الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf :.....

Centre Universitaire de Mila

Institut des Sciences et de la Technologie Département de Mathématiques et Informatique

Mémoire préparé En vue de l'obtention du diplôme de licence

En -Filière Mathématiques Fondamentales

Thème

Congruence et théorème des restes chinois

Préparé par :

1) Benmekhlouf Sabrina
2) Bouaicha Assia
3) Bousellah Nadjet
4) Merabet Sara

Dirigé par :

Khalfaoui Mohamed
Grade Maitre assistant -b-

Année universitaire : 2013/2014

Remerciement

C'est avec l'aide de DIEU tout puissant que ce modeste mémoire a pu être réalisé, DIEU qui nous a donné fois, raison et lucidité.

Nous tenons à remercier notre encadreur, KHALFAOUI MOHAMED pour nous avoir orientés et de nous avoir offert l'opportunité de travailler sur ce projet. Nous le remercions pour son grand soutien pédagogique, scientifique et moral, pour ses conseils, ses suggestions et ses encouragements qu'il n'a cessé de nous apporter pendant toute la durée de l'élaboration de ce mémoire.

Nous tenons à remercier et à saluer tous les professeurs du département science et technologie.

Enfin un grand merci à Damak Feriel et Chellouf Yassmine pour leur aide et leur soutien qu'ils nous ont accordé.

Merci à tous.

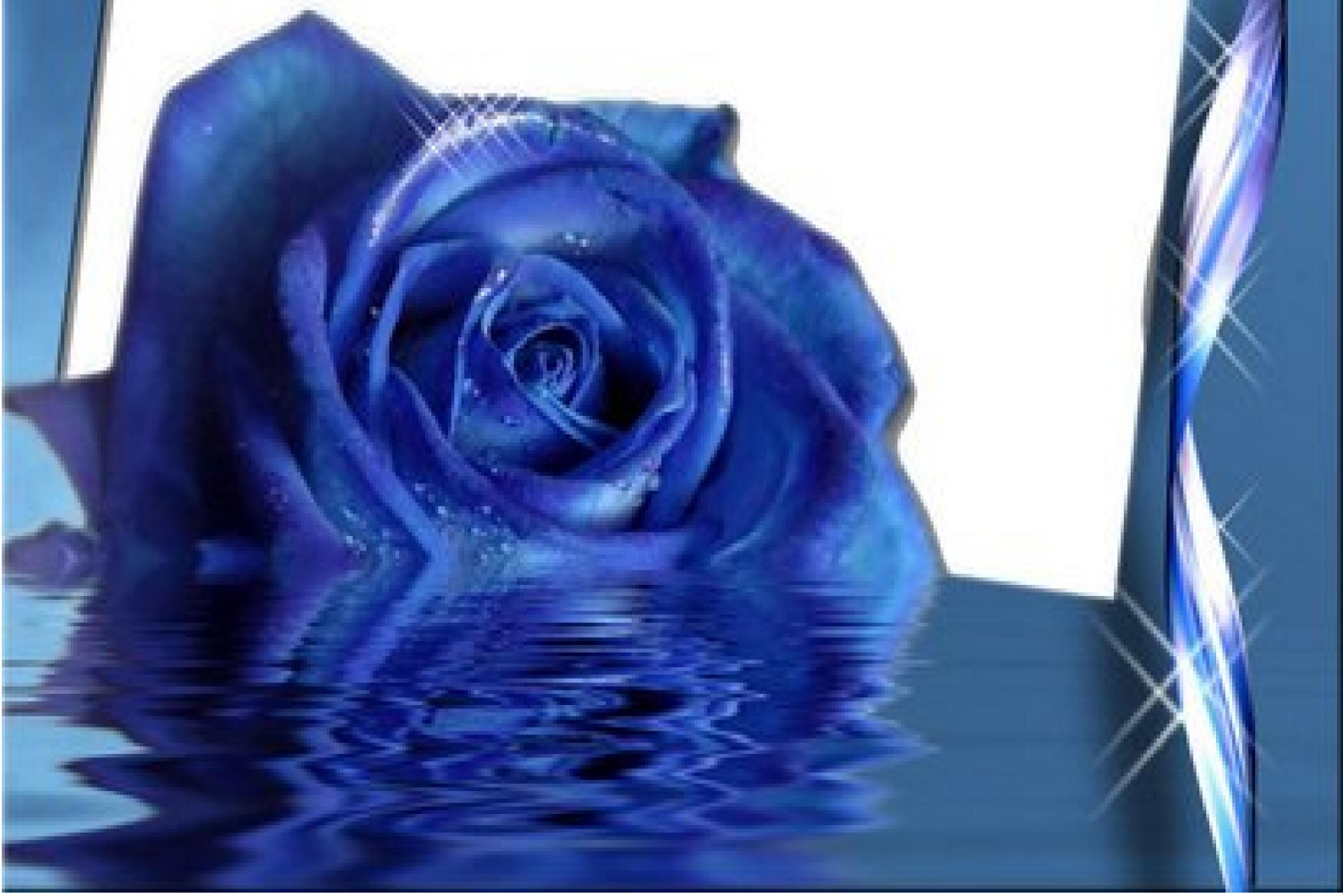

Table des matières

Introduction

La forme originale du théorème des restes chinois apparait sous forme de probléme, Sun Zi écrit vers l'an 300 un traité de mathématique dont ce probléme est le suivant :"soient des objets dont on ignore le nombre, en les comptant 3 par 3 il en reste 2, en les comptant 5 par 5 il en reste 3, en les comptant 7 par 7 il en reste 2, combien y a-t-il d'objets ?".

Qin Jiushao (1202-1261) developpe ce théorème sont traité est remarquablement avancé, il est traite d'un système d'équation linéaire de congruences dans le cas où les modulo ne sont pas premiers entre eux deux à deux.

Le 14^{eme} siécle voit un declin progressif puis un oubli de ces resultats, le savoire de Qin Jiushao ne dépasse pas les frontières chinois avant le 20^{eme} siécle. Il est redécouvert par les travaux de l'historien des sciences Joseph Needham. En revanche, de nombreuses similarités entre les notations arabes et chinois laissent penser à des contacts durant les perriodes précedentes.

L'Inde posséde aussi une tradition en arithmetique, Aryabhata(476-550) recherche de maniére systematique les solutions entières de l'équation linéaire à deux inconnues à coéfficients entiers, il utilise pour ce la un algorithme appelé"Kuttaka".

En Asie centrale et en l'Europe de l'ouest, dans l'erudit islamique Ibn Al-Haitham est un probléme pour resoudre :

$$x \equiv 1 \,(\mathrm{mod}\, 2) \equiv 1 \,(\mathrm{mod}\, 3) \equiv 1 \,(\mathrm{mod}\, 4) \equiv 1 \,(\mathrm{mod}\, 6) \equiv 0 \,(\mathrm{mod}\, 7)\,.$$

Dans d'autres œuvres occidentales des $14^{eme} - 17^{eme}$ siécles apparu quelque problémes de restes avec des solutions simplement incomplètes, au 18^{eme} siécle les grands mathématiciens Euler, Lagrange et Gauss ont étudié successivement les problémes de restes et ils ont accompli de grand réalisation.

Dans notre mémoire on fait des recherches consernant les congruences et théorème des restes chinois et il est partagé en quatre chapitre.

Dans le premier chapitre, on met quelques-unes des définitions afin de clarifier certains des termes que nous avons utilisé dans les chapitres suivantes.

D'abord, dans le deuxième chapitre, on s'interresse aux congruences telle que on parle

de congruence modulo un entier et modulo un polynôme.

En suite, dans le troixième chapitre, on étude trois formes de théorème des restes chinois.

Enfin, le quatrième chapitre contient des applications du théorème des restes chinois.

Chapitre 1

Rappels

Cet chapitre contient des définitions et des notions pour faciliter l'étude des chapitres suivantes. Dans ce chapitre on va donné quelques notions générales sur la théorie d'ensembles et sur l'arithmétique.

1.1 Division euclidienne

On considère deux entiers a et b, si b n'est pas nul, on peut effectuer une division euclidienne de a par b. Cela permet d'obtenir un quotient q et un reste r tels que :

$$a = b \cdot q + r$$

1.2 PGCD et PPCM

Définition 1.2.1 *(PGCD)*

Soit a et b deux nombres entiers, on définit le plus grand commun diviseur de a et b, noté $pgcd(a, b)$, comme étant le plus grand nombre positif qui divise à la fois a et b.

Exemple 1.2.2 *On a $pgcd(12, 14) = 2$.*

En effet, l'ensemble des diviseurs de 12 est $D_{12} = \{1, 2, 3, 4, 6, 12\}$et l'ensemble des diviseurs de 14 est $D_{14} = \{1, 2, 7, 14\}$. L'ensemble des diviseurs commun à 12 et à 14 est donc $D_{12} \cap D_{14} = \{1, 2\}$. Ainsi, le plus grand commun diviseur est 2.

Définition 1.2.3 *Deux nombres a et b tels que $pgcd(a, b) = 1$ sont dit premiers entre-eux.*

Définition 1.2.4 *(PPCM)*

Soit a et b deux nombres entiers, on définit le plus petit commun multiple de a et b, noté $ppcm(a, b)$, comme étant le plus petit nombre positif qui est multiple à la fois de a et de b.

Exemple 1.2.5 *On a* $ppcm(12, 14) = 84$.

En effet, l'ensemble des multiples positifs (ou nul) de 12 *est* $M_{12} = \{0, 12, 24, 36, 48, 60, 72, 84, ...\}$ *et l'ensemble des multiples positifs (ou nul) de* 14 *est* $M_{14} = \{0, 14, 28, 42, 56, 70, 84, 98, ...\}$

L'ensemble des multiples positifs (ou nul) commun à 12 *et à* 14 *est donc* $M_{12} \cap M_{14} = \{0, 84, 168, 252, ...\}$. *Ainsi, le plus petit commun multiple est* 84.

1.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition 1.3.1 *Pour chaque* $n \in \mathbb{N}$, *on définit :*

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, ..., n-1\}$$

En suivant le principe ci-dessus, l'addition et la multiplication de $\mathbb{Z}$ *permet de mettre une structure d'anneau sur cet ensemble.*

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *est appelé l'anneau des restes de division modulo* n. *Lorsqu'on calcule dans un tel anneau, on utilise le symbole* $\equiv$ *au lieu de* $=$.

1.4 Un idéal

Définition 1.4.1 *(Idéal d'un anneau)*

Soit $\mathbb{A}$ *un anneau commutatif. Un sous-ensemble* $I \subset \mathbb{A}$*est un idéal si :*

i) $a + a' \in I$ *pour tout* $a, a' \in I$.

ii) $ra \in I$ *pour tout* $a \in I$ *et tout* $r \in \mathbb{A}$.

En d'autres termes, un idéal est un sous-ensemble fermé pour l'addition et stable par multiplication par un élément quelconque de $\mathbb{A}$.

Les idéaux $I = \{0\}$*et* $I = \mathbb{A}$ *sont appelés les idéaux triviaux.*

1.5 Idéaux comaximaux

Définition 1.5.1 *Soit* $(\mathbb{A}, +, \cdot)$*un anneau commutatif, soient* I *et* J *deux idéaux de* $\mathbb{A}$. *On dit que* I *et* J *sont comaximaux si et seulement si* $I + J = \mathbb{A}$.

Il y a une certaine analogie entre les notions d'idéaux comaximaux dans un anneau commutatif et de nombres premiers entre eux dans $\mathbb{Z}$, la différence principale étant que cela concerne non plus des éléments mais des idéaux.

Dans $\mathbb{Z}$ ou dans $\mathbb{K}[x]$, si deux éléments sont premiers entre eux, alors leur *ppcm* est égal à leur produit.

Proposition 1.5.2 *Soit* $(\mathbb{A}, +, \cdot)$*un anneau commutatif, soient* I *et* J *deux idéaux de* $\mathbb{A}$*. si* I *et* J *sont comaximaux, on a* $IJ = I \cap J$*.*

1.6 Domaine d'intégrité

Un domaine d'intégrité est un anneau intègre ou anneau d'intégrité.

Définition 1.6.1 *Soit* $(\mathbb{A}, +, \times)$ *un anneau commutatif unitaire,* $\mathbb{A}$ *est un domaine d'intégrité s'il est :*

- *différent de l'anneau nul, c'est-à-dire s'il possède au moins deux éléments.*
- *sans diviseur de zéro, c'est-à-dire :*

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

1.7 L'indicatrice d'Euler

La fonction indicatrice d'Euler φ associe a un entier $n \geq 2$, l'entier $\varphi(n)$ défini par :

$$\varphi(n) = card\{a; 0 \leq a \leq n \text{ et } pgcd(a, n) = 1\}. \qquad (1)$$

Proposition 1.7.1 *Soit* p *un nombre premier et* $\alpha \in \mathbb{N}^*$*. On a*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

En particulier $\varphi(p) = p - 1$*.*

Corollaire 1.7.2 *Soient* $m, n \geq 2$*. Si* $pgcd(m, n) = 1$*, alors* $\varphi(mn) = \varphi(m)\varphi(n)$*.*

Chapitre 2

Congruence

Dans ce chapitre, on s'interresse à l'étude des congrunce. En suite, nous allons pouvoir définir une congrunce modulo un polyôme et les polynômes unitaires ainsi que la division et les anneaux de polynôme commutatifs unitaires et enfin nous parlons aux polynôme premiers.

2.1 Congruence

Soit a et b deux entier relatifs, et n un entier naturel non nul.

Définition 2.1.1 *On dit que a et b sont congru modulo n si a et b on même reste dans la division euclidienne par n et on note $a \equiv b\,[n]$ ou $a \equiv b\,(\mathrm{mod}\, n)$.*

Théorème 2.1.2 *a et b ont le même reste dans la division euclidienne par n si et seulement si $a - b$ est divisible par n et en note $n|\,(a-b)$.*

Preuve.

1. Si a et b ont même reste dans la division euclidienne par n, $a = nq_1 + r$ et $b = nq_2 + r$ avec q_1 et q_2 dans $\mathbb{Z}$ et $0 \leq r < n$.

   Alors

$$a - b = nq_1 + r - (nq_2 + r) = n\,(q_1 - q_2)$$

Donc $n|\,(a-b)$

1. Réciproquement, si $n|(a-b)$, $\exists k \in \mathbb{Z}$ tel que $a - b = kn$. Soit r le reste de la division euclidienne de b par n, alors $b = nq + r$, avec $q \in \mathbb{Z}$et $0 \leq r < n$, donc

$$a = b + kn = nq + r + kn = (q + k)n + r$$

avec $0 \leq r < n$, $(q+k) \in \mathbb{Z}$, alors r est aussi le reste de la division euclidienne de a par n.

■

Corollaire 2.1.3 *D'après le théorème précédent,* $a \equiv b\,[n]$ *si et seulement si* $n|(a-b)$.

Exemple 2.1.4

$$13 \equiv 35 \equiv 43 \equiv -2\,[5]$$

$$41 \equiv 17 \equiv 56 \equiv -1\,[6]$$

$$35 \equiv 11 \equiv 1 \equiv -3\,[2]$$

L'ensemble de tous les entiers qui sont congrus à b modulo n est l'ensemble $\{b + kn/k \in \mathbb{Z}\}$. Ceci nous permet de démontrer le résultat suivant :

Théorème 2.1.5 *Soit* m *un entier* > 1. *Alors tout nombre entier* a *est congru modulo* n a *un et un seul entier* r *de l'ensemble* $\{1, 2, 3, ..., n-1\}$. *De plus, cet entier* r *est exactement le reste de la division de* a *par* n. *En d'autres termes, si* $0 \leq r < m$, *alors* $a \equiv r(\mathrm{mod}\, n)$ *si et seulement si* $a = qn + r$ *où* q *est le quotient de* a *par* n *et* r *le reste.*

Preuve. C'est une conséquence immédiate de la défnition de la congruence et de la division euclidienne. ■

La relation de la congruence $\equiv$ est une relation d'équivalence.

Théorème 2.1.6 *Soit* a, b *et* n *des entiers avec* $n > 1$, *alors :*

i) $a \equiv a(\mathrm{mod}\, n)$.

ii) *Si* $a \equiv b(\mathrm{mod}\, n)$ *alors* $b \equiv a(\mathrm{mod}\, n)$.

iii) *Si* $a \equiv b(\mathrm{mod}\, n)$ *et* $b \equiv c(\mathrm{mod}\, n)$, *alors* $a \equiv c(\mathrm{mod}\, n)$.

Preuve. Les partie (i) et (ii) sont évidentes, nous démontrons (iii).

Les hypothéses impliquent que $b = a + kn$ et $c = b + ln$, mais alors $c = a + kn + ln = a + n(k + l)$ ce qui montre que a et c sont congrus modulo n. ■

la relation de congruence $\equiv$ est compatible avec la somme et le produit.

Théorème 2.1.7 *Soient* a, b, a_1, b_1 *et* $n > 1$ *des entiers tels que* $a \equiv b(\mathrm{mod}\, n)$ *et* $a_1 \equiv b_1(\mathrm{mod}\, n)$ *alors :*

a) $a + a_1 \equiv b + b_1(\mathrm{mod}\, n)$.

b) $aa_1 \equiv bb_1(\mathrm{mod}\, n)$.

c) *Si* $a \equiv b(\mathrm{mod}\, n)$*, alors* $a^k \equiv b^k(\mathrm{mod}\, n)$ *pour tous les entiers positifs* k*.*

d) *Soit* $f(x)$ *un polynôme à coefficients entiers, si* $a \equiv b(\mathrm{mod}\, n)$ *alors* $f(a) \equiv f(b)\,(\mathrm{mod}\, n)$*.*

Preuve. On a $a = b + kn$ et $a_1 = b_1 + ln$ on a alors :

$$a + a_1 \equiv b + b_1(l + k)n$$

ce qui démontre a), on a également :

$$aa_1 = bb_1 + lbn + b_1kn + lkn^2 = bb_1 + sn$$

ce qui montre b)

c) Prenant $c = a$ et $b = d$ dans iii) du théorème 2.1.6 nous voyons que $a \equiv b(\mathrm{mod}\, n)$ implique $a^2 \equiv b^2(\mathrm{mod}\, n)$ nous appliquons oncor iii) une fois nous obtenons :

$a^3 \equiv b^3(\mathrm{mod}\, n)$et le cas général suit par induction.

d) Supposons que $f(x) = \sum_{j=0}^{m} c_j x^{\ j}$,utilisons c) on obtient $a^j \equiv b^j(\mathrm{mod}\, n)$ pour chaque j.

Puis $c_j a^j \equiv c_j b^j(\mathrm{mod}\, n)$ de iii) du théorème 2.1.6 et enfin, l'application répétée de a) donne

$$f(a) = \sum_{j=0}^{m} c_j a^j \equiv \sum_{j=0}^{m} c_j b^j = f(b)(\mathrm{mod}\, n).$$

■

Théorème 2.1.8 *Soit* c *un nombre entier non null.*

i) *Si* $ca \equiv cb(\mathrm{mod}\, n)$*, alors être* $a \equiv b(\mathrm{mod}\, n/pgcd(c, n))$*.*

ii) *Si* $ca \equiv cb(\mathrm{mod}\, n)$ *et* $pgcd(c, n) = 1$ *alors* $a \equiv b(\mathrm{mod}\, n)$*.*

Preuve.

i) Soit $d = pgcd(c, n)$,

si $ca \equiv cb(\mathrm{mod}\, n)$, alors $n|c(a-b)$ et $\frac{n}{d}|\frac{c}{d}(a-b)$ de puis $pgcd(\frac{n}{d}, \frac{c}{d}) = 1$ il s'ensuit que $\frac{n}{d}|(a-b)$ i,e : $a \equiv b(\mathrm{mod}\, \frac{n}{d})$ ■

Un système de congruence peut être remplacé par une congruence dans ce que suit façon :

Théorème 2.1.9 *Soit* $m_1, m_2, ..., m_r$ *êtres des entiers positifs, les deux déclarations suivantes sont équivalentes :*

i) $a \equiv b(\mathrm{mod}\, m_i)$ *pour* $i = 1, 2, ..., r$*.*

ii) $a \equiv b(\mathrm{mod}\, ppcm\,[m_1, ..., m_p])$.

Preuve. Supposons que $a \equiv b(\mathrm{mod}\, m_i)$ pour tout i puis $(a-b)$ est un multiple commun de tout les m_i, et par conséquent $ppcm\,[m_1, ..., m_p]\,|(a-b)$ cela signifie que $a \equiv b(\mathrm{mod}\, ppcm\,[m_1, ..., m_p])$. ■

Remarque 2.1.10 *La relation $\equiv$ se comporte sur de nombreux points comme la relation d' égalité $=$, néanmoins, une propriété de la relation d'égalité n'est plus vraie pour celle de congruence, a savoir la simplification :*

Si $ab \equiv ac\,(\mathrm{mod}\, m)$, on n'a pas nécessairement $b \equiv c\,(\mathrm{mod}\, m)$. Par exemple $2 \cdot 1 \equiv 2 \cdot 3(\mathrm{mod}\, 4)$ mais 1 et 3 ne sont pas congrus modulo 4.

De même, $4 \cdot 3 \equiv 4 \cdot 6\,(\mathrm{mod}\, 12)$ mais 3 et 6 ne sont pas congrus modulo 12.

Nous verrons plus loin quelle règle utiliser lors des simplifications.

Théorème 2.1.11 *(d'Euler)*

Soit a et m deux entiers tels que $m > 1$ et $pgcd\,(a, m) = 1$.

Alors

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

Théorème 2.1.12 *(Petit théorème de Fermat)*

Soit a un nombre entier et p un premier ne divisant pas a.

Alors

$$a^{p-1} \equiv 1\,(\mathrm{mod}\, p)\,.$$

Preuve. C'est une conséquence immédiate du théorème d'Euler en sachant que $\varphi\,(p) = p - 1$ lorsque p est premier. ■

2.2 Une congruence modulo un polynôme

Soit $\mathcal{F}$ un corps, $p\,(x)$ un polynôme à coéfficients dans $\mathcal{F}$, pour $f(x)$ et $g(x)$ dans $\mathcal{F}\,[x]$, on dit que $f(x)$ est congru à $g(x)$ (modulo $p(x)$), et écrit $f(x) \equiv g(x)(\mathrm{mod}\, p(x))$ si $p(x)$ divise $f(x) - g(x)$, où de façon équivalente

$$f(x) = g(x) + m(x)p(x)$$

pour certains polynôme $m(x)$ dans $\mathcal{F}\,[x]$.

Propriété 2.2.1 *Congruence modulo $p\,(x)$ a des propriétés identiques à congruence modulo m de entiers, où m est un nombre naturel.*

1. *Si* $f \equiv g(\mathrm{mod}\, m)$, *alors* $kf \equiv kg(\mathrm{mod}\, m)$, $k \in \mathbb{R}$.
2. *Si* $f_1 \equiv g_1(\mathrm{mod}\, m)$ *et si* $f_2 \equiv g_2(\mathrm{mod}\, m)$ *alors on a :* $f_1 + f_2 \equiv g_1 + g_2(\mathrm{mod}\, m)$ *et* $f_1 f_2 \equiv g_1 g_2(\mathrm{mod}\, m)$.
3. *Si* $f \equiv g(\mathrm{mod}\, m)$ *et* $g \equiv h(\mathrm{mod}\, m)$ *donc :* $f \equiv h(\mathrm{mod}\, m)$.

Preuve.

1. On a $f = g + f_1 m$

$$kf = kg + kf_1 m, k \in \mathbb{R}.$$

On pose $kf_1 = f_2$, alors

$$kf = kg + f_2 m \implies kf \equiv kg(\mathrm{mod}\, m).$$

1. On a $f_1 \equiv g_1(\mathrm{mod}\, m)$ et $f_2 \equiv g_2(\mathrm{mod}\, m)$, il existe donc f' et $f'' \in \mathcal{F}[x]$ tels que : $f_1 - g_1 = mf'$ et $f_2 - g_2 = mf''$.
Le polynôme $f_1 + f_2 - (g_1 + g_2)$ est un multiple de m.
En effet :

$$\begin{aligned} f_1 + f_2 - (g_1 + g_2) &= (f_1 - g_1) + (f_2 - g_2) \\ &= mf' + mf'' \\ &= m(f' + f'') \end{aligned}$$

On a donc :

$$f_1 + f_2 \equiv g_1 + g_2(\mathrm{mod}\, m)$$

D'autre part, on a :

$$\begin{aligned} f_1 f_2 &= (mf' + g_1)(mf'' + g_2) \\ f_1 f_2 - g_1 g_2 &= (mf' + g_1)(mf'' + g_2) - g_1 g_2 \\ &= m^2 f' f'' + mf' g_2 + mf'' g_1 + g_1 g_2 - g_1 g_2 \\ &= m(mf' f'' + f' g_2 + f'' g_1) \end{aligned}$$

L'égalité $f_1 f_2 \equiv g_1 g_2(\mathrm{mod}\, m)$ est donc également vérifiée.

2. On a $f = g + f_1 m$ et $g = h + f_2 m$ donc :

$$\begin{aligned} f &= h + f_2 m + f_1 m \\ &= h + m(f_1 + f_2) \implies f \equiv h(\mathrm{mod}\, m). \end{aligned}$$

■

2.3 Polynômes unitaires

Soit $\mathbb{A}$ un anneau unitaire ayant $1_{\mathbb{A}}$ pour unité, alors $1_{\mathbb{A}} = 1_{\mathbb{A}}x^0$ est l'unité de $\mathbb{A}[x]$ puisque $1_{\mathbb{A}}x^0 \cdot \alpha(x) = \alpha(x)$ pour tout $\alpha(x) \in \mathbb{A}[x]$. De plus, écrivant $x = 1_{\mathbb{A}}x^1 = 0_{\mathbb{A}}x^0 + 1_{\mathbb{A}}x^1$, nous avons $x \in \mathbb{A}[x]$. A présent $a_k\underbrace{(x \times x \times ... \times x)}_{k \text{ facteurs}} = a_k x^k \in \mathbb{A}[x]$ de sorte que dans $\alpha(x) = a_0 + a_1x + a_2x^2 + ...$ nous pouvons considèrer l'indice superieur i dans a_ix^i comme étant véritablement un exposant, la juxtaposition dans tout terme a_ix^i comme la multiplication de l'anneau (des polyôme), et le connecteur + comme l'addition de l'anneau (des polyôme).

Tout polyôme $\alpha(x)$ de degré m sur $\mathbb{A}$ dont le coefficient du terme de plus haut degré est $1_{\mathbb{A}}$, l'unité de $\mathbb{A}$ est dit unitaire.

Exemple 2.3.1 *Les polynômes* 1, $x+3$*et* x^2-5x+4 *sont unitaire tandis que* $2x^2-x+5$ *n'est pas un polynôme unitaire sur* $\mathbb{Z}$.

2.4 Division

Théorème 2.4.1 *Soit* $\mathbb{A}$ *un anneau ayant pour unité* $1_{\mathbb{A}}$, *soit* $\alpha(x) = a_0+a_1x+a_2x^2+...+a_mx^m \in \mathbb{R}[x]$ *le polynôme nul où de degré* m, *et* $\beta(x) = b_0+b_1x+b_2x^2+...+ux^n \in \mathbb{A}[x]$ *un polynôme unitaire de degré* n. *Alors il existe des polynômes uniques* $q_{\Re}(x)$, $r_{\Re}(x)$, $q_{\pounds}(x)$, $r_{\pounds}(x) \in \mathbb{A}[x]$ *où* $r_{\Re}(x)$, $r_{\pounds}(x)$ *sont soit égaux au polynôme nul soit de degré* $< n$ *tel que :*

i) $\alpha(x) = q_{\Re}(x) \cdot \beta(x) + r_{\Re}(x)$

ii) $\alpha(x) = \beta(x) \cdot q_{\pounds}(x) + r_{\pounds}(x)$

Dans la proposition (i) du théorème 2.4.1 nous disons que $\alpha(x)$ a été divisé à droite par $\beta(x)$ pour obtenir le quotient à droite $q_{\Re}(x)$ et le reste à droite $r_{\Re}(x)$. De façon analogue, dans (ii) nous disons que $\alpha(x)$ a été divisé à gauche par $\beta(x)$ pour obtenir le quotient à gauche $q_{\pounds}(x)$ et le reste à gauche $r_{\pounds}(x)$. Quand $r_{\Re}(x) = 0_{\mathbb{A}}(r_{\pounds}(x) = 0_{\mathbb{A}})$, nous appelons $\beta(x)$ un diviseur à droite(à gauche) de $\alpha(x)$.

Pour le cas particulier $\beta(x) = 1_{\mathbb{A}}x - b = x - b$, le théorème 2.4.1 donne le :

Théorème 2.4.2 *Les restes à droite et à gauche de la division de* $\alpha(x)$ *par* $x-b$, $b \in \mathbb{A}$, *sont respectivement*

$$r_{\Re}(x) = a_0 + a_1b + a_2b^2 + ... + a_nb^n$$

et

$$r_{\pounds}(x) = a_0 + ba_1 + b^2a_2 + ... + b^na_n$$

Il s'ensuite le :

Théorème 2.4.3 *Un polynôme $\alpha(x)$ est divisible à droite(à gauhe) par $x-b$ si et seulement si $r_{\Re}(x)=0_{\mathbb{A}}(r_{\pounds}(x)=0_{\mathbb{A}})$.*

2.5 Annaux de polynôme commutatifs unitaires

Soit $\mathbb{A}$ un anneau comutatif unitaire, alors $\mathbb{A}[x]$ est un anneau commutatif unitaire (quelle est sont unité ?) et les théorèmes 2.4.1 à 2.4.3 peuvent être enoncés à nouveau sans faire de destruction entre les quotients à droite et à gauche (on remplace $q_{\Re}(x)=q_{\pounds}(x)$ par $q(x)$), entre les restes à droite et à gauche(on remplace $r_{\Re}(x)=r_{\pounds}(x)$ par $r(x)$) et entre diviseurs à droite et à gauche. Ainsi les propositions (i) et (ii) du théorème 2.4.1 peuvent être remplacées par :

iii) $\alpha(x)=q(x)\cdot\beta(x)+r(x)$

Et en particulier, nous avons le :

Théorème 2.5.1 *Dans un anneau de polynôme commutatif unitaire, un polynôme $\alpha(x)$ de degré m admet $x-b$ comme diviseur si et seulement si le reste :*

$$r=a_0+a_1b+a_2b^2+...+a_mb^m=0_{\mathbb{A}}.$$

Quand, comme dans le théorème 2.5.1, $r=0_{\mathbb{A}}$ alors b est appeellé un zéro(racine) du polynôme $\alpha(x)$.

Exemple 2.5.2 *Le polynôme x^2-4 sur $\mathbb{Z}$ admet 2 et -2 comme zéros puisque $(2)^2-4=0$ et que $(-2)^2-4=0$*

Quand $\mathbb{A}$ est n'a pas de diviseurs de zéro, il en est de même de $\mathbb{A}[x]$. en effet, supposons que $\alpha(x)$ et $\beta(x)$ soient des éléments de $\mathbb{A}[x]$, de degré respectifs m et n et que :

$$\alpha(x)\cdot\beta(x)=a_0b_0+(a_0b_1+a_1b_0)x+...+a_mb_nx^{m+n}=0$$

Alors chaque coéfficient du produit et en particulier a_mb_n est égal à $0_{\mathbb{A}}$. Mais $\mathbb{A}$ est n'a pas de diviseur de zéro, ainsi $a_mb_n=0_{\mathbb{A}}$ si et seulement si $a_m=0_{\mathbb{A}}$ ou $b_n=0_{\mathbb{A}}$. Puisque cela contredit l'hipothèse que $\alpha(x)$ et $\beta(x)$ sont de degré m et n, $\mathbb{A}[x]$ est n'a pas de diviseurs de zéro.

Il s'ensuit le :

Théorème 2.5.3 *Un anneau de polynômes $\mathbb{A}[x]$ est un domaine d'integrité si et seulement si l'anneau des coefficients $\mathbb{A}$ est un domaine d'integrité.*

2.6 L'anneau de polynômes $\mathcal{F}[x]$

Le plus important des anneaux de polynômes apparaît quand l'anneau des coefficient est un corps commutatif $\mathcal{F}$. Nous rappelons que tout élément non nul d'un corp $\mathcal{F}$ est une unité de $\mathcal{F}$ et enonçons à nouveau pour le domaine d'integrité $\mathcal{F}[x]$ les résultats principaux des paragraphes ci dessous comme suit :

L'algorithme de la division :

Si $\alpha(x)$ et $\beta(x) \in \mathcal{F}[x]$ où $\beta(x) \neq 0_{\mathcal{F}}$ il existe des polynômes uniques $q(x)$, $r(x)$ un polynôme nul où de degré inferieur de $\beta(x)$, tels que :

$$\alpha(x) = q(x) \cdot \beta(x) + r(x)$$

Quand $r(x)$ est le polynôme nul, $\beta(x)$ est appelé un diviseur de $\alpha(x)$ et nous écrivons $\beta(x) \mid \alpha(x)$.

Théorème de reste :

Si $\alpha(x)$, $x - b \in \mathcal{F}[x]$, le reste de la division de $\alpha(x)$ par $x - b$ est $\alpha(b)$.

Théorème de factorisation :

Si $\alpha(x) \in \mathcal{F}[x]$ et $b \in \mathcal{F}$, alors $x-b$ est un facteur de $\alpha(x)$ si et seulement si $\alpha(b) = 0_{\mathcal{F}}$, ie $x - b$ est un facteur de $\alpha(x)$ si et seulement si b est un zéro de $\alpha(x)$.

Il s'ensuit le :

Théorème 2.6.1 *Soit $\alpha(x) \in \mathcal{F}[x]$ de degré $m > 0$ et de coefficient du terme de plus haut degré égal à a si les éléments distincts $b_1, b_2, ..., b_m$ de $\mathcal{F}$ sont des zéros de $\alpha(x)$, alors :*

$$\alpha(x) = a(x - b_1)(x - b_2)...(x - b_m)$$

Théorème 2.6.2 *Tout polynôme $\alpha(x) \in \mathcal{F}[x]$ de degré $m > 0$ admet au plus m zéros distincts dans $\mathcal{F}$.*

Exemple 2.6.3 *:*

a) *Le polynôme $2x^2 + 7x - 15 \in \mathbb{Q}[x]$ admet comme zéros $3/2$, $-5 \in \mathbb{Q}$.*

b) *Le polynôme $x^2 + 2x + 3 \in \mathbb{C}[x]$ admet comme zéros $-1 + i\sqrt{2}$ et $-1 - i\sqrt{2}$ dans $\mathbb{C}$, cependant $x^2 + 2x + 3 \in \mathbb{Q}[x]$ n'admet pas de zéros dans $\mathbb{Q}$.*

Théorème 2.6.4 *Soient $\alpha(x)$, $\beta(x) \in \mathcal{F}[x]$ tels que $\alpha(s) = \beta(s)$ pour tout $s \in \mathcal{F}[x]$. Alors si le nombre d'éléments de $\mathcal{F}$ est superieur aux degrés de $\alpha(x)$ et $\beta(x)$, nous avons nécéssairement $\alpha(x) = \beta(x)$.*

2.7 Polynôme premiers

Il n'est pas difficile de montrer que les seules unités d'un anneau de polynôme $\mathcal{F}[x]$ sont les éléments non nuls (i,e les unités) de l'anneau des coefficients $\mathcal{F}$. Ainsi les seuls éléments associés à $\alpha(x) \in \mathcal{F}[x]$ sont les éléments $v \cdot \alpha(x)$ de $\mathcal{F}[x]$ où v est une unité quelconque de $\mathcal{F}$.

Puisque pour tout $v \neq z \in \mathcal{F}$ et tout $\alpha(x) \in \mathcal{F}[x]$

$$\alpha(x) = v^{-1} \cdot \alpha(x)v.$$

Tendis que si $\alpha(x) = q(x) \cdot \beta(x)$

$$\alpha(x) = \left[v^{-1}q(x)\right] \cdot \left[v\beta(x)\right].$$

Il s'ensuite que (a) tout unité de $\mathcal{F}$ et tout élément associée de $\alpha(x)$ et (b) si $\beta(x)$

$|\alpha(x)$ il ent est de même de tous les éléments associés à $\beta(x)$, les éléments de $\mathcal{F}$ et les éléments associés de $\alpha(x)$ sont appelés diviseurs triviaux de $\alpha(x)$, les autres diviseurs de $\alpha(x)$ s'il en existes, sont appelés diviseurs non triviaux.

Un polynôme $\alpha(x) \in \mathcal{F}$ de degré $m \geq 1$ est appelé un polynôme premier(irréductible)dans $\mathcal{F}$ si et seulement si ces diviseures sont triviaux.

Exemple 2.7.1 *:*

(a) *Le polynôme* $3x^2 + 2x + 1 \in \mathbb{R}[x]$ *est un polynôme premier dans* $\mathbb{R}$.

(b) *Tout polynôme* $ax + b \in \mathcal{F}[x]$*, avec* $a \neq z$ *est un polynôme premier dans* $\mathcal{F}$.

Chapitre 3

Théorème des restes Chinois

Dans ce chapitre, nous prouvons le théorème des restes chinois, qui donne conditions dans lesquelles un système d'équations linéaires est garanti d'avoir une solution. Au 4ème siècle un mathématicien chinois posé la question suivante :

Question : Combien l'armée de Han Xing comporte-t-elle de soldats si : rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

En notation moderne, le question précédent nous demande de trouver une solution de nombre entier positif au système de trois équations suivantes :

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

Le théorème des restes chinois affirme qu'il existe une solution, et la preuve donne une méthode pour en trouver un.

3.1 Le théorème des restes chinois

Lemme 3.1.1 *Supposons que $m_1, m_2, ..., m_t$, m sont des entiers non nuls tel que :*

$$pgcd\,(m, m_i) = 1, \forall i = 1, ..., t.$$

Alors :

$$pgcd\,(m, m_1, m_2, ..., m_t) = 1.$$

Preuve. Supposons que $pgcd\,(m, m_1, m_2, ..., m_t) > 1$, puis il existe un nombre premier

p satisfait $p|m$ et $p|\left(m_1, m_2, ..., m_t\right)$, comme p premier on a $p|m_i\ \forall i$ et donc $PGCD\left(m; m_i\right) \neq 1$, donc contradiction. ■

Théorème 3.1.2 *(Théorème des restes chinois) :*
Soient $m_1, m_2, ..., m_t$ des entiers positives deux à deux premiers entre eux, et $m = m_1 m_2 ... m_t$.
Soient $a_1, a_2, ..., a_t \in \mathbb{Z}, \exists c \in \mathbb{Z}$ tel que :

$$\begin{cases} c \equiv a_1 \left(\operatorname{mod} m_1\right), \\ c \equiv a_2 \left(\operatorname{mod} m_2\right), \\ \qquad \vdots \\ c \equiv a_t \left(\operatorname{mod} m_t\right). \end{cases}$$

Si c est une solution alors la solution générale est :

$$x = c + ms; s \in \mathbb{Z}.$$

Preuve.

1. Pour $i = 1, 2, ..., t$, soit $n_i = \frac{m}{m_i}$ alors $m = n_i m_i$ notez que $pgcd\left(m_i, n_i\right) = 1$, pour tout $i = 1, 2, ..., t$, d'aprés le lemme 3.1.1, et comme les m_i sont deux à deux premiers entre eux.
   Par consèquent, pour chaque i la congruence $n_i x \equiv 1 \left(\operatorname{mod} m_i\right)$ est résoluble autrement dit : pour tout i il existe un entier b_i satisfaisant :

$$n_i b_i \equiv 1 \left(\operatorname{mod} m_i\right) \qquad (1)$$

   D'autre part : si $j \neq i$ alors :

$$n_j b_j \equiv 0 \left(\operatorname{mod} m_i\right) \qquad (2)$$

   Puisque $m_i | n_j$ maintenant : Soit $c = a_1 n_1 b_1 + ... + a_t n_t b_t$.
   D'aprés (2)

$$a_j n_j b_j \equiv 0 \left(\operatorname{mod} m_i\right), \forall j \neq i$$

   et donc

$$c = a_i n_i b_i \left(\operatorname{mod} m_i\right).$$

   Mais d'aprés (1) $n_i b_i \equiv 1 \left(\operatorname{mod} m_i\right)$ et donc $c \equiv a_i \left(\operatorname{mod} m_i\right)$.
2. Supposons que d est un autre solution de ce système alors :

$$c \equiv d \left(\operatorname{mod} m_i\right), \forall i \implies c \equiv d \left(\operatorname{mod} m\right).$$

De sorte que : $d = c + ms, \forall s$. Inversement, si $d \equiv c + ms, \forall s$ alors, $d \equiv c \pmod{m}$ et donc pour tout i, $d \equiv c \equiv a_i \pmod{m_i}$, alors d est une solution.

■

Exemple 3.1.3 *:*

$$\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 5 \pmod{7}, \\ x \equiv 7 \pmod{11}. \end{cases}$$

Dans ce systéme : $a_1 = 3, a_2 = 5, a_3 = 7$

$$m_1 = 5, m_2 = 7, m_3 = 11$$

donc : $n_1 = 7 \times 11 = 77$

$n_2 = 5 \times 11 = 55$

$n_3 = 5 \times 7 = 35$

Pour obtenir b_1 *: résoudre* $77x \equiv 1 \pmod{5}$ *; c'est à dire* $2x \equiv 1 \pmod{5}$, *donc nous pouvons prendre* $b_1 = 3$.

Pour obtenir b_2 *: résoudre* $55x \equiv 1 \pmod{7}$ *; c'est à dire* $-x \equiv 1 \pmod{7}$ *,(depuis* $55 \equiv -1 \pmod{7}$*) donc nous pouvons prendre* $b_2 = -1$.

Pour obtenir b_3 *: résoudre* $35x \equiv 1 \pmod{11}$ *; c'est à dire* $2x \equiv 1 \pmod{11}$ *,donc nous pouvons prendre* $b_3 = 6$.

Enfin, la solution de ce systéme est :

$$\begin{aligned} c &= a_1 n_1 b_1 + a_2 n_2 b_2 + a_3 n_3 b_3 \\ &= 77 \times 3 \times 3 + 55 \times 5 \times (-1) + 35 \times 7 \times 6 \\ &= 693 - 275 + 1470 = 1888 \end{aligned}$$

Maintenant : $m = m_1 m_2 m_3 = 5 \times 7 \times 11 = 385$ *donc la solution générale est :*

$$x = 1888 + 385t, t \in \mathbb{Z}$$

Il s'agit de la classe de 1888 *modulo* 385 *depuis* $1888 \equiv 348 \pmod{385} \iff x = 348 + 385t$, $t \in \mathbb{Z}$.

3.2 Le théorème des restes chinois pour les polynômes

Théorème 3.2.1 *Soit* $\mathcal{F}$ *un corps, soit* $a_1(x) ... a_n(x)$ *des polynômes quleconque et* $m_1(x) ... m_n(x)$ *des polynômes deux à deux premiers entre eux dans* $\mathcal{F}[x]$*, alors il existe un polynôme*

$f(x) \in \mathcal{F}[x]$ *tel que :*

$$\begin{cases} f(x) \equiv a_1(x) \pmod{m_1(x)}, \\ \vdots \\ f(x) \equiv a_n(x) \pmod{m_n(x)}. \end{cases}$$

Si $f_1(x)$ *et* $f_2(x)$ *sont deux solutions, alors :*

$$f_1(x) \equiv f_2(x) \pmod{m_1(x) ... m_n(x)}.$$

Ce théorème peut être prouvé de la même maniére que le théorème des restes chinois pour les entiers, voici une preuve :

Preuve. Comme $m_i(x)$ est premier à $m_j(x)$ pour tout $j \neq i$, $m_i(x)$ rester premier sur le produit

$$l_i(x) = m_1(x) m_2(x) ... m_{i-1}(x) m_{i+1}(x) ... m_n(x)$$

Ainsi, nous pouvons rèsoudre l'equation

$$1 = h_i(x) m_i(x) + k_i(x) l_i(x).$$

Pour $k_i(x)$ et $h_i(x)$ par le lemme de Bezout, alors $k_i(x) l_i(x)$ satisfait por tout $j \neq i$

$$\begin{aligned} k_i(x) l_i(x) &\equiv 1 \pmod{m_i(x)}, \\ k_i(x) l_i(x) &\equiv 0 \pmod{m_j(x)}. \end{aligned}$$

Donc, nous resolvons le système principal du théorème des restes chinois, en definissant $f(x) = f_0(x)$ où :

$$f_0(x) = a_1(x) k_1(x) l_1(x) + a_2(x) k_2(x) l_2(x) + ... + a_n(x) k_n(x) l_n(x).$$

Comme, avec les chiffres, si $f_0(x)$ est une solution du systéme principal du théorème des restes chinois, alors tout solution $f(x)$ satisfera :

$$f(x) \equiv f_0(x) \pmod{m_1(x) ... m_n(x)}.$$

Si les $m_i(x)$ sont deux à deux premiers entre eux, En particulier, il existe un unique solution du système principal du théorème des restes chinois dont le degré est inferieur au degré de $m_1(x) ... m_n(x)$ si $r_1 ... r_n$ sont des élèments distincts de $\mathcal{F}$ et $s_1 ... s_n$ sont des élèments quelconques de $\mathcal{F}$, il existe un unique polynôme $q(x) \in \mathcal{F}[x]$ de degré $< n$ tel que : $q(r_i) = s_i$ pour tout $i = 1, ..., n$. ■

3.3 Théorème des restes chinois dans $\mathbb{Z}$

Théorème 3.3.1 *Soit $n = n_1 \times n_2 \times ... \times n_k$ avec les nombres $(n_i)_{1\leq i\leq k}$ deux à deux premiers entre eux. Alors l'application*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z} \\ x &\rightarrow (x_1,\ x_2, ...,\ x_k)\,, \end{aligned}$$

où les x_i est la classe de x modulo n_i, est un isomorphisme d'anneaux.

Pour bien comprendre ce théorème, nous allons détailler un exemple. Prenons $n = 30 = 2 \times 3 \times 5$ et notons $\varphi : \mathbb{Z}/30\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ l'isomorphisme décrit ci-dessus. Les valeurs de φ sont données dans le tableau ci-dessous.

$\varphi(0) = (0,0,0)$	$\varphi(1) = (1,1,1)$	$\varphi(2) = (0,2,2)$	$\varphi(3) = (1,0,3)$	$\varphi(4) = (0,1,4)$
$\varphi(5) = (1,2,0)$	$\varphi(6) = (0,0,1)$	$\varphi(7) = (1,1,2)$	$\varphi(8) = (0,2,3)$	$\varphi(9) = (1,0,4)$
$\varphi(10) = (0,1,0)$	$\varphi(11) = (1,2,1)$	$\varphi(12) = (0,0,2)$	$\varphi(13) = (1,1,3)$	$\varphi(14) = (0,2,4)$
$\varphi(15) = (1,0,0)$	$\varphi(16) = (0,1,1)$	$\varphi(17) = (1,2,2)$	$\varphi(18) = (0,0,3)$	$\varphi(19) = (1,1,4)$
$\varphi(20) = (0,2,0)$	$\varphi(21) = (1,0,1)$	$\varphi(22) = (0,1,2)$	$\varphi(23) = (1,2,3)$	$\varphi(24) = (0,0,4)$
$\varphi(25) = (1,1,0)$	$\varphi(26) = (0,2,1)$	$\varphi(27) = (1,0,2)$	$\varphi(28) = (0,1,3)$	$\varphi(29) = (1,2,4)$

On voit bien que l'on a obtenu une bijection, mais de plus on peut vérifier que φ est un morphisme, par exemple :

$$\begin{aligned} \varphi(5) + \varphi(7) &= (1,2,0) + (1,1,2) = (0,0,2) = \varphi(12) \\ \varphi(3) \times \varphi(4) &= (1,0,3) \times (0,1,4) = (0,0,2) = \varphi(12)\,. \end{aligned}$$

On voit qu'on peut étudier les éléments de $\mathbb{Z}/30\mathbb{Z}$ en regardant les triplets de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. L'intérêt essentiel est que les facteurs de droite sont des corps, donc on voit par exemple qu'un élément de $\mathbb{Z}/30\mathbb{Z}$ est inversible si et seulement s'il correspond à un triplet formé de trois éléments non nuls. Prenons 23, qui correspond à $(1,2,3)$; il est donc inversible et son inverse correspond à$(1^{-1}, 2^{-1}, 3^{-1}) = (1,2,2)$(car $2 \times 2 \equiv 1 (\mathrm{mod}\, 3)$ et $2 \times 3 \equiv 1 (\mathrm{mod}\, 5)$), et donc l'inverse de 23 est 17.

Nous allons généraliser ce théorème dans un anneau $\mathbb{A}$ commutatif. Soient I, J deux idéaux de $\mathbb{A}$ et soit $x \in \mathbb{A}$. on rappelle que la classe de x dans $\mathbb{A}/IJ$ est égale à $x + IJ$, comme $IJ \subset I$ on voit que $x + IJ \subset x + I$. Donc si deux éléments x et y sont égaux modulo IJ,alors ils sont égaux modulo I (respectivement modulo J)donc on peut définir une application de $\mathbb{A}/IJ$ dans A/I (respectivement A/J) qui à $x + IJ$ associe $x + i$ (respectivement $x + j$).

Noter que, dans le cas de $\mathbb{Z}/n\mathbb{Z}$ avec $n = n_1 \times n_2 \times ... \times n_k$, ces application de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n_i\mathbb{Z}$ sont celles qui composent l'isomorphisme du théorème des restes chinois.

Lemme 3.3.2 *Dans $(\mathbb{A}, +, \cdot)$un anneau commutatif, si un idéal I est comaximal avec des idéaux $I_1, I_2, I_3, ...I_k$, alors il est comaximal avec leur produit.*

Proposition 3.3.3 *Soit $(\mathbb{A}, +, \cdot)$ un anneau commutatif et soient I_1, I_2, ..., I_k des idéaux deux à deux comaximaux. On a :*

$$I_1 I_2 ... I_k = I_1 \cap I_2 ... \cap I_k.$$

Théorème 3.3.4 *(Théorème des restes chinois)*

Soit $(\mathbb{A}, +, \cdot)$ un anneau commutatif et soient I_1, I_2, ..., I_k des idéaux deux à deux comaximaux. Notons $P = I_1 I_2 ... \ I_k$ l'application

$$\begin{aligned} \varphi : \mathbb{A}/P &\rightarrow \mathbb{A}/I_1 \times \mathbb{A}/I_2 \times ... \times \mathbb{A}/I_k \\ x + P &\rightarrow (x + I_1, x + I_2, ...x + I_k). \end{aligned}$$

est un isomorphisme d'anneaux.

Preuve. La définition des anneaux quotients induit que φ est un morphisme d'anneaux. Il suffit de montrer que φ est bijectif. Tout d'abord montrons que φ est injectif.

Soient x, $y \in \mathbb{A}$ tels que $\varphi\ (x + p) = \varphi\,(y + p)$. Alors $\forall 1 \leq i \leq k$, $x - y \in I_i$ donc $x - y \in I_1 \cap I_2 ... \cap I_k$. où $I_1 \cap I_2 ... \cap I_k = I_1 I_2 ... I_k$ d'après la proposition 3.3.3. donc $x - y \in P$ et donc $x + P = y + P$.

Montrons maintenant que φ est surjectif. Soient x_1, x_2, ..., $x_k \in \mathbb{A}$ il suffit de montrer qu'il existe $x \in \mathbb{A}$ tel que, pour tout $\forall 1 \leq i \leq k$ on ait $x - x_i \in I_i$ En effet, $x + P$ est alors un antécédent de $(x + I_1, x + I_2, ...x + I_k)$. Fixons un entier r compris entre 1 et k et notons

$$J_r = \bigcap_{\substack{i=1 \\ i \neq r}}^{k} I_i = \prod_{\substack{i=1 \\ i \neq r}}^{k} I_i$$

Les idéaux I_r et J_r sont comaximaux d'après le lemme 3.3.2. Donc il existe $a_r \in I_r$ et $c_r \in J_r$ tels que $a_r + c_r = 1_{\mathbb{A}}$.

Les éléments $(c_r)_{1 \leq r \leq k}$ vérifient alors :

- $\forall 1 \leq i, r \leq k, i \neq r \implies c_r \in I_i$.
- $\forall 1 \leq r \leq k$, $c_r - 1_{\mathbb{A}} \in I_r$.

Posons

$$x = \sum_{r=1}^{k} c_r x_r.$$

Montrons que x est l'élément recherché, c'est-à-dire que pour tout $1 \leq i \leq k$ on a $x - x_i \in I_i$.

$$x - x_i = \sum_{\substack{r=1 \\ r \neq i}}^{k} c_r x_r + (c_i - 1_{\mathbb{A}})\, x_i.$$

Comme pour $i \neq r$, $c_r \in I_i$ le terme $\sum\limits_{\substack{r=1 \\ r \neq i}}^{k} c_r x_r$ est un élément de I_i. Par ailleurs $c_i - 1_{\mathbb{A}} \in I_i$ donc $(c_i - 1_{\mathbb{A}})\, x_i \in I_i$. ■

Chapitre 4

Applications de théorèmes des restes chinois

Dans ce chapitre, nous etudions les applications de théorème des restes chinois sure la méthode d'interpolation de Lagrange et la multiplication polynômiale rapide, et nous prouvons le système de cryptogrphie RSA.

4.1 La méthode d'interpolation de Lagrange

Pour la factorisation d'un polynôme à coefficients entiers, nous pouvons supposer que les facteurs ont coefficients entiers. pour la méthode d' interpolation de Lagrange nous utilisons ces informations pour décrire une procédure permettant de tenir compte toute polynôme dans $\mathbb{K}[x]$. la mèthode attribuée à Kronecker, autour de 1883, mais est apparemment dû à l'origine à Schubert (1793) il est basé sur le théorème des restes chinois.

Soit$\{a_1, ..., a_n\}$ et $\{b_1, ..., b_n\}$ deux familles d'éléments du corps $\mathbb{K}$, le problème consiste à trouver un polynôme $L \in \mathbb{K}[x]$ de degré strictement inférieur à n tel que pour tout i, $1 \leq i \leq n$, on ait $L(a_i) = b_i$.

Soient $P \in \mathbb{K}[x]$ et $a \in \mathbb{K}$; effectuons la division euclidienne de P par $x - a$. Il existe deux polynômes Q et R tels que

$$P = Q \times (x - a) + R$$

avec $\deg(R) < \deg(x - a) = 1$. Donc R est un polynôme constant et $P(a) = R$, finalement :

$$P \equiv P(a) \,(\mathrm{mod}\langle x - a\rangle).$$

Notre problème se reformule ainsi, on cherche un polynôme L vérifiant, pour tout i,

$1 \leq i \leq n$, $L \equiv b_i \,(\mathrm{mod}\langle x - a_i\rangle)$. Notons que si $a \neq b$. Alors les idéaux $\langle x-a\rangle$ et $\langle x-b\rangle$ sont comaximaux en effet, on a :

$$\frac{1}{b-a}\left((x-a)-(x-b)\right) = 1_{\mathbb{K}[x]}.$$

Donc $\langle x-a\rangle + \langle x-b\rangle = \mathbb{K}[x]$. Par conséquent, si on applique le théorème des restes chinois dans l'anneau $\mathbb{K}[x]$ aux idéaux $\{\langle x-a_i\rangle\}_{1\leq i\leq n}$ qui sont comaximaux deux à deux, on obtient que le n-uplet$(b_1, ..., b_n)$ de $\mathbb{K}[x]/\langle x-a_1\rangle \times ... \times \mathbb{K}[x]/\langle x-a_n\rangle$ admet un unique antécédent dans $\mathbb{K}[x]/\langle P\rangle$ avec

$$P = \prod_{i=1}^{n}(x-a_i).$$

De cet antécédent il suffit de choisir le représentant de degré inférieur à n et nous obtenons ainsi L de plus, on voit que L est l'unique solution à notre problème, puisque deux polynômes de degré inférieur à n qui sont égaux modulo $\prod_{i=1}^{n}(x-a_i)$ sont égaux.

Reprenons la preuve du théorème des restes chinois. Un antécédent M de $(b_1, ..., b_n)$ est de la forme :

$$M = \sum_{r=1}^{n} c_r b_r.$$

Où c_r est un élément de l'idéal engendré par le polynôme P_r où

$$P_r = \prod_{\substack{i=1\\ i\neq r}}^{n}(x-a_i) = \frac{p}{(x-a_r)}.$$

Vérifiant $c_r \equiv 1\,(\mathrm{mod}\langle x-a_r\rangle)$. Comme $\deg(P) = n-1$, nous allons chercher c_r sous la forme $\alpha_r P_r$ où α_r est un polynôme constant. Mais, par ailleurs, on sait que $c_r \equiv c_r(a_r)\,(\mathrm{mod}\langle x-a_r\rangle)$ donc on doit avoir

$$c_r(a_r) = 1 = \alpha_r P_r(a_r) = \alpha_r \prod_{\substack{i=1\\ i\neq r}}^{n}(a_r - a_i).$$

Ce qui donne :

$$\alpha_r = \frac{1}{\prod_{\substack{i=1\\ i\neq r}}^{n}(a_r - a_i)}.$$

Et finalement :

$$L = \sum_{\substack{r=1\\ i\neq r}}^{n} b_r \prod_{\substack{i=1\\ i\neq r}}^{n}\frac{(x-a_i)}{(a_r-a_i)}.$$

Il est facile de vérifier que l'on a bien $L(a_i) = b_i$ pour tout i, $1 \leq i \leq n$. Ce polynôme L est appelé : polynôme d'interpolation de Lagrange.

4.2 Multiplication polynômiale rapide

La multiplication est l'une des deux opérations algebrique de base sur les polynômes. Mais il n'est pas particulièrement attrayante.

Rappellez vous comment il fonctionne.

Supposer

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$$

et

$$g(x) = b_0 + b_1x + b_2x^2 + ... + b_dx^d$$

Sont deux polynômes de degré d, la méthode standard pour multiplier

$$f(x)g(x) = (a_0 + a_1x + a_2x^2 + ... + a_dx^d) \times (b_0 + b_1x + b_2x^2 + ... + b_dx^d)$$

est à multiplier chaque a_ix^i par chaque b_jx^j et la collection des coefficient de chaque puissance de x pour obtenir :

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + ... + c_{2d}x^{2d}$$

tel que

$$\begin{aligned}
c_0 &= a_0b_0 \\
c_1 &= a_0b_{1+}a_1b_0 \\
c_2 &= a_0b_{2+}a_1b_1 + a_2b_0 \\
&\vdots \\
c_d &= a_0b_{d+}a_1b_{d-1} + ... + a_{d_1}b_1 + a_db_0 \\
c_{d+1} &= a_1b_{d+}a_2b_{d-1} + ... + a_{d_1}b_2 + a_db_1 \\
&\vdots \\
c_{2d} &= a_db_d
\end{aligned}$$

Pour mesurer l'efficacitè de cette mèthode est, on compte le nombre de multiplications numeriques n'ècessaires. un tel compte est facile si f et g les deux ont degré d, alors

les deux ont $d+1$ coefficients, et chaque coefficient de $f(x)$ est multiplié par chaque coefficient de $g(x)$. Ainsi la multiplication de deux pôlynomes de degré d de façon standard nécessite $(d+1)^2$nombre de multiplications est- il un moyen plus efficace de multiplier deux polynômes ? plus précisément, est-il un moyen de multiplier deux polynômes de degré d qui utilise moins de $(d+1)^2$ numéro multiplications ?

La réponce est oui.

Voici les grandes ligne d'une stratégie pour multiplier deux polynômes $f(x)$ et $g(x)$ de degré d à coefficients dans $\mathbb{C}$:

I- Evaluer : choisir $2d+1$ points $a_1, a_2..., a_{2d+1}$ et évaluer $f(x)$ et $g(x)$ à chacune des $2d+1$ points ; qui est trouver $f(a_1), f(a_2), ..., f(a_{2d+1})$ et $g(a_1), g(a_2), ..., g(a_{2d+1})$.

II- Multiplier : multiplier $f(a_i) g(a_i)$ pour tout $i = 1, 2, ..., 2d+1$.

III- Interpoler :trouver un polynôme $h(x)$ de degré ≤ 2 tel que $h(a_i) = f(a_i) g(a_i)$ pour tout $i = 1, 2, ..., 2d+1$

Mais il y a une note de valeur comme aspect de cet strategie, dans (I) nous avons fait $2d+1$ numéro de multiplications, plutôt que les $(d+1)^2$ numéro de multiplications quand on multiple $f(x)$ et $g(x)$ par la méthode standard.

Avant de passé à l'éfficacité des (I) et (III) nous devons rependre à la question plus fondamentale : est ce que $h(x)$ qui sorte en (III) vraiment $f(x) g(x)$? cette question répendu par une propriété de le théorème des restes chinois.

Théorème 4.2.1 *Soient $a_1, a_2..., a_e$ sont des nombres complexes différents et soient $h_1, h_2, ..., h_e$ des nombres complexes, alors il existe un polynôme unique $h(x)$ de degré $< e$ ainsi que $h(a_i) = h_i$ pour tout $i = 1, 2, ..., e$.*

La preuve de ce théorème est une conséquence immédiate de théorème de reste et le théorème des restes chinois. Celui-ci implique que $a_1, a_2..., a_e$ sont tous distincts, alors il existe un unique polynôme $h(x)$ de degré $< e$ pour que

$$h(x) \equiv h_i \pmod{(x - a_i)}.$$

pour tout $i = 1, 2, ...e$

Le théorème du reste implique que pour tout $i = 1, 2, ...e$ et tout polynôme $h(x)$ nous avons :

$$h(x) \equiv h_i \pmod{(x - a_i)}.$$

Ainsi, il existe un unique polynôme $h(x)$de degré $< e$ de sorte que pour tout i, nous avont :

$$h(a_i) \equiv h_i \pmod{(x - a_i)}.$$

Mais puis que $h(a_i)$ et h_i sont tous deux nombres, c'est un polynôme de degré ≤ 0, il s'ensuit que si elles sont congruent modulo $x - a_i$, il doivent être égaux, d'où $h(a_i) = h_i$ pour tout i.

Appliquer (III) de notre stratégie pour multipler deux polynômes $f(x)$ et $g(x)$ de degré d, si nous touvons un polynôme $h(x)$ de degré $2d$ de sorte que $h(a_i) = f(a_i)\, g(a_i)$ pour tout $i = 1, 2, ..., 2d + 1$, puis à partir de $f(x)\, g(x)$ est également un polynôme de degré $\leq 2d$ avec les mêmes valeurs de $a_1, a_2..., a_{2d+1}$que $h(x)$, alors les polynômes $h(x)$ et $f(x)\, g(x)$ doivent être égaux. C'est notre stratégie en trois étapes pour trouver $f(x)\, g(x)$ va vraiment travailler.

Exemple 4.2.2 *Soit* $f(x) = x + 1$, $g(x) = x + 2$. *Nous trouvons* $f(x)g(x)$*par notre stratégie en trois étapes.*

Soit $a_1 = 0$, $a_2 = 3$, $a_3 = -1$, *ensuit les étapes (I) et (II) sont :*

$$\begin{aligned} f(a_1) &= 1, g(a_1) = -2 \text{ et donc } f(a_1)\, g(a_1) = -2. \\ f(a_2) &= 4, g(a_2) = 1 \text{ et donc } f(a_2)\, g(a_2) = 4. \\ f(a_3) &= 0, g(a_3) = -3 \text{ et donc } f(a_3)\, g(a_3) = 0. \end{aligned}$$

Pour l'étape (III) nous avons besoin d'interpoler un polynôme $h(x)$ *de degré* < 3 *avec* $h(0) = -2, h(3) = 4$ *et* $h(-1) = 0$, *et pour trouver* $h(x)$ *de degré* ≤ 2 *est d'écrire* $h(x)$ *avec des coefficients inconnus :* $h(x) = rx^2 + sx + t$, *et d'évaluer* $h(x)$ *à* 0, 3 *et* -1 *pour obtenir trois équations pour trouver les coefficients inconnus :*

$$\begin{aligned} h(0) &= -2 = t; \\ h(3) &= 4 = 9r + 3s + t; \\ h(-1) &= 0 = r - s + t. \end{aligned}$$

La résolution de ces équations donne $t = -2$, $r = 1$, $s = -1$, *donc* $h(x) = x^2 - x - 2$.

Définition 4.2.3 *Une racine de l'unité dans un corps* $\mathcal{F}$ *est un élément* w *pour que* $w^f = 1$. *pour certaines* $f > 0$.

Exemple 4.2.4 *:*

1) 1 *et* -1 *des racines de l'unité sur* $\mathbb{R}$.

2) $\alpha = \cos(2\pi/n) + i \sin(2\pi/n)$ *est une racine* n*-ième primitive de l'unité dans* $\mathbb{C}$.*Si* α *est une racine* n*-ième primitive de l'unité, et* $(r, n) = 1$, *alors* α^r *est une racine* n*-ième primitive de l'unité.*

4.3 Le système de cryptographie RSA

Le plus célèbre et le premier des systèmes de cryptographie à clé publique est le système RSA (Ronald Rivest, Adi Shamir et Leonard Adleman). Entre autres, ce système est à la base des méthodes de paiements par Internet.

Théorème 4.3.1 *RSA*

Soit p et q deux nombres premiers distincts et $n = pq$. Si e est un nombre premier à $\varphi(n)$ (tel que $\varphi(n) = card\{a : 0 \leq a \leq n-1$ et $PGCD(a,n) = 1\}$ et si d est son inverse modulo $\varphi(n)$, alors pour tout entier a $(a < n)$, on a :

$$(a^e)^d \equiv \left(a^d\right)^e \equiv a \,(\mathrm{mod}\, n)\,.$$

Preuve. Puisque p et q sont des nombres premiers distincts, on sait que $n = ppcm(p,q)$. Ainsi pour montrer que $a^{de} \equiv a \,(\mathrm{mod}\, pq)$ il suffit de montrer que a^{de} est solution du système chinois suivant :

$$\begin{cases} x \equiv a \,(\mathrm{mod}\, p) \\ x \equiv a \,(\mathrm{mod}\, q) \end{cases}$$

En effet, dans ce cas a^{de} serait solution du système, au même titre que a. Par unicité de la solution modulo pq, on saurait que $a^{de} \equiv a \,(\mathrm{mod}\, pq)$.

On ne va démontrer que $a^{de} \equiv a \,(\mathrm{mod}\, p)$, car pour l'autre, on reprend les mêmes arguments en échangeant les rôles de p et de q.

Par hypothèse, on sait que $de \equiv 1 \,(\mathrm{mod}\, \varphi(n))$. Ainsi, il existe $k \in \mathbb{Z}$ tel que :

$$de = 1 + k\varphi(n) = 1 + k(p-1)(q-1)\,.$$

Donc, comme $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$ grâce au théorème de Fermat, on obtient :

$$a^{de} = a^{1+k(p-1)(q-1)} = a^1\left(a^{k(p-1)(q-1)}\right) = a\left(a^{p-1}\right)^{k(q-1)} \equiv a \times 1 \equiv a \,(\mathrm{mod}\, p)\,.$$

■

Bibliographie

[1] SHEN KANGSHENG. Historical Development of the Chinese Remainder Theorem. Communicated by C. TRUESDEL.Department of Mathematics Hangzshou University(June 1, 1987).

[2] Cours de Dr Kevin Hutchinson School of Mathematical Sciences Dublin Ireland.

[3] Jean Chanzy. Congruence dans $\mathbb{Z}$. Université de Paris-Sud.

[4] Pierre Bornsztein, Xavier Caruso,Pierre Nolin et Mehdi Tibouchi.Cours d'arithmétique Première partie.D´ecembre 2004

[5] Stéphane Perret. Mathématiques Option Spécifique. Version 3.000.

[6] William Stein.Elementary Number Theory : Primes, Congruences, and Secrets. November 16, 2011.

[7] Lars- Ake Lindahl. Lectures on Number Theory. 2002.

[8] François Arnault, Gilles Bailly-Maitre, Yves Benjamin et autres. Mathématiques L3 Algèbre, Cours complet avec 400 tests et exercices corrigés.

[9] Dr. Philippe Chabloz, Prof. Ev a Ba yer Fluckiger. Algèbre pour communications numériques.octobre 2004.

[10] Mehmed Mustafa Akyurek. The Chinese Remainder Theorem for Polynomials and its Applications, MCS 492, Graduation Project II. C ankaya University Department of Mathematics and Computer Science. May 29, 2009.

[11] Frank Ayres JR, traduction française par Michel LOBENBERG. Algèbre moderne cours et problemes, 425 exercices resolus.

[12] Ibrahim Assem, Pierre Yves Leduc. Cours d'algèbre Groupes, anneaux, modules et corps.

[13] A. A. Pantchichkine. Master-1 de mathématiques (MAlg 1), 2004/2005, module MAlg 1 "Algèbre" (Master-1, MAT 401i). Institut Fourier, FRANCE.

Résumer

Le but d'étude le théorème des restes chinois est résoudre des problèmes des congruences. Ce théorème apparait sous forme d'un système d'équation linéaire de congruence. Le théorème a appliqué sur plusieurs domaines et surtout sur la cryptographie.

ملخص

الهدف من دراسة نظرية البواقي الصينية هو حل بعض المشاكل في الموافقات. هذه النظرية تقوم على أساس جملة من المعادلات الخطية في شكل موافقات. تم تطبيق النظرية في العديد من المجالات و بالأخص في التشفير.