors il existe un isomorphisme unique $\overline{f}$ de l'anneau-quotient $A/\ker(f)$ sur le sous-anneau $f(A)$ de B tel que $f = j \circ \overline{f} \circ \pi$.

Théorème 2.1.2 : (Théorème d'isomorphisme).
Si $f : A \to B$ est un morphisme d'anneau,alors :
$$A/Ker(f) \simeq Im(f)$$
($\simeq$ désigne un isomorphisme d'anneaux).

Démonstration :
Décrivons cet isomorphisme, noté $\overline{f}$: on pose $\overline{f}(\overline{a}) = f(a)$.Il faut vérifier que cela ne dépend pas du représentant choisi pour la classe de a :
$\overline{a} = \overline{b} \Rightarrow a - b \in Ker(f) \Rightarrow f(a-b) = 0 \Rightarrow f(a) = f(b)$
$\overline{f}(\overline{a+b}) = f(a+b) = f(a) + f(b) = \overline{f}(\overline{a}) + \overline{f}(\overline{b})$
idem pour le produit et pour l'image de$1_{A/\ker f}$: c'est bien un morphisme d'anneaux. Il est surjectif par choix de l'ensemble d'arrivée, et injectif car son noyau est l'ensemble des a pourtous les $a \in Ker f$,
c'est donc $\{\overline{0}\}$.

Théorème 2.1.3: (Premier théorème d'isomorphisme)
Soient $f : A \to A'$ un morphisme d'anneaux le noyau $\ker f$ est un idéal de A , son image $\operatorname{Im} f$ est un sous-anneau de A' et l'on obtient par passage au quotient un isomorphisme $\overline{f} : A/\ker f \to \operatorname{Im} f$,
d'où le diagramme commutatif

$$\begin{array}{ccc} A & \underset{f}{\to} & A' \\ p\downarrow & & i\uparrow \\ A/\ker f & \underset{\overline{f}}{\dashrightarrow} & \operatorname{Im} f \end{array}$$

dans lequel i désigne l'inclusion de $\operatorname{Im} f$ dans A'.

Démonstration:
Encore une fois, seules les propriétés relatives à la multiplication restent à démontrer. Nous prouverons simplement que $\ker f$ est un idéal de A, et $\mathrm{Im}\, f$ un sous-anneau de A'.
On sait déjà que ce sont des sous-groupes. Si $x \in \ker f$ et $a \in A$.
on écrit :
$f\ (ax) = f(a)f(x) = f(a)0_{A'} = 0_{A'} \Rightarrow ax \in \ker f$
Si $y, y' \in \mathrm{Im}\, f$,on écrit $y = f(x)$, $y' = f(x')$,d'où :
$yy' = f(x)f(x') = f(xx') \in \mathrm{Im}\, f$.
Enfin, par définition d'un morphisme d'anneaux, $1_{A'} = f(1_A) \in \mathrm{Im}\, f$.

Exemple :
Soit $f : P \mapsto P(i)$ le morphisme de $\mathbb{Z}[X]$ dans $\mathbb{C}$ tel que $X \mapsto i$.
Puisque $i^{2p} = (-1)^p \in \mathbb{Z}$ et que $i^{2p+1} = (-1)^p i \in \mathbb{Z}i$ son image est le sous-anneau

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

de $\mathbb{C}$: c'est l'anneau des entiers de Gauß. Son noyau est égal à $< F >$ avec $F = x^2 + 1$.

En effet, pour tout $P \in \mathbb{Z}[X]$, la division euclidienne $P = QF + R$ est telle que $Q, R \in \mathbb{Z}[X]$ et $degR < 2$. Si P est dans le noyau,c'est-à-dire si $P(i) = 0$ on a $R(i) = 0$, donc $R = 0$, et l'on voit que $P \in < F >$.
Du premier théorème d'isomorphisme on déduit donc l'isomorphisme d'anneau:

$$\mathbb{Z}[i] \simeq \mathbb{Z}[X]\ / < X^2 + 1 > .$$

2.2) Idéaux étrangers:

Définition 2.2.1:(Produits d'idéaux de A)
1) *Soient $I_1, ..., I_m$ des idéaux de A, non nécessairement distincts. On note $I_1 \cdots I_m$ l'idéal engendré par les produits $x_1 \cdots x_m$, où $x_j \in I_j$ pour $j = 1, ..., m$. C'est l'ensemble des sommes finies de tels produits.*
2) *On observe que si chaque I_j est principal, c-à-d, $I_j = (a_j)$, alors $I_1 \cdots I_m$ est l'idéal engendré par $a_1 \cdots a_m$.*
3) *Si $I_1, ..., I_m$ sont tous égaux à I, on obtient l'idéal I^m, formé des sommes finies arbitraires de produits de m éléments de I :*

$$I^m = \{\sum x_1 \cdots x_m \ \ / x_i \in I\ \}$$

Remarque 2.2.2:
1) On prendra garde que, en général, I^m est stictement plus grand que l'idéal engendré par les puissances m-ièmes d'éléments de I.
Par exemple, si $A = k[X, Y]$ et si I est l'idéal engendré par$X$et Y, alors I^2 est engendré par X^2, XY et Y^2, et XY n'est pas un carré.
2) On a toujours $I_1 \cdots I_m \subseteq I_1 \cap \cdots \cap I_m$, et l'inclusion est en général stricte (prendre, par exemple, $I_j = (a)$, pour tout j).

Soient $I_1, ..., I_n$ des idéaux de A. On note $I_1 + \cdots + I_n$ l'idéal formé des sommes $x_1 + \cdots + x_n$, où $x_j \in I_j$ pour $j = 1, ..., n$.

Définition 2.2.3 : (Idéaux étrangers).
Soient $I_1, ..., I_n$ des idéaux de A.
1) *On dit que $I_1, ..., I_n$ sont étrangers (ou « premiers entre eux ») si l'on a $I_1 + I_2 + ... + I_n = A$.*
2) *On dit que $I_1, ..., I_n$ sont étrangers deux à deux si I_r et I_s sont étrangers, pour tout $r \neq s$.*

Remarque 2.2.4 :
On prendra garde à ne pas confondre ces deux notions. Si $n \geqslant 3$, la deuxième condition est beaucoup plus forte que la première ! Pour éviter les confusions, on dira parfois dans le premier cas que $I_1, ..., I_n$ sont étrangers « dans leur ensemble » .

Lemme 2.2.5:
On suppose que I est étranger à $J_1, ..., J_m$ (on ne suppose pas les J_i nécessairement distincts). Alors I est étranger à $J_1, ..., J_m$.

Démonstration :
Par hypothése, il existe, pour $i = 1, ..., m$, des éléments $x_i \in I$ et $y_i \in I$ tels que $x_i + y_i = 1$. Alors

$$1 = \prod_{i=1}^{m} (x_i + y_i),$$

et en développant ce produit on obtient le terme $y_1 \cdots y_m$ qui appartient à $J_1 \cdots J_m$, et une somme de termes qui contiennent au moins un x_i donc appartiennent à I . Ceci prouve le lemme.

Corollaire 2.2.6 :

Supposons $I_1, ..., I_n$ *étrangers deux à deux, et soient* $m_{1,..}, m_n$ *des entiers* $\geqslant 1$.

1) *On a* $I_1 \cdots I_n = I_1 \cap ... \cap I_n$.

2) $I_1^{m_1}, ..., I_n^{m_n}$ *sont étrangers deux à deux.*

3) *Posons, pour* $k = 1, ..., n$,

$$J_k = \prod_{j \neq k} I_j^{m_j}, \quad alors \quad J_1 + ... + J_n = A,$$

c-à-d, $J_1, ..., J_n$ *sont étrangers « dans leur ensemble » .*

Démonstration :

Dans 1), il suffit de montrer l'inclusion $\supseteq$, puisque l'autre est évidente.
On va prouver les assertions 1) et 2) par récurrence sur n. Supposons d'abord $n = 2$.
Par hypothèse, il existe $x_1 \in I_1$ et $x_2 \in I_2$ et tels que $x_1 + x_2 = 1$.
Alors, pour tout $a \in I_1 \cap I_2$, l'on a :
$a = a \cdot 1 = ax_1 + ax_2 \in I_1 I_2$,d'ou $I_1 I_2 = I_1 \cap I_2$.
D'autre part, d'après le lemme précédent, I_1 est ètranger à I_2^{m2},
puis $I_2^{m_2}$ est étranger à $I_1^{m_1}$, ce qui prouve 2) dans le cas $n = 2$.
Supposons $n \geqslant 3$ et les deux assertions établies pour $n-1$. Par hypothése de récurrence, $I_2 \cap .... \cap I_n = I_2 \cdot \cdots \cdot I_n$, et, d'aprés le lemme, cet idéal est étranger à I_1. On a donc

$$I_1 \cap ... \cap I_n = I_1 \cap (I_2 ... I_n) = I_1 \cdot I_2 \cdots I_n,$$

ce qui prouve 1). D'autre part, par hypothése de récurrence, $I_2^{m_2}, ..., I_n^{m_n}$ sont étrangers deux à deux. De plus, d'aprés le cas $n = 2$, chaque $I_k^{m_k}$ est étranger $I_1^{m_1}$ avec $I_1^{m_1}$. L'assertion 2) est démontrée.
Démontrons l'assertion 3). D'abord, $I_1^{m_1}, ..., I_r^{m_r}$ sont étrangers deux à deux, d'aprés l'assertion 2). Donc, sans perte de généralité, on peut se limiter au cas où $m_k = 1$ pour tout k .
Pour chaque k , I_k et J_k sont étrangers, d'aprés le lemme 2.3 , donc il existe $x_k \in I_k$ et $y_k \in J_k$ tels que $1 = x_k + y_k$.
On obtient donc

. $$1 = \prod_{k=1}^{n} (x_k + y_k) \ .$$

Développons le produit : les termes qui contiennent un y_k appartiennent à J_k et donc à $J_1 + \cdots + J_r$; le seul autre terme est $x_1 \cdots x_r$, qui appartient à J_k pour tout k.
Ceci montre que $1 \in J_1 + \cdots + J_r$, ce qui termine la preuve du corollaire.

Remarque 2.2.7:
On voit facilement que si un idéal premier P contient un produit d'idéaux $j_1 \cdots j_r$,alors il contient l'un des j_k.

2.3) Le théorème des restes chinois:

Définition 2.3.1: (Produits d'anneaux):
Soit $(A_i)_{i\in I}$ une famille d'anneaux. Le groupe abélien $\prod_{i\in I} A_i$ est muni d'une structure d'anneau, où la multiplication est définie coordonnée par coordonnée :

$$(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i b_i)_{i\in I}$$

L'élément neutre, noté 1, est la famille $(a_i)_{i\in I}$ telle que $a_i = 1$ pour tout $i \in I$. Si I est fini, disons $I = \{1, ..., n\}$, cet anneau se noté

$$A_1 \times \cdots \times A_n \ .$$

Théorème 2.3.2 :
Soient $p_1, ..., p_n$ des entiers premiers entre eux deux à deux.
Alors en tant qu'anneaux, $\mathbb{Z}/p_1p_2...p_n \simeq \mathbb{Z}/p_1\mathbb{Z} \times ... \times \mathbb{Z}/p_n\mathbb{Z}$.
Inversément , si $\mathbb{Z}/p_1p_2...p_n \simeq \mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times ... \times \mathbb{Z}/p_n\mathbb{Z}$
alors les nombres $p_1, ..., p_n$ sont premiers entre eux deux à deux.

Exemple : $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Corollaire 2.3.3 :
Soient $p_1, ..., p_n$ des entiers premiers entre eux deux à deux.
Alors en tant que groupes,

$$(\mathbb{Z}/p_1p_2...p_n)^\times \simeq (\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times ... \times \mathbb{Z}/p_n\mathbb{Z})^\times.$$

Théorème 2.3.4:(théorème des restes chinois)
Soient A un anneau, et $(I_i)_i = \{1, ..., n\}$ des idéaux vérifant :
$\forall i, j \in \{1, ..., n\}$, $i \neq j \Longrightarrow I_i + I_j = A$. *Alors*
$A/\cap_{i=1}^{n} I_i \to A/I_1 \times \cdots \times A/I_n$ *est un isomorphisme.*

Démonstration : On note π_i la surjection canonique de A sur A/I_i.
Le morphisme $f : A \to A/I_1 \times \cdots \times A/I_n$ défini par
$f(x) = (\pi_1(x), ..., \pi_n(x))$ est surjectif grâce.
Calculons
$ker f = \{x \in A$, tel que $\pi_i(x) = 0$ pour tout $i = 1, ..., n\}$
$= \{x \in A$ tel que $x \in I_i$ pour tout $i = 1, ..., n\} = \cap_{i=1}^{n} I_i$.

Théorème 2.3.5 : *Soit A un anneau commutatif et soient I_1 et I_2 deux idéaux étrangers de A. Soient a et b deux éléments de A donnés arbitrairement (les restes). Alors il existe $x \in A$ tel que l'on ait :*

$$x \equiv a \ mod \ I_1 \quad et \quad x \equiv b \ mod \ I_2.$$

Démonstration :
On a $I_1 + I_2 = A$,donc il existe $\alpha \in I_1$ et $\beta \in I_2$ tels que $1 = \alpha + \beta$,
soit alors $x = a\beta + b\alpha$ et montrons que x a les propriétés requises :
on a $x \equiv a\beta \bmod I_1$ (car α ,donc $b\alpha$, est dans I_1) , ou $\beta = 1 - \alpha$,
d'où $x \equiv a(1 - \alpha) \bmod I_1$, soit $x \equiv a - a\alpha \equiv a \bmod I_1$ (car $a\alpha \in I_1$).
De même, $x \equiv b\alpha \bmod I_2$, soit de façon analogue,
$x \equiv b(1 - \beta) \equiv b - b\beta \equiv b \bmod I_2$.

Corollaire 2.3.6 :
Soient $I_1, ..., I_n$, $n \geqslant 2$, des idéaux de A, étrangers deux à deux (i.e.$I_i + I_j = A$, pour tout i, $j = 1, ..., n, i \neq j$). Soient $a_1, ..., a_n$ des éléments quelconques de A. Alors il existe $x \in A$ tel que l'on ait
$x \equiv a_i \bmod I_i$, *pour tout* $i = 1, ..., n$.

Chapitre 03:
Quelques applications

.3.1) la congruence:

Théorème 3.1.1:
soit $m_1, ..., m_r$ des entiers premiers deux à deux
(i.e,$(m_i, m_j) = 1$ si $i \neq j$) et $a_1, ..., a_r$, des entiers quelconques .
Alors il existe un entier x tel que

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1) \\ x \equiv a_2 (\mathrm{mod}\, m_2) \\ \qquad \vdots \\ x \equiv a_r (\mathrm{mod}\, m_r). \end{cases}$$

De plus , si x et x' sont deux entiers qui sont solutions de ce systéme de congruence, alors

$$x \equiv x' mod M$$

où $M = m_1 m_2 \cdots m_r$
Réciproquement, si x est une solution et $x \equiv x'(modM)$ alors x' est aussi une solution .

Définition 3.1.2 :
Soit a et b deux entiers relatifs. On dit que a est congru à b modulo n si $a - b$ est un multiplede n. Cette propriété se note $a \equiv b[n]$.

Remarque 3.1.3 :
Deux nombres sont congrus modulo n si et seulement si ils ont le même reste dans la division euclidienne par n.

Proposition 3.1.4:
La relation de congruence modulo n est une relation d'équivalence.

Démonstration :
1) Réflexive: car $a \equiv a[n]$. En effet $a - a = 0$ est un multiple de a.
2)Symétrique : Si $a \equiv b[n] \Rightarrow a - b$ est un multiple de $n \Rightarrow b - a$ est un multiple de $n \Rightarrow b \equiv a[n]$
3)Transitive : Si $a \equiv b[n]$ et $b \equiv c[n]$alors $\exists k, k' \in \mathbb{Z}$ tels que $a - b = kn$ et $b - c = k'n \Rightarrow a - c = (k + k')n \Rightarrow a \equiv c[n]$

Définition 3.1.5:
Soient $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n si $a - b$ est un multiple de n, i.e.$\exists k \in \mathbb{Z}$, $a - b = kn$ .On note $a \equiv b[n]$

Théorème 3.1.6:
La relation de congruence est compatible avec les lois usuelles $+$ et $\times$.
Autrement dit :
- Si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors $a + a' \equiv b + b'[n]$
- Si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors $a - a' \equiv b - b'[n]$
- Si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors $aa' \equiv bb'[n]$
- Si $a \equiv b[n]$ alors $a^k \equiv b^k[n], k > 1$ (se montre par récurrence sur k)

Démonstration :
Montrons seulement les points 1 et 3.
1 Si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors $\exists k, k' \in \mathbb{Z}$ tels que $a - b = kn$
et $a' - b' = k'n$.
En les ajoutant on trouve : $(a+a')-(b+b') = (k+k')n \Rightarrow a+a' \equiv b+b'[n]$
3 Si $a \equiv b[n]$ et $a' \equiv b'[n]$ alors $\exists k, k' \in \mathbb{Z}$ tels que
$a - b = kn \quad \times a' \quad a\,a' - ba' = kna'$
$a' - b' = k'n \quad \times \ b \quad a'b - b'b = k'nb$
En les ajoutant membre à membre on trouve : $aa' - bb' = n(ka' + k'b) \Rightarrow$
$aa' \equiv bb'[n]$

Remarque 3.1.7:
On ne peut pas simplifier une congruence comme une égalité.
$$2a \equiv 2b[n] \not\Rightarrow \ a \equiv b[n].$$
Par exemple, $16 \equiv 20[4]$ mais 8 et 10 ne sont pas congrus modulo 4.

Théorème 3.1.8:
$a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Démonstration :
Si $a \equiv b[n]$ alors $\exists k \in \mathbb{Z}$ tel que $a - b = kn$ soit $a = b + kn$.
Si r est le reste de la division euclidienne de a par n et r'celui de b par n, on a : $a = q_1 n + r$ et $b = q_2 n + r'$ avec $0 \leqslant r < n$ et $0 \leqslant r' < n$. Ainsi : $q_1 n + r = q_2 n + r' + kn \Rightarrow r - r' = n(k + q_2 - q_1)$. n divise donc $r - r\prime$, et comme $|r - r'| < n$ on $r - r' = 0$ soit $r = r'$.

Réciproquement, si $a = nq_1 + r$ et $b = nq_2 + r$ avec $0 \leqslant r < n$, on a $a - b = n(q_1 - q_2)$, alors $a - b$ est un multiple de $n \Rightarrow a \equiv b[n]$.
La relation de congruence (et l'ensemble $\mathbb{Z}/n\mathbb{Z}$ que l'on verra plus loin) permettent de simplifier les calculs à « un multiple de n près ».

Exemple d'application 3.1.9:

Les congruences sont très utilisées dans le domaine de l'arithmétique.
calcul de reste : Trouver le reste dans la division euclidienne de 7077^{277} par 11.
$7077^{277} \equiv 4^{277} \equiv 4 \times (4^3)^{92} \equiv 4 \times 9^{92} \equiv 4 \times 4^{46} \equiv 4 \times 5^{23} \equiv 20 \times 25^{11}$
$\equiv 9 \times 3^{11} \equiv 27 \times 9^5 \equiv 5 \times 9 \times 81^2 \equiv 1 \times 4^2 \equiv 16 \equiv 5[11]$
Le reste vaut 5

3.1.1) Anneau $\mathbb{Z}/n\mathbb{Z}$:

Définition 3.1.1.1:

On appelle classe d'équivalence de $x \in \mathbb{Z}$ modulo n, noté $\overline{x}$, l'ensemble $\overline{x} = \{y \in \mathbb{Z} \mid x \equiv y[n]\} = x + n\mathbb{Z}$.

Remarques 3.1.1.2 :
i) $x \equiv y[n] \Leftrightarrow \overline{x} = \overline{y}$
ii) $\overline{x}$ est l'ensemble des entiers dont le reste de la division euclidienne par n est égal à x.

Définition 3.1.1.3:

L'ensemble quotient de $\mathbb{Z}$ par la relation $\equiv$ de congruence modulo n est l'ensemble des classes d'équivalences pour la relation $\equiv$.
On ne note $\mathbb{Z}/_{\equiv[n]} = \mathbb{Z}/n\mathbb{Z}$

Théorème 3.1.1.4:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

Démonstration :

Soit ,$x \in \mathbb{Z}$ on fait la division euclidienne de x par n : $\exists!(q, r) \in \mathbb{Z}^2$ tel que $x = nq + r \qquad 0 \leqslant r < n \Rightarrow x - r = nq \Rightarrow x \equiv r[n]$
et r ne peut prendre que les valeurs $0, 1, 2, \ldots, n-1$.
Donc $\mathbb{Z}/n\mathbb{Z} \subset \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.La réciproque est triviale.

Propriété 3.1.1.5:
Les classes d'équivalences de l'ensemble $\mathbb{Z}/n\mathbb{Z}$ forment une partition de $\mathbb{Z}$.

Théorème 3.1.1.6:
On peut définir sur $\mathbb{Z}/n\mathbb{Z}$ une loi interne $\overline{+}$ définie par : $\overline{x}\overline{+}\overline{y} = \overline{x+y}$
Par cohérence avec la loi + usuelle, on notera +au lieu de $\overline{+}$.
On a alors que l'ensemble $(\mathbb{Z}/n\mathbb{Z}, +)$est un groupe abélien.

Démonstration :
Il faut montré que la loi " + " est bien définie, i.e. qu'elle ne dépende pas du représentant choisi. En effet, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ alors $x \equiv x'[n]$ et $y \equiv y'[n]$. Ainsi $x + y \equiv x' + y'[n] \Rightarrow \overline{x+y} = \overline{x'+y'}$.
De plus la loi " + "est commutative, associative, possède comme élément neutre $\overline{0}$ et tout élément $\overline{x}$ possède un symétrique qui est $\overline{-x}$.

Remarque 3.1.1.7:
$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe monogène engendré par $\overline{1}$, comme il est fini on dit qu'il est cyclique.On pourrait étudier le groupe $((\mathbb{Z}/n\mathbb{Z})^{\times}, \times)$, c'est un groupe de cardinal $\varphi(n)$ où φ est l'indicatrice d'Euler.

Théorème 3.1.1.8:
On définit une loi interne noté «·» dans $\mathbb{Z}/n\mathbb{Z}$ par : $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$
On a alors que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$est un anneau unitaire commutatif.

Démonstration :
On montre que cette loi ne dépend pas du choix du représentant choisi comme pour le théorème précédent. De plus il est facile de vérifier que cette loi est associative, distributive par rapport à la loi +,
est commutative et admet pour élément neutre $\overline{1}$.

Remarque 3.1.1.9:
Cet anneau n'est pas forcément intègre. Par exemple dans $\mathbb{Z}/4\mathbb{Z}$ on a $\overline{2} \times \overline{2} = \overline{4} = \overline{0}$ et $\overline{2} \neq \overline{0}$.

Définition 3.1.1.10:
$\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est inversible s'il existe $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x} \cdot \overline{y} = \overline{1}$

Théorème 3.1.1.11 :
Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{x} \neq \overline{0}$. Alors $\overline{x}$ inversible $\iff$ $p \gcd(x, n) = 1$.

Démonstration :
$\overline{x}$ inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x} \cdot \overline{y} = 1$

$\Leftrightarrow$ $\exists \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{x \cdot y} = 1$

$\Leftrightarrow$ $\exists y \in \mathbb{Z}/n\mathbb{Z}$ tel que $xy \equiv 1[n]$

$\Leftrightarrow$ $\exists y, k \in \mathbb{Z}$ tels que $xy - kn = 1$

$\Leftrightarrow$ $p \gcd(x, n) = 1$ par le théorème de Bézout.

Théorème 3.1.1.12*:*
$\overline{x}$ inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \cdot) \Leftrightarrow \overline{x}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$

Démonstration :
$\overline{1}$est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$, on note $< \overline{x} >= \{k\overline{x} \mid k \in \mathbb{Z}\}$
Il faut montrer que $\overline{x}$ inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \cdot) \Leftrightarrow \overline{1} \in < \overline{x} >$
$\overline{1} \in < \overline{x} > \Leftrightarrow \exists m \in \mathbb{Z}$ tel que $m\overline{x} = 1$
$\Leftrightarrow \exists m \in \mathbb{Z}$ tel que $mx \equiv 1[n]$
$\Leftrightarrow \exists m, q \in \mathbb{Z}$ tels que $mx - nq = 1$
$\Leftrightarrow p \gcd(x, n) = 1$ (par le théorème de Bézout)
$\Leftrightarrow \overline{x}$ inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ (par le théorème précédent)
Finalement on a montré que :
$p \gcd(x, n) = 1 \Leftrightarrow \overline{x}$ inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \cdot) \Leftrightarrow \overline{x}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$

Corollaire 3.1.1.13:
$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est premier.

Théorème 3.1.1.14 :
Si m et n sont deux entiers premiers entre eux, il existe un isomorphisme d'anneaux de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/\ m\mathbb{Z} \times \mathbb{Z}/\ n\mathbb{Z}$

Démonstration :
On part de $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$x \mapsto (\overline{x}^m, \overline{x}^n)$
φ est un morphisme d'anneaux : $\varphi(x+y) = \varphi(x) + \varphi(y)$;
$\varphi(xy) = \varphi(x)\varphi(y)$; $\varphi(1) = (\overline{1}, \overline{1})$, $x \in \ker\varphi \Leftrightarrow x \equiv 0[n]$ et $x \equiv 0[m] \Leftrightarrow$
$\exists\ \alpha, \beta$tels que $x = \alpha n = \beta m$ Comme $p\gcd(m,n) = 1$ on en déduit par le théorème de Gauss que m divise α, $\exists \mu$ tel que $\alpha = m\mu$.Ainsi
$x = (mn)\mu$ et donc $x \in mn\mathbb{Z}$. $\ker\varphi = mn\mathbb{Z}$
On sait qu'on a un isomorphisme entre $\mathbb{Z}/\ker\varphi$ et $\mathrm{Im}\,\varphi$,
$\mathbb{Z}/mn\mathbb{Z} \to \mathrm{Im}\,\varphi \subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et par cardinalité on en déduit que
$\mathrm{Im}\,\varphi = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Applications :

Application 1 :
A la recherche d'inverses :
Trouver l'inverse de $\overline{16}$ dans $\mathbb{Z}/19\mathbb{Z}$
$p\gcd(16,19) = 1$ donc l'inverse de $\overline{16}$ dans $\mathbb{Z}/19\mathbb{Z}$ existe bien
$\mathbb{Z}/19\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{18}\}$ car 19 est premier.
Soit $\overline{x}$ l'inverse de $\overline{16}$ dans $\mathbb{Z}/19\mathbb{Z}$, on a
$\overline{x} \cdot \overline{16} = \overline{16 \cdot x} = \overline{1} \Leftrightarrow 16x \equiv 1[19] \Leftrightarrow$
$\exists y \in \mathbb{Z}, 16x - 19y = 1$.L'ensemble des solutions à
cette équation est $S = \{(19k+6, 16k+5) \mid k \in \mathbb{Z}\}$
Nous on cherche seulement le x qui est dans S
et qui est dans $\mathbb{Z}/19\mathbb{Z}$.
La solution est donnée pour $K = 0$ et on trouve que :
$\overline{x} = \overline{16}^{-1} = \overline{6}$ dans $\mathbb{Z}/19\mathbb{Z}$
En fait toutes les valeurs de K marchent mais après il faut trouver un représentant irréductible.

Application 2 :
Problème de rangement, système de congruences
Pierre veut ranger sa collection de livres. S'il range les livres par 11 il en reste 7, s'il les range par 26 il en reste 12.Combien Pierre a de livres dans sa collection sachant qu'il en a moins de 200?
Soit x le nombre de livres dans la collection de Pierre. Il faut résoudre

le système : $\begin{cases} x \equiv 7[11] \\ x \equiv 12[26] \end{cases}$

Donc il existe u et v dans $\mathbb{Z}$ tels que : $x = 11u + 7$ et $x = 26v + 12$.
Il faut donc résoudre l'équation : $11u - 26v = 5$.
11 et 26 sont premiers entre eux, le système de congruence admet donc un solution x dont la classe modulo $11 \times 26 = 286$ est unique (théorème chinois) $\mathbb{Z}/286\mathbb{Z} \to \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ (isomorphisme)
on trouve que : $S = \{(26k - 35, 11k - 15) \mid k \in \mathbb{Z}\}$
Finalement $x = 11u + 7 = 11(26k - 35) + 7 = 286k - 378$.
$x = 286k - 378$
La solution au problème est obtenue pour $k = 2$, Pierre a 194 livres dans sa collection.

3.2) L'interpolation de lagrange:

la formule d'interpolation de lagrange:
soit k un corps commutatif ,$\alpha_i (i = \overline{1,n})$ n élèments distincts de k (si $i \neq j, \alpha_i \neq \alpha_j$) et $\beta_i (i = \overline{1,n})$ n élèment quelconques,distincts ou non de k.

proposons nous de determiner les polynomes f de $A = k[x]$ telque $f(\alpha_i) = \beta_i$ $(i = \overline{1,n})$.
introduction les idéaux principaux $\mathfrak{m}_i = (x - \alpha_i), i = \overline{1,n}$.
on a $\mathfrak{m}_i + \mathfrak{m}_j = A$ pour $i \neq j$ suivant
le théorème des restes chinois, il existe $f \in A$ tel que $f \equiv \beta_i (\mathrm{mod}\, \mathfrak{m}_i)$, c'est à dire tel que $f(\alpha_i) = \beta_i$

posons $g_j(x) = \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{(x-\alpha_i)}{\alpha_{j-\alpha_i}}$
on a $g_j(x) \equiv 1 (\mathrm{mod}\, \mathfrak{m}_j)$ et
$g_j \equiv 0 (\mathrm{mod}\, \mathfrak{m}_i)$ pour $i \neq j$
alors suivant le théorème des restes chinois:
$f = \beta_1 g_1 + \beta_2 g_2 + ... + \beta_n g_n$ d'où la formule dite d'niterploation de lagrange

$$f(x) = \sum_{j=1}^{n} \beta_j \prod_{\substack{i=1 \\ i \neq j}}^{n} \frac{x-\alpha_i}{\alpha_j - \alpha_i}$$

Exemple:
trouver le polynome de lagrange $p_n$qui verifier les condition suivantes:

x_i	0	1	3	4
y	1	3	2	5

$$
\begin{aligned}
p_3(x) &= \sum_{i=0}^{3} L_i(x) f_i \\
&= L_0(x)f_0 + L_1(x)f_1 + L_2(x)f_2 + L_3(x)f_3 \\
L_i(x) &= \frac{\prod_{j=0}^{3} (x - x_j)}{\prod_{i=0}^{3} (x_i - x_j)} \\
L_0(x) &= \frac{(x-x_1)(x-x_2)(x-x_3)}{(0-1)(0-3)(0-4)} \\
&= \frac{-1}{12}(x^3 - 8x^2 + 19x - 12) \\
L_1(x) &= \frac{(x-x_0)(x-x_2)(x-x_3)}{(1-0)(1-3)(1-4)} \\
&= \frac{1}{6}(x^3 - 7x^2 + 12x) \\
L_2(x) &= \frac{(x-x_0)(x-x_1)(x-x_3)}{(3-0)(3-1)(3-4)} \\
&= \frac{-1}{6}(x^3 - 5x^2 + 4x) \\
L_3(x) &= \frac{(x-x_0)(x-x_1)(x-x_2)}{(4-0)(4-1)(4-3)} \\
&= \frac{1}{12}(x^3 - 4x^2 + 3x)
\end{aligned}
$$

donc:

$p_3(x) = L_0(x) \times 1 + L_1(x) \times 3 + L_2(x) \times 2 + L_3(x) \times 5$

$p_3(x) = -\frac{1}{2}x^3 + \frac{17}{6}x^2 + \frac{4}{3}x + 1.$

Bibliographie:

[1] A. Paterson. *Differential equations and numerical analysis.* Cambridge university press, Cambridge1991.

[2] J. Briançon, Ph. Maisonobe, *Éléments d'algèbre commutative (niveau M1), Ellipses,* 2004.

[3] M.Crouzeix and A. L. Mignot. *Analyse numérique des équations différentielles.* Masson, Paris, 1984.

[4] M. Sibony and J. C. Mardon R. *Analyse numérique (2 tomes) .* Hermann, Paris, 1982.

[5] N. Bourbaki, *Algèbre, Chapitres 4 à 7*, Masson, 1981.

[6] R. Elkik, *Cours d'algèbre*, Ellipses, 2002.

Résumé :

Dans ce travail, on s'intéresse au théorème des restes chinois dans un anneau commutatif quelconque (pas nécessairement $\mathbb{Z}$) et ainsi quelques applicationss.

Conclusion :

Dans ce travail, on s'est intéresse au théorème des restes chinois dans un anneau commutatif quelconque (pas nécessairement $\mathbb{Z}$) et ainsi quelques applications.

Dans le premier chapitre, on a cite quelques notions préliminaires concernant les anneaux, les idéaux, les anneaux quotient, et les idéaux premiers et maximaux.

Dans le deuxième chapitre, on a étudie l'homomrphismes , l'isomorphisme, les idéaux étrangers et le théorème des restes chinois.

Dans le troisième chapitre ,on a appliqué le théorème à la congruence et l'interpolation de Lagrange.

Bibliographie:

[1] A. Paterson. *Differential equations and numerical analysis*. Cambridge university press, Cambridge1991.

[2] J. Briançon, Ph. Maisonobe, *Éléments d.algèbre commutative (niveau M1), Ellipses,* 2004.

[3] M.Crouzeix and A. L. Mignot. *Analyse numérique des équations différentielles*. Masson, Paris, 1984.

[4] M. Sibony and J. C. Mardon R. *Analyse numérique (2 tomes)* . Hermann, Paris, 1982.

[5] N. Bourbaki, *Algèbre, Chapitres 4 à 7*, Masson, 1981.

[6] R. Elkik, *Cours d.algèbre*, Ellipses, 2002.