UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE

HOUARI BOUMEDIENE - ALGER -

FACULTÉ DE MATHEMATIQUES

THESE

pour l'obtention du Grade de :

Magister en mathématiques

Option : algèbre et théorie des nombres

MOKHFI SIHAM

Séries de Hurwitz et congruences

Soutenue publiquement le : Lundi 16 septembre 2002

Devant le jury composé des messieurs :

K.BETINA	Professeur (USTHB)	Président
B.BENZAGHOU	Professeur (USTHB)	Directeur de thèse
M.ZITOUNI	Professeur (USTHB)	Examinateur
A.KHELLADI	Professeur (USTHB)	Examinateur
A.TADJINE	Chargé de cours (USTHB)	Examinateur

2001 / 2002

Dédicace

Je dédie ma thèse à :

- *Mes chers parents qui m'ont tout donné et qui m'ont constamment encouragé à emprunter la voie du savoir.*
- *Aucun mot ne pourra exprimer tout l'amour et la gratitude que j'ai pour eux.*
- *Mes chers sœurs et frères en lesquels j'ai trouvé un soutien permanent.*
- *Tous mes enseignants qui sans leurs enseignements cette thèse n'aurait pu être.*
- *Toutes mes amies et que tout ceux qui de prés au de loin ont contribué à l'aboutissement de ce travail trouvent ici l'expression de ma profonde reconnaissance.*

Siham

Remerciements

Je tiens à exprimer ma reconnaissance à Mr Benzaghou pour m'avoir guidé et conseillé jusqu'à l'accomplissement de cette étude.

Je remercie Mr Bellina d'avoir accepter de présider le jury d'examination de ce travail.

Je remercie également Mr Zitouni, Mr Khelladi et Mr Tadjine pour l'honneur qu'ils m'ont fait en acceptant de faire part de mon jury.

Je remercie vivement Mr Chabour pour ses précieux conseils.

J'adresse mes vifs remerciements à Lotfi pour son aide généreuse dans l'accomplissement de la frappe de ma thèse.

Table des Matières

Introduction **3**

1 Séries de Hurwitz et composition de suites **5**

1.1 Séries de Hurwitz 5

1.1.1 **.Généralités** 5

1.1.2 **Séries de Hurwitz définies sur l'anneau des entiers rationnels** $\mathbb{Z}$ et p-adique $\mathbb{Z}_p$ 6

1.1.3 **Quelques résultats sur les séries bornées** 21

1.2 **Composition de suites et nombres de Stirling** 28

1.2.1 **Les nombres de Stirling** 31

1.2.2 **Opérateurs de Shift et de dérivation** 32

1.2.3 **Transformation de Mellin-Barsky** 35

2 Généralisation du théorème de Von Staudt -Claussen à des séries de Hurwitz **36**

3 Congruences de Kummer pour les cofficients des séries Hurwitz **54**

3.1 Généralites 51

3.2 Congruence de Kummer pour des séries linéaires spéciales . 62

4 Théorèmes de Barsky **70**

4.1 **Théorème 1** 70

4.2 **Théorème 2** 86

Introduction

Le sujet de notre magister fait partie des domaines de mathématiques pures, il concerne les domaines de l'analyse et de l'algèbre.

Le but de notre étude est de faire une synthèse de quelques résultats sur les séries de Hurwitz d'une part et d'autre part de démontrer par des exemples l'apport d'aisance que procure le calcul ombral dans la preuve de propriétés intéréssantes qui ne sont pas toujours faciles à prouver par d'autre méthodes .

nous avons réparti notre travail en quatre chapitres :

le premier chapitre regroupe toutes les définitions , propriétés générales relatives aux séries de Hurwitz , à l'algèbre de Hurwitz des suites, en particulier les deux suites de nombres de Stirling de $1^{ère}$éspèce et de $2^{ème}$éspèce, et enfin la notion des opérateurs de dérivation et de Shift et la transformation de Mellin -Barsky .

Dans le deuxième chapitre , nous avons énoncé le théorème de Von Staudt - Claussen qui concerne la suite des nombres de Bernoulli , puis avons démontré un théorème le généralisant : c'est le théorème de Carlitz .

Dans le troisième chapitre , nous avons éssayé de reformuler les énoncés des théorèmes cités dans le travail de Carlitz cf[8] et de les prouver autrement en faisant intervenir le calcul ombral, aprés avons démontré des congruences de Kummer pour des séries linéaires.

le quatrième chapitre est consacré à la redémonstration de deux théorèmes de Barsky [4]

Chapitre 1

Séries de Hurwitz et composition de suites

Ce chapitre est une synthèse des principaux résultats concernant les séries de Hurwitz

1.1 Séries de Hurwitz

1.1.1 .Généralités

Soit A un anneau commutatif unitaire de caractéristique zéro

Définition1

une série de Hurwitz sur un anneau A est une série formelle de la forme

$f(X) = \sum_{m \geq 0} c_m \frac{X^m}{m!}$ où $c_m \in A$ pour tout entier m positif

l'ensemble des séries de Hurwitz définies sur A est noté $H(A)$

Définition2

Soit $f(X) = \sum_{m \geq 0} c_m \frac{X^m}{m!}$ une série non nulle de $H(A)$

L' ordre de $f(X)$ est le plus petit entier m tel que $c_m \neq 0$

Définition3

Soient f, g deux séries de Hurwitz de $H(A)$.

f, g sont dites associées s'il existe un élément inversible h de $H(A)$

tel que $f = h.g$.

1.1.2 Séries de Hurwitz définies sur l'anneau des entiers rationnels $\mathbb{Z}$ et p-adique $\mathbb{Z}_p$

Soient $f(X) = \sum_{m \geq 0} c_m \frac{X^m}{m!}$ et $g(x) = \sum_{m \geq 0} b_m \frac{X^m}{m!}$ deux séries de hurwitz

ces deux séries sont dites congrues à un entier naturel k si, tous les coéfficients c_m et b_m le sont

Proposition1

Soient f, g deux séries de $H(\mathbb{Z})$ $(resp. H(\mathbb{Z}_p))$ alors

$$f + g \in H(A) \;\; ; \;\; f.g \in H(A)$$

si $g(0) \in \mathbb{Z}^*(resp.\mathbb{Z}_p^*)$ alors

$$\frac{f}{g} \in H(A)$$

si $f(0) = 0$ alors

$$\frac{f^m}{m!} \in H(A)$$

et si $g(0) = 0$ alors

$$f(g) \in H(A)$$

Preuve:cf [11]

Définition4

Une série $f(X)$ de $H(\mathbb{Z})\,(resp.H(\mathbb{Z}_p))$ est dite linéaire si $c_0 = 0$,

$c_1 = 1\ (resp.c_1 \in \mathbb{Z}_p^*)$.

notons $H_1(\mathbb{Z})(resp.H_1(\mathbb{Z}_p)$ l'ensemble des séries de Hurwitz linéaires sur $\mathbb{Z}(resp.\mathbb{Z}_p)$

Définition5

Une série $f(X) = \sum\limits_{m\geq 0} c_m \frac{X^m}{m!}$ à coéfficients rationnels($c_m \in \mathbb{Q}$) est dite bornée dans $H(\mathbb{Z})$ s'il existe un entier k telque $k.f(X) \in H(\mathbb{Z})$

Définition6

Une série $f(X) = \sum\limits_{m\geq 0} c_m \frac{X^m}{m!}$ à coéfficients rationnels p-adiques ($c_m \in \mathbb{Q}_p$)est dite bornée, s'il existe un entier k telque $p^k.f(X) \in H(\mathbb{Z}_p)$

Proposition2

Les ensembles des séries de Hurwitz $H(\mathbb{Z})$ et $H(\mathbb{Z}_p)$ satisfont l'inclusion

$$H(\mathbb{Z}) \subset H(\mathbb{Z}_p)$$

Définition7

La série de Hurwitz $f(X)=\sum\limits_{m\geq r} c_m \dfrac{X^m}{m!}$ d'ordre r est dite réduite si les coéfficients c_m satisfont les inégalités $0<c_m<\binom{m}{r}c_r$

Théorème1

Deux séries de Hurwitz réduites et associées sont identiques.

Preuve:cf.[6]

Théorème2

Une série de $H(\mathbb{Z})$ d'ordre r est l'associée d'une unique série réduite.

Preuve:

Soit $f(X)=\sum\limits_{m\geq r} c_m \dfrac{X^m}{m!}$ une série d'ordre r

supposons que $f(X)$ est associée à deux séries réduites différentes

$g(X)=\sum\limits_{m\geq r} a_m \dfrac{X^m}{m!}$ et $\phi(X)=\sum\limits_{m\geq r} b_m \dfrac{X^m}{m!}$

telles que $\left\{\begin{array}{c} f(X)=h(X).g(X) \quad (1) \\ \\ et \\ \\ f(X)=h'(X).\phi(x) \quad (2) \end{array}\right.$ où $\left(\begin{array}{c} h(X)\in H(\mathbb{Z})^* \\ \\ \text{et} \\ \\ h'(X)\in H(\mathbb{Z})^* \end{array}\right)$

de (1) et (2) on déduit que $\dfrac{h(X)}{h'(X)}.g(x)=\phi(x)$

comme $h'(X)\in H^*(\mathbb{Z})$, alors $\dfrac{1}{h'(X)}\in H(\mathbb{Z})^*$

et ainsi $\dfrac{h(X)}{h'(X)}.\in H(\mathbb{Z})^*$ d'où $g(X)$ et $\phi(X)$ sont associées et réduites en même temps alors d'aprés le théorème 1.2.8 on doit avoir $g(X)=\phi(X)$.$\square$

Corollaire1

l'ensemble des séries de hurwitz $H(\mathbb{Z})$ possède une infinité de séries non associées d'ordre r

Preuve:

d'aprés la définition 6, il existe une infinité de séries réduites d'ordre r

donc d'aprés le théorème 1, elles ne peuvent être associées.$\square$

Corollaire2

Soit $f(X) = \sum_{m \geqslant 1} \frac{X^m}{m!}$ et $g(x) = \sum_{m \geqslant 0} \frac{X^{km+1}}{(km+1)!}, k \in \mathbb{N}$, alors $\frac{f(X)}{g(X)} \notin H(\mathbb{Z})$

Preuve:

Raisonnons par l'absurde

Soit l'hypothèse $\frac{f}{g} \in H(\mathbb{Z})$ (1)

la donnée $\frac{f}{g}(0) = 1$ (car f, g sont linéaires) (2)

(1) et (2) impliquent $\frac{f(X)}{g(X)} = h(X) \in H(\mathbb{Z})^*$,

c'est à dire $f(X)$ et $g(X)$ sont associées dans $H(\mathbb{Z})$,

or $f(X)$ est une série réduite car elle vérifie :

$$0 < a_m = 1 < \binom{m}{1} a_1 = m \qquad \text{pour tout entier } m$$

$g(X)$ est aussi réduite car ses coefficients b_m :

$$b_m = \begin{cases} 0 \text{ si } m \neq k\alpha + 1 \\ \\ 1 \text{ si } m = k\alpha + 1 \end{cases} \quad \forall \alpha \in \mathbb{N}$$

satisfont

$$0 \leq b_m < \binom{m}{1} b_1 = m$$

d'où $f(X)$ et $g(X)$ sont réduites et associées en même temps.

le théorème1 implique qu'elles sont identiques.contradiction.

Il en résulte la relation $\dfrac{f}{g} \notin H(\mathbb{Z})$ □

Proposition3

Il existe des séries de Hurwitz qui ne sont pas associées dans $H(\mathbb{Z})$ mais qui sont associées dans $H(\mathbb{Z}_p)$, pour un certain nombre premier p

Exemple

Les séries X et $\sum\limits_{m>0} \dfrac{X^{2m+1}}{(2m+1)!}$ ne sont pas associées dans $H(\mathbb{Z})$ mais sont associées dans $H(\mathbb{Z}_2)$

en effet

X et $\sum\limits_{m\geqslant 0} \dfrac{X^{2m+1}}{(2m+1)!}$ ne sont pas associées dans $H(\mathbb{Z})$ sinon cela implique

$$\frac{\sum\limits_{m\geqslant 0} \frac{X^{2m+1}}{(2m+1)!}}{X} = \sum_{m\geqslant 0} \frac{X^{2m}}{(2m+1)!} \in H^*(\mathbb{Z})$$

or $\sum\limits_{m\geqslant 0} \dfrac{X^{2m}}{(2m+1)!} = \sum\limits_{m\geqslant 0} \dfrac{X^{2m}}{(2m+1)(2m)!} \notin H(\mathbb{Z})$ car $\dfrac{1}{2m+1} \notin \mathbb{Z}\ \forall m \geqslant 1$

D'autre part , on a : $\sum\limits_{m\geqslant 0} \dfrac{X^{2m}}{(2m+1)(2m)!} \in H(\mathbb{Z}_2)$ car $\dfrac{1}{2m+1} \in \mathbb{Z}_2\ \forall m$

donc X et $\sum\limits_{m\geqslant 0} \dfrac{X^{2m+1}}{(2m+1)!}$ sont associées dans $H(\mathbb{Z}_2)$ $\square$

Définition8

Soit $f(X)$ une série linéaire de $H(\mathbb{Z})$ ou $H(\mathbb{Z}_p)$

on dit que la série $\lambda(X)$ est la réciproque de $f(X)$ si la composée $f(\lambda(X))$ est égale à X

Théorème3

Toute série linéaire de $H(\mathbb{Z})$ $(resp. H(\mathbb{Z}_p))$ admet une réciproque qui elle aussi est linéaire de $H(\mathbb{Z})$ $(resp. H(\mathbb{Z}_p))$

Preuve:

Soit $Y = f(X) = \sum\limits_{m\geq 1} c_m \dfrac{X^m}{m!}$ une série linéaire de $H(\mathbb{Z})$;

notons sa réciproque $\lambda(X) = \sum\limits_{m\geq 1} c_m \dfrac{X^m}{m!}$ et prouvons que les $c_m \in \mathbb{Z}$

on a $\lambda(f(X)) = \lambda(Y) = \sum\limits_{m\geq 1} c_m \dfrac{Y^m}{m!} = X$

on déduit que $c_m = \dfrac{d^m X}{dY^m}(0)$

utilisons la propriété suivante pour déterminer les $c_m = \dfrac{d^m X}{dY^m}(0) \qquad (\forall m \geqslant 1)$

Proposition4

$$\left(\frac{d^m X}{dY^m}\right)\left(\frac{dY}{dX}\right)^{2m-1} \text{ est un polynôme en } \frac{dY}{dX}, \dots, \frac{d^m Y}{dX^m} \text{ à coéfficients entiers}$$

Preuve:

$Y = f(X)$ implique que $\lambda(Y) = X$ (1)

(1) implique que $\lambda'(Y)\dfrac{dY}{dX} = \dfrac{dX}{dX}$ d'où $\lambda'(Y)\dfrac{dY}{dX} = 1$ (2)

(2) implique $X'(Y) = \dfrac{1}{\dfrac{dY}{dX}} = \dfrac{1}{f'(X)}$

Vérifions la relation de récurrence

Vérifions la relation de récurrence pour $m = 2$

calculons $\left(\dfrac{d^2X}{dY^2}\right)\left(\dfrac{dY}{dX}\right)^3$:

$$\text{on a } \frac{d^2X}{dY^2} = \frac{d}{dY}\left(\frac{dX}{dY}\right) = \frac{d}{dY}\left(\frac{1}{\dfrac{dY}{dX}}\right) = \frac{-\dfrac{d\left(\dfrac{dY}{dX}\right)}{dY}}{\left(\dfrac{dY}{dX}\right)^2} = \frac{-1}{\left(\dfrac{dY}{dX}\right)^2}.\frac{d\left(\dfrac{dY}{dX}\right)}{dX}.\frac{dX}{dY}$$

$$\text{c'est à dire} \frac{d^2X}{dY^2} = \frac{-1}{\left(\dfrac{dY}{dX}\right)^3}\left(\frac{d^2Y}{dX^2}\right)$$

$$\text{d'où } \left(\frac{d^2X}{dY^2}\right)\left(\frac{dY}{dX}\right)^3 = \frac{-d^2Y}{dX^2}$$

Supposons que la propriété suivante est vraie pour l'ordre m

$$\frac{d^mX}{dY^m} = \frac{1}{\left(\dfrac{dY}{dX}\right)^{2m-1}} P\left(\frac{dY}{dX}, \frac{d^2Y}{dX^2}, \ldots\ldots, \frac{d^mY}{dX^m}\right);$$

.

calculons l'ordre suivant

$$\frac{d^{m+1}X}{dY^{m+1}}=\frac{d}{dY}\left(\frac{P\left(\dfrac{dY}{dX},\ldots\ldots,\dfrac{d^mY}{dX^m}\right)}{\left(\dfrac{dY}{dX}\right)^{2m-1}}\right)$$

$$=\frac{d}{dX}\left(\frac{P\left(\dfrac{dY}{dX},\ldots\ldots,\dfrac{d^mY}{dX^m}\right)}{\left(\dfrac{dY}{dX}\right)^{2m-1}}\right)\frac{dX}{dY}$$

$$=\frac{\dfrac{1}{\dfrac{dY}{dX}}\left(\dfrac{d}{dX}P\left(\dfrac{dY}{dX},..,\dfrac{d^mY}{dX^m}\right)\left(\dfrac{dY}{dX}\right)^{2m-1}\right)}{\left(\dfrac{dY}{dX}\right)^{4m-2}}-$$

$$\frac{\dfrac{1}{\dfrac{dY}{dX}}\left(\left(\dfrac{dY}{dX}\right)^{2m-2}(2m-1)\dfrac{d^2Y}{dX^2}P\left(\dfrac{dY}{dX};..,\dfrac{d^mY}{dX^m}\right)\right)}{\left(\dfrac{dY}{dX}\right)^{4m-2}}$$

$$=\frac{\hat{P}\left(\dfrac{dY}{dX},\ldots\ldots,\dfrac{d^{m+1}Y}{dX^{m+1}}\right)}{\left(\dfrac{dY}{dX}\right)^{4m-2+1-2m+1}}-\frac{(2m-1)\,P\left(\dfrac{dY}{dX},\ldots\ldots,\dfrac{d^mY}{dX^m}\right)\dfrac{d^2Y}{dX^2}}{\left(\dfrac{dY}{dX}\right)^{4m-2+1-2m+2}}\ ;$$

où $\hat{P}$ est un polynôme en $\frac{dY}{dX},...,\frac{d^{m+1}Y}{dX^{m+1}}$

$$= \frac{1}{\left(\frac{dY}{dX}\right)^{2m+1}} \left(\frac{dY}{dX}\right) \hat{P}\left(\frac{dY}{dX},.....,\frac{d^{m+1}Y}{dX^{m+1}}\right) - (2m-1) P\left(\frac{dY}{dX},.....,\frac{d^{m}Y}{dX^{m}}\right)\frac{d^2Y}{dX^2}$$

d'où le résultat.

Maintenant revenons à la preuve du théorème

comme $c_m = \frac{d^m X}{dY^m}(0)$,

alors la propriété précédente implique que

$$c_m = \frac{1}{\left(\frac{dY}{dX}(0)\right)^{2m-1}} P\left(\frac{dY}{dX}(0),...,\frac{d^mY}{dX^m}(0)\right)$$

comme $\frac{dY}{dX}(0) = 1$ alors $c_m = P(c_1,.....,c_m) \in \mathbb{Z}$; pour tout $m > 0$ $\square$

La preuve se fait similairement pour le cas p-adique.

Proposition5

L'ensemble des séries de Hurwitz linéaires $H_1(\mathbb{Z})$ $(resp.H_1(\mathbb{Z}_p))$ muni de la loi composition est un groupe

preuve:

1] la compositon est associative

2] X est l'elément neutre de H_1

3] $\forall f(X) \in H_1(\mathbb{Z})$ $(resp.H_1(\mathbb{Z}_p))$, $\exists g(X) \in H_1(\mathbb{Z})$ $(resp.H_1(\mathbb{Z}_p))$tel que $fog(X) = X$, il suffit de prendre $g(X)$ la série réciproque de $f(X)$ qui selon le théorème1.2.14 est dans $H_1(\mathbb{Z})$ $(resp.H_1(\mathbb{Z}_p))$ $\square$

Définiton9

Soient $f(X), g(X)$ deux séries de $H(\mathbb{Z})\,(resp.H(\mathbb{Z}_p))$

On dit qu'elles sont équivalentes si et seulement il existe une série

$\lambda(X) \in H_1(\mathbb{Z})\ (resp.H_1(\mathbb{Z}_p))$ tel que $f(\lambda(X)) = g(X)$

Proposition6

Toute série linéaire est équivalente à X

preuve:

Soit $f(X) \in H_1(\mathbb{Z})\,(resp.H_1(\mathbb{Z}_p))$

Cherchons une série $g(X) \in H_1(\mathbb{Z})\,(resp.H_1(\mathbb{Z}_p))$ tel que $g(f(X)) = X$

il suffit de prendre $g(X)$ égale à la réciproque de $f(X)$

Corollaire1

Toutes les séries de $H_1(\mathbb{Z})\,(resp.H_1(\mathbb{Z}_p))$sont équivlentes deux à deux

.preuve:

Soient $f(X), g(X) \in H_1(\mathbb{Z})\,(resp.H_1(\mathbb{Z}_p))$

$f(X)$ et $g(X)$sont équivalentes signifie qu'il existe une série $h(X) \in H_1(\mathbb{Z})$

(resp.$H_1(\mathbb{Z}_p)$)telle que $g(h(X)) = f(X)$

Il suffit de prendre $h(X) = g^{-1}(f(X))$ où g^{-1}désigne la réciproque de g.

Théorème4

La réciproque $\lambda(X)$ de $f(X) = \sum\limits_{m>0} c_m \dfrac{X^{km+1}}{(km+1)!} \in H(\mathbb{Z})$ où $c_0 = 1$

est de la forme $\lambda(X) = \sum\limits_{m>0} c_m \dfrac{X^{km+1}}{(km+1)!}$

.preuve:

Pour prouver ce théorème on fait appel à la proposition suivante

Proposition

Soit m un entier positif ; et soit θ une racine primitive $m^{i\grave{e}me}$de l'unité

et soit $f(X)$ une série de $H(\mathbb{Z})$, alors on a

$$\left(f(X)=\sum_{t\geqslant 0}a_t\frac{X^{tm+1}}{(tm+1)!}\right)\Longleftrightarrow\left(\ f(\theta X)=\theta f(X)\ \right)$$

.preuve de la proposition

1] Prouvons que $f(\theta X)=\theta f(X)$

$$\begin{aligned}f(\theta X)&=\sum_{t\geqslant 0}a_t\frac{\theta^{tm+1}X^{tm+1}}{(tm+1)!}\\&=\sum_{t\geqslant 0}a_t\frac{\theta X^{tm+1}}{(tm+1)!}\qquad\qquad \text{car } \theta^{tm+1}=\theta\\&=\theta f(X)\end{aligned}$$

2] Soit $f(X)=\sum_{\alpha\geqslant 0}a_\alpha\frac{X^\alpha}{\alpha!}$ tel que$f(\theta X)=\theta f(X)$ prouvons que $f(X)$ est de la forme $f(X)=\sum_{\alpha\geqslant 0}a_\alpha\frac{X^{\alpha m+1}}{(\alpha m+1)!}$

On a $f(\theta X)-\theta f(X)=\sum_{\alpha\geqslant 0}a_\alpha\left(\theta^\alpha-\theta\right)\frac{X^\alpha}{\alpha!}=\sum_{\alpha\geqslant 0}a_\alpha\left(\theta^{\alpha-1}-1\right)\theta\frac{X^\alpha}{\alpha!}=0$

on déduit alors que $a_\alpha\left(\theta^{\alpha-1}-1\right)\theta=0$ et ce $\forall\alpha\geqslant 0$

mais $f(X)$ n'est pas une série nulle , donc a_α ne peut être nul pour tout α

et aussi $\theta\neq 0$ par hypothèse ,

on déduit alors que $\theta^{\alpha-1}=1$;d'où $\alpha-1=tm$ (où $t\in N$) puisque θ est une racine $m^{i\grave{e}me}$de l'unité

d'où $f(X)=\sum_{t\geqslant 0}a_t\frac{X^{tm+1}}{(tm+1)!}$ $\square$

Maintenant revenons à la preuve du théorème d'aprés la proposition du dessus, prouver que $\lambda(X)$ est de la forme

$\lambda(X) = \sum\limits_{m\geqslant 0} c_m \dfrac{X^{km+1}}{(km+1)!}$ revient à prouver que$\lambda(\theta X) = \theta\lambda(X)$,

en particulier pour la variable $Y = f(X)$

désignons par φ l'application : $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]$

$$X \longmapsto X\theta$$

on alors $fo\varphi = \theta f = \varphi of$

d'où $\lambda ofo\varphi = \lambda o\varphi of = \varphi$

i.e $\lambda o\varphi ofo\lambda = \varphi o\lambda$

i.e $\lambda o\varphi = \varphi o\lambda$

d'où $\lambda(X)$ est de la forme $\sum\limits_{m\geqslant 0} c_m \dfrac{X^{km+1}}{(km+1)!}$ $\square$

Théorème5

Soient $\Phi(X), \Psi(X)$ deux séries équivalentes à coefficients rationnels et soient p un nombre premier et k un entier, alors on a

$$p^k\Phi(X) \in H(\mathbb{Z}_p) \Longleftrightarrow p^k\Psi(X) \in H(\mathbb{Z}_p)$$

autrement dit

$$\Phi(X) \text{ est bornée} \Longleftrightarrow \Psi(X) \text{ est bornée}$$

Preuve

Dire que $\Phi(X), \Psi(X)$sont équivalentes dans $H(\mathbb{Z}_p)$ implique l'existence d'une série$\lambda(X) \in H_1(\mathbb{Z}_p)$ tel que $\Phi(\lambda(X)) = \Psi(X)$

D'autre part $\Phi(X)$ est bornée implique l'existence d'un entier k positif tel que $p^k\Phi(X) \in H(\mathbb{Z}_p)$

vérifions que $p^k\Psi(X) \in H(\mathbb{Z}_p)$:

$p^k\Psi(X) = p^k\Phi(\lambda(X)) = p^k \sum\limits_{m\geqslant 0} a_m \dfrac{(\lambda(X))^m}{m!}$; où $\Phi(X) = \sum\limits_{m\geqslant 0} a_m \dfrac{X^m}{m!}$

comme $p^k\Phi(X) \in H(\mathbb{Z}_p)$, on a alors $p^k a_m \in \mathbb{Z}_p$ $\forall m$ et comme

$\dfrac{(\lambda(X))^m}{m!} \in H(\mathbb{Z}_p)$ $\forall m$

on déduit alors que $p^k\Psi(X) \in H(\mathbb{Z}_p)$ d'où le résultat $\square$

Théorème6

soient $\Phi(X)$, $\Psi(X)$ deux séries équivalentes à coéfficients rationnels

alors on a

$$k\Phi(X) \in H(\mathbb{Z}) \Longleftrightarrow k\Psi(X) \in H(\mathbb{Z})$$

Preuve:

Similaire à la preuve du théorème précédent.

Théorème7

Soit $f(X)$une série de $H_1(\mathbb{Z})$ (resp.$H_1(\mathbb{Z}_p)$).on a :

$$\frac{f(X)}{X} \in H(\mathbb{Z})\,(\text{resp.}H(\mathbb{Z}_p)) \Longleftrightarrow \frac{X}{f(X)} \in H(\mathbb{Z})\,(\text{resp.}H(\mathbb{Z}_p))$$

Preuve:

1] Soit $f(X) = X + \sum\limits_{m\geqslant 2} c_m \dfrac{X^m}{m!}$

De l'ecriture$\dfrac{f(X)}{X} = \dfrac{X + \sum_{m\geqslant 2} c_m \dfrac{X^m}{m!}}{X} = 1 + \sum_{m\geqslant 2} \dfrac{c_m}{m} \dfrac{X^{m-1}}{(m-1)!}$

on remarque que$\dfrac{f(X)}{X}(0) = 1$

d'où tenant compte de l'hypothèse$\dfrac{f(X)}{X} \in H(\mathbb{Z})$ on déduit que$\dfrac{f(X)}{X} \in H^*(\mathbb{Z})$

et donc$\dfrac{X}{f(X)} \in H^*(\mathbb{Z})$,d'où $\dfrac{X}{f(X)} \in H(\mathbb{Z})$.

2] La preuve de la réciproque sera maintenant évidente □

Théorème8

Soit $f(X)$ une série de $H_1(\mathbb{Z})$ (resp.$H_1(\mathbb{Z}_p)$)et soit $\lambda(X)$ sa réciproque alors

$$\frac{X}{f(X)} \in H(\mathbb{Z})\,(\text{resp.} H(\mathbb{Z}_p)) \Longleftrightarrow \frac{X}{\lambda(X)} \in H(\mathbb{Z})\,(\text{resp.} H(\mathbb{Z}_p))$$

Preuve:

1] Posons $Y = \lambda(X)$

comme $\dfrac{X}{f(X)} \in H(\mathbb{Z})$ et$Y = \lambda(X) \in H(\mathbb{Z})$; alors leur composée est aussi dans $H(\mathbb{Z})$, d'où $\dfrac{Y}{f(Y)} \in H(\mathbb{Z})$

Or $\dfrac{Y}{f(Y)} \in H(\mathbb{Z}) \Longleftrightarrow \dfrac{f(Y)}{Y} \in H(\mathbb{Z})$ (et ce d'aprés le théorème 1.2.21)

mais $\dfrac{f(Y)}{Y} = \dfrac{X}{\lambda(X)}$; d'où $\dfrac{X}{\lambda(X)} \in H(\mathbb{Z})$

2] la preuve de la réciproque sera maintenant évidente.□

Pour $H(\mathbb{Z}_p)$ la preuve se fait de la même manière.

Théorème9

Soit $f(X) = \sum\limits_{m\geqslant 1} c_m \dfrac{X^m}{m!}$ une série de $H_1(\mathbb{Z})$ (resp.$H_1(\mathbb{Z}_p)$) ,

soit $\lambda(X) = \sum\limits_{m\geqslant 1} e_m \dfrac{X^m}{m!}$ sa réciproque

On a alors $\dfrac{c_m}{m} \in \mathbb{Z} \Longleftrightarrow \dfrac{e_m}{m} \in \mathbb{Z}$

Preuve:

$$\frac{X}{f(X)} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \Longleftrightarrow \frac{X}{\lambda(X)} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \qquad (1)\ ;$$

(voir thm5)

$$\frac{X}{f(X)} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \Longleftrightarrow \frac{f(X)}{X} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \qquad (2)\ ;$$

(voir thm7)

$$\frac{X}{\lambda(X)} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \Longleftrightarrow \frac{\lambda(X)}{X} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \qquad (3)\ ;$$

(voir thm7)

en combinant les relations (1) ; (2) ; (3) on obtient

$$:\frac{f(X)}{X} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \Longleftrightarrow \frac{\lambda(X)}{X} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p))$$

c'est à dire

$$\sum_{m\geqslant 1} \frac{c_m}{m} \frac{X^{m-1}}{(m-1)!} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p)) \Longleftrightarrow \sum_{m\geq 1} \frac{e_m}{m} \frac{X^{m-1}}{(m-1)!} \in H(\mathbb{Z})\,(\text{resp}.H(\mathbb{Z}_p))$$

et donc $\dfrac{c_m}{m} \in \mathbb{Z} \Longleftrightarrow \dfrac{e_m}{m} \in \mathbb{Z}$ $\square$

Théorème10

Soit $f(X)$ une série de $H_1(\mathbb{Z})$ (resp.$H_1(\mathbb{Z}_p)$), on a

$\dfrac{X}{f(X)}$ bornée $\Longleftrightarrow \dfrac{\lambda(X)}{X}$ bornée

Preuve:

Si on prouve que $\dfrac{X}{f(X)}$ et $\dfrac{\lambda(X)}{X}$ sont équivalentes, alors le thm.1.2.21 implique le résultat recherché

On a $\frac{X}{f(X)}(\lambda(X)) = \frac{\lambda(X)}{X}$;

d'où effectivement $\frac{X}{f(X)}$ et $\frac{\lambda(X)}{X}$ sont équivalentes $\square$

Proposition7

Soient $f(X)$ et $g(X)$ deux séries de $H_1(\mathbb{Z})$, alors

-

$$\frac{f(X)}{g(X)} \in H(\mathbb{Z}) \Longleftrightarrow \frac{g(X)}{f(X)} \in H(\mathbb{Z})$$

Preuve:

$\frac{f(X)}{g(X)} \in H(\mathbb{Z})$ tel que $\frac{f}{g}(0) = 1$ alors $\frac{f}{g} \in H^*(\mathbb{Z})$

d'où $\frac{g}{f} \in H^*(\mathbb{Z}) \subset H(\mathbb{Z})$ $\square$

Proposition8

Soient $f(X) \in H_1(\mathbb{Z})$ et $\lambda(X)$ sa réciproque

soit $g(X)$une série de$H(\mathbb{Z})$

$g(X) \backslash f(X) \Longleftrightarrow X \backslash g(\lambda(X))$

Preuve:

$g(X) \backslash f(X) \Longleftrightarrow \frac{f(X)}{g(X)} \in H(\mathbb{Z}) \Longleftrightarrow \frac{g(X)}{f(X)} \in H(\mathbb{Z})$, (voir propo1.2.26)

d'où $\frac{g(\lambda(X))}{f(\lambda(X))} \in H(\mathbb{Z})$ c'est à dire $\frac{g(\lambda(X))}{X} \in H(\mathbb{Z})$

donc $X \backslash g(\lambda(X))$ $\square$

1.1.3 Quelques résultats sur les séries bornées

Proposition8 :L'inverse d'une série bornée n'est pas toujours bornée

Exemple1

Pour tout nombre premier ,on a

1] $\Phi(X) = \dfrac{X}{e^X - 1}$ est bornée dans $H_1(\mathbb{Z}_p)$ mais ;

2] $\dfrac{1}{\Phi(X)} = \dfrac{e^X - 1}{X}$ n'est pas bornée dans $H_1(\mathbb{Z}_p)$

Preuve:

1]$\Phi(X) = \dfrac{X}{e^X - 1} = \sum\limits_{m>1} B_m \dfrac{X^m}{m!}$ où B_m désigne le m^{ieme} nombre de Bernoulli

qui vérifie

$$B_m = \begin{cases} a_{2\alpha} - \sum\limits_{p-1\backslash 2\alpha} \dfrac{1}{p} & \text{si } m = 2\alpha \\ 0 & \text{si } \quad m = 2\alpha + 1 \end{cases} \qquad (\alpha \in \mathbb{N},\ a_{2\alpha} \in \mathbb{Z})$$

grâce au théorème *de* Von staudt Claussen [10]

On constate qu'en multipliant $\Phi(X)$ par p^2 les coefficients de $p^2\ \Phi(X)$

i.e $p^2 B_m$sont des entiers p- adiques , autrement dit $p^2\ \Phi(X)$ est une série de

$H(\mathbb{Z}_p)$ et doncd'aprés le thm1.2.21 $\Phi(X)$ serait bornée quel que soit p premier

.

2]raisonnons par l' absurde ;

supposons que $\dfrac{1}{\Phi(X)}$ est bornée i.e il existe $k \in \mathbb{N}$ tel que $p^k \dfrac{1}{\Phi(X)} \in H(\mathbb{Z}_p)$.

or $p^k \dfrac{1}{\Phi(X)} = p^k \dfrac{e^X - 1}{X} = p^k \sum\limits_{m\geq 1} \dfrac{1}{m} \dfrac{X^{m-1}}{(m-1)!}$

et $p^k \dfrac{1}{\Phi(X)} \in H(\mathbb{Z}_p)$ implique $\dfrac{p^k}{m} \in Z_p, \forall m \geqslant 1$;

ce qui n'est pas vrai car si $m = p^{k+2}$, $\dfrac{p^k}{m} = \dfrac{1}{p^{2n}} \notin Z_p$; contradiction .

d'où$\dfrac{1}{\Phi(X)}$ n'est pas bornée dans $H(\mathbb{Z}_p)$,pour tout nombre p premier.

Exemple2

Par contre l'inverse d'une série unité est toujours bornée .

Proposition9

La racine $\mathrm{p}^{\text{ième}}$ d'une unité de $H(\mathbb{Z})$ (resp.$H(\mathbb{Z}_p)$) n'est pas toujours bornée .

Exemple1

Soit p un nombre premier de Z

Soit $f(X) = 1 - X$ une unité de $H(\mathbb{Z}_p)$

On a $(f(X))^{1/p}$n'est pas bornée dans $H(\mathbb{Z}_p)$

En effet

$(f(X))^{1/p} = (1-X)^{1/p} = \sum\limits_{m\geq 0} \frac{1}{p}\left(\frac{1}{p}-1\right)\ldots\left(\frac{1}{p}-m+1\right)(-1)^m \frac{X^m}{m!}$

Supposons que $(1-X)^{1/p}$est bornée dans $H(\mathbb{Z}_p)$ i.e $\exists k \in \mathbb{N}$

tel que $p^k(1-X)^{1/p} \in H(\mathbb{Z}_p)$

i.e $\quad p^k\frac{1}{p}\left(\frac{1}{p}-1\right)\left(\frac{1}{p}-2\right)\ldots\ldots\left(\frac{1}{p}-m+1\right) \in Z_p$et ce $\forall\, m \in \mathbb{N}$.

or si $m = k$ la valeur $p^k\frac{1}{p}\left(\frac{1}{p}-1\right)..\left(\frac{1}{p}-k+1\right)$ n'est pas bornée

car $v_p\left(p^k\frac{1}{p}\left(\frac{1}{p}-1\right)\ldots\ldots\left(\frac{1}{p}-k+1\right)\right) = v_p\left(p^k\right) - v_p\left(p^{k+1}\right) = k-k-1$
$= -1 < 0$

contradiction.

On déduit alors que $(1-X)^{1/p}$ n'est pas bornée.

Exemple2

Soit p un nombre premier

La série $f(X) = 1 - \dfrac{X^{2p-1}}{p}$ est une unité de $H(\mathbb{Z}_p)$

et $(f(X))^{1/p}$est bornée dans $H(\mathbb{Z}_p)$

Preuve

soit $f(X) = (1 - \dfrac{X^{2p-1}}{p})^{\frac{1}{p}}$

$$= \sum_{j=0}^{+\infty} \binom{\frac{1}{p}}{j} (-1)^j (\frac{X^{2p-1}}{p})^j$$

$$= \sum_{j=0}^{+\infty} \frac{1.(1-p)....(1-pj+p)}{p^{2j} j!} .(2p-1)j!.(-1)^j \frac{X^{(2p-1)j}}{(2p-1)j!}$$

$f(X)$ bornée dans $H(\mathbb{Z}_p) \Longleftrightarrow \exists k$ tq $p^k \dfrac{1.(1-p)....(1-pj+p)}{p^{2j} j!}$ $(2p-1)j! \in \mathbb{Z}_p$

i.e $v_p(\frac{1.(1-p)....(1-pj+p)}{p^{2j}j!}(2p-1)j!.)$ est bornée inférieurement

or $v_p(\frac{1.(1-p)....(1-pj+p)}{p^{2j}j!}(2p-1)j!.) = v_p(\frac{(2p-1)j!}{j!}) - 2j$

$$v_p(\frac{(2p-1)j!}{j!}) = ((j+1)...2j)(2j+1...2j+j)....((2p-2)j+1)...(2p-2)j+j))$$

le membre droit de cette égalité est un produit de $(2p-2)j$ termes qui se suivent

donc $v_p(\frac{(2p-1)j!}{j!}) = \left[\frac{(2p-2)j}{p}\right] + \left[\frac{(2p-2)j}{p^2}\right] + \left[\frac{(2p-2)j}{p^3}\right] + ..$ $\qquad (*)$

<u>$1^{er}cas$</u> : $j = p^l$, $l \in \mathbb{N}$

$$\begin{aligned}
v_p(\frac{(2p-1)j!}{j!}) &= v_p(\frac{(2p-1)p^l}{p^l!}) \\
&= \left[\frac{(2p-2)p^l}{p}\right] + \left[\frac{(2p-2)p^l}{p^2}\right] + ... \left[\frac{(2p-2)p^l}{p^{l+1}}\right] + ... \quad \text{(d'aprés } (*)\text{)} \\
&= (2p-2)p^{l-1} + (2p-2)p^{l-2} + ... + 2p - 2 + \left[\frac{(2p-2)}{p}\right] \\
&= 2p^l - 2 + 1 = 2p^l - 1
\end{aligned}$$

alors $v_p(\frac{(2p-1)j!}{j!}) - 2j = 2p^l - 1 - 2p^l = -1$

donc dans ce cas la série est bornée

<u>$2^{ème}cas$</u> : $j = kp^l$, $l \in \mathbb{N}$, $1 \leq k \leq p-1$

$$v_p(\frac{(2p-1)j!}{j!}) = v_p(\frac{(2p-1)kp^l!}{(kp^l)!})$$

$$= \left[\tfrac{(2p-2)kp^l}{p}\right] + \left[\tfrac{(2p-2)kp^l}{p^2}\right] + \dots \left[\tfrac{(2p-2)kp^l}{p^{l+1}}\right] + \dots$$

$$= 2kp^l - 2kp^{l-1} + 2kp^{l-1} - 2kp^{l-2} + \dots. + 2pk - 2k + \left[2k - \tfrac{2k}{p}\right] + \left[\tfrac{2k}{p} - \tfrac{2k}{p^2}\right] + ..$$

$$\geq 2kp^l - 2k + 2k - \tfrac{2k}{p} - 1 \geq 2j - 3 \qquad \text{car } \left[\tfrac{2k}{p} - \tfrac{2k}{p}\right] = 0$$

$$= 2kp^l - 2kp^{l-1} + 2kp^{l-1} - 2kp^{l-2} + \dots. + 2pk - 2k + \left[2k - \tfrac{2k}{p}\right] + \left[\tfrac{2k}{p} - \tfrac{2k}{p^2}\right] + \dots$$

.alors $v_p(\dfrac{(2p-1)j!}{j!}) - 2j \geq -3$

et donc la série est bornée

$\underline{3^{ème}cas}$: $j = kp^l + \alpha \quad \alpha, l \in \mathbb{N}$, $0 \leq k \leq p-1$

$$v_p(\frac{(2p-1)j!}{j!}) = \left[\tfrac{(2p-2)(kp^l+\alpha)}{p}\right] + \left[\tfrac{(2p-2)(kp^l+\alpha)}{p^2}\right] + \dots \left[\tfrac{(2p-2)(kp^l+\alpha)}{p^{l+1}}\right] + \dots$$

$$= \left[2kp^l - 2kp^{l-1} + 2\alpha - \tfrac{2\alpha}{p}\right] + \left[2kp^{l-1} + \tfrac{2\alpha}{p} - 2kp^{l-2} - \tfrac{2\alpha}{p^2}\right] + .. \left[2k + \tfrac{2\alpha}{p^l} - \tfrac{2k}{p} - \tfrac{2\alpha}{p^{l+1}}\right]$$

dans le premier terme de la somme du membre droit ci-dessus

$\left[2kp^{l}-2kp^{l-1}+2\alpha-\frac{2\alpha}{p}\right]$ on a $\dfrac{-2\alpha}{p}>\dfrac{-2(p-1)}{p}>-2$

d'où $\left[2kp^{l}-2kp^{l-1}+2\alpha-\frac{2\alpha}{p}\right]>\left[2kp^{l}-2kp^{l-1}+2\alpha-2\right]=2kp^{l}-2kp^{l-1}-2$

et dans le deuxième terme $\left[2kp^{l-1}+\frac{2\alpha}{p}-2kp^{l-2}-\frac{2\alpha}{p^2}\right]=\left[2kp^{l-1}-2kp^{l-2}+\frac{2\alpha}{p}-\frac{2\alpha}{p^2}\right]$

on a $\dfrac{2\alpha}{p}>\dfrac{2\alpha}{p^2}>0$

d'où $\left[2kp^{l-1}-2kp^{l-2}+\frac{2\alpha}{p}-\frac{2\alpha}{p^2}\right]>\left[2kp^{l-1}-2kp^{l-2}\right]=2kp^{l-1}-2kp^{l-2}$

et dans le dernier terme on a

$\left[2k+\frac{2\alpha}{p^l}-\frac{2k}{p}-\frac{2\alpha}{p^{l+1}}\right]>2k-\dfrac{2k}{p}>2k-2$ car $1\leq k\leq p-1$

d'où $v_p(\dfrac{(2p-1)kp^l!}{(kp^l)!})>2kp^{l}-2kp^{l-1}-2+2kp^{l-1}-2kp^{l-2}+...2k-2$

i.e $v_p(\dfrac{(2p-1)kp^l!}{(kp^l)!}>2(kp^l+\alpha)-4$ et donc la série est bornée.□

Proposition10

Soient $f(X), g(X)$ deux séries de $H(\mathbb{Z})$ (*resp.* $H(\mathbb{Z}_p)$)d'ordre supérieur

ou égale à 1 alors on a

$$\frac{f(X)}{g(X)} \text{ est bornée dans} H(\mathbb{Z})\,(resp. H(\mathbb{Z}_p)) \;\Rightarrow \exists k \text{ tq } \frac{f^{k+1}(X)}{g(X)}\in H(\mathbb{Z})\,(resp. H(\mathbb{Z}_p))$$

Preuve

$\dfrac{f(X)}{g(X)}$ est bornée $\Longleftrightarrow \exists\alpha\in\mathbb{Z}($ *resp.*$\mathbb{Z}_p)$tel que $\alpha\dfrac{f(X)}{g(X)}\in H(\mathbb{Z})\,(resp. H(\mathbb{Z}_p))$

Soit $k>\alpha$; $\dfrac{f^{k+1}(X)}{g(X)}\in H(\mathbb{Z})\,(resp. H(\mathbb{Z}_p))$

En effet $\dfrac{f^{k+1}(X)}{g(X)}=\left(\dfrac{f^k(X)}{k!}\right)\times\left(\dfrac{k!f(X)}{g(X)}\right)$

On a $\frac{f^k(X)}{k!} \in H(\mathbb{Z})$ $(resp. H(\mathbb{Z}_p))$ d'aprés la proposition 1.1.4

$k!$ est un multiple de α alors $k!\frac{f(X)}{g(X)} \in H(\mathbb{Z})$ (ou$H(\mathbb{Z}_p)$) ; d'où le résultat $\square$

1.2 Composition de suites et nombres de Stirling

considérons les notations suivantes

*/ C =Corps commutatif de caractéristique zero

*/ $Z(C) = \{u : \mathbb{Z} \to C\}$

*/ $Suppu = \{n \in \mathbb{Z}; u(n) \neq 0\}$

*/ $Ordu = \inf Suppu$

*/ $Degu = \sup Suppu$

*/ $S(C) = \{u \in Z(C), Ordu > -\infty\}$

*/ $S_0(C) = \{u \in Z(C), Ordu > 0\}$

*/ $\gamma(.)$ =factorielle de Roman où $\gamma(n) = \begin{cases} n! & \text{si } n \geq 0 \\ \frac{(-1)^{-n-1}}{(-n-1)!} & \text{sinon} \end{cases}$

*/ $f_k = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{sinon} \end{cases}$; $f_k \in Z(C)$

Définition9

La série génératrice exponentielle $g_u(X)$ associée à la suite $u \in S(C)$ est définie par $g_u(X) = \sum_{n\in\mathbb{Z}} u(n)\frac{X^n}{\gamma(n)}$

Remarquons que lorsque $u \in S_0(C)$, $g_u(X)$ n'est que la série de Hurwitz $\sum\limits_{n\geq 0} u(n)\dfrac{X^n}{n!}$

Définition10

Le produit de Hurwitz de deux suites u, v de $S(C)$ noté $u\Psi v$ est la suite associée au produit des deux séries g_u et.g_v

et on écrit $g_{u\Psi v} = g_u \cdot g_v$

Proposition11

$$u\Psi v(n) = \sum_{i+j=n} \frac{\gamma(n)}{\gamma(i)\gamma(j)} u(j)\, v(n-j)$$

Proposition12

$(S(C), +, \Psi)$ est un corps appelé corps de Hurwitz associé à C

Preuve :[5]

Définition11

Soient $u \in S_0(C)$ tel que $ordu \geqslant 1$ et $v \in S_0(C)$

La composition des deux suites u et v notée vou est la suite associée à la composée des deux séries g_u et g_v ie à la série $g_v o g_u$ et on écrit $g_{vou} = g_v o g_u$

Propriété1

$$ord(uov) = ordu.ordv$$

Preuve :

$$ord(g_v o g_u) = ordg_v.ordg_u = ordv.ordu$$

Propriété2

$$f_k o u = \frac{u^{\Psi k}}{k!}$$

Preuve :

$$g_{f_k o u} = g_{f_k} o g_u = g_{f_k}(g_u) = \frac{\Psi^k g_u}{k!} = \frac{g_{u^{\Psi k}}}{k!}$$

Définition 12

Les $B_{n,k}(u)$ polynomes exponentiels partiels de Bell associés à u sont définis par

$$\frac{g_u^k(X)}{k!} = \sum_{n \geq k} B_{n,k}(u) \frac{X^n}{n!}$$

Proposition13

$$vou(n) = \sum_{k=1}^{n} v(k) B_{n,k}(u)$$

Preuve :[5]

Soit$\Omega_1(C) = \{u \in S(C) \text{ tel que } ordu = 1\}$

Proposition14

$(\Omega_1(C), o)$ est un groupe dont l'élement neutre est f_1

Notons $\bar{u}$ l'inverse de u dans $(\Omega_1(C), o)$

Corollaire

$$\text{Soit } Y = g_u(X) \text{ alors } X = g_{\bar{u}}(Y)$$

donnons des exemples sur des suites et leurs inverses

Exemple1

Soit a la suite associée à la série $e^X - 1 = \sum_{n\geq 1} \frac{X^n}{n!}$ notée $g_a(X)$

i.e $a(n) = \begin{cases} 0 & \text{si } n = 0 \\ 1 & \text{si } n \geq 1 \end{cases}$

d'où $\overline{a}$ est définie par

$\overline{a}(n) = \begin{cases} 0 & \text{si } n = 0 \\ (-1)^{n-1}(n-1)! & \text{si } n \geq 1 \end{cases}$

Exemple2

Soit α la suite associée à la série$1 - e^{-X} = \sum_{n\geq 1} (-1)^{n-1} \frac{X^n}{n!}$ notée $g_\alpha(X)$

i.e $\alpha(n) = \begin{cases} 0 & \text{si } n = 0 \\ (-1)^{n-1} & \text{si} n \geq 1 \end{cases}$

$\bar{\alpha}$ est définie par

$\bar{\alpha}(n) = \begin{cases} 0 & \text{si } n = 0 \\ (n-1)! & \text{si } n \geq 1 \end{cases}$

Définition-notation 13

pour $\alpha \in C^*$,notons α^q la suite définie par $\alpha^q(n) = \alpha^n$

et pour $\alpha = 0$, $\alpha^q = f_0$

Proposition15

$g_{\alpha^q ou} = \exp(\alpha g_u(X))$

1.2.1 Les nombres de Stirling

Définition14

Les nombres de Stirling de 2$^{\text{ème}}$ éspèce sont définis par

$$S(n,k) = B_{n,k}(a) = \frac{a^{\Psi k}}{k!}(n)$$

Définition15

Les nombres de Stirling de $1^{\text{ère}}$ éspèce sont définis par

$$s(n,k) = B_{n,k}(\overline{a}) = \frac{\overline{a}^{\Psi k}}{k!}(n)$$

1.2.2 Opérateurs de Shift et de dérivation

Définition16

L'opérateur shift T est défini sur $S_0(C)$ par

$$Tu(n) = u(n+1) \qquad \forall n \geqslant 0$$

Définition17

L'opérateur de dérivation q est défini sur $S_0(C)$ par

$$qu(n) = nu(n) \qquad \forall n \geqslant 0$$

Proposition16

$$\begin{aligned} g_{Tu}(X) &= \frac{d}{dX} g_u(X) \\ g_{qu}(X) &= \frac{Xd}{dX} g_u(X) \end{aligned}$$

Propietés des nombres de Stirling:

Proposition17

$$S(n+1,k) = S(n,k-1) + kS(n,k)$$

Preuve:

$TS(q,k) = Tf_k oa$

$$\begin{aligned}
&= [(Tf_k)oa]\,\Psi Ta \\
&= (f_{k-1}oa)\Psi Ta \\
&= \frac{a^{\Psi(k-1)}}{(k-1)!}\Psi 1^q \\
&= k\frac{a^{\Psi(k-1)}}{k!}\Psi(f_0 + a) \\
&= k\frac{a^{\Psi(k-1)}}{k!}\Psi f_0 + k\frac{a^{\Psi(k-1)}\Psi a}{k!} \\
&= \frac{a^{\Psi(k-1)}}{(k-1)!} + k\frac{a^{\Psi k}}{k!} \\
&= S(q,k-1) + kS(q,k) \quad \square
\end{aligned}$$

Proposition 18

$$t^n = \sum_{k=1}^{n} S(n,k)\, t(t-1)\ldots(t-n+1)$$

$$t\,(t-1)\,....\,(t-n+1)=\sum_{k=1}^{n}s\,(n,k)\,t^{k}$$

Preuve:

d"aprés la proposition 15 on a

$g_{t^q o\bar{a}}=\exp(t\log(1+X))=(1+X)^{t}=\sum\limits_{n>0}\binom{t}{n}X^{n}=\sum\limits_{n>0}t(t-1)....(t-n+1)\frac{x^{n}}{n!}$

notons $(t)_q(n)=(t)_n=t(t-1)....(t-n+1)$

alors $t^q o\bar{a}=(t)_q(n)$ i.e $t^q=(t)_q oa$

ie $t^q(n)=(t)_q oa(n)=\sum\limits_{k=0}^{n}t(t-1)....(t-k+1)S(n,k)$

de la même relation on déduit aussi

$(t)_q(n)=t^q o\bar{a}(n)=\sum\limits_{k=0}^{n}t^{k}s(n,k)$

Définition -Propriètè18

$$S\,(n,k)=\sum_{j=1}^{n}\frac{(-1)^{k-j}}{j!\,(k-j)!}j^{n}$$

Proposition 19

$$(T^{p}-T)\,S\,(q,k)=S\,(q,k-p)\bmod p$$

Preuve:

$S\,(q+1,k)=S\,(q,k-1)+kS\,(q,k)$

$(T-k)S\,(q,k)=S\,(q,k-1)$

$(T-k)(T-(k-1))...(T-(k-j))S\,(q,k)=S\,(q,k-j)$

$(T-k)(T-(k-1))...(T-(k-p+1)) = T^p - T + p\varphi_k(T)$

la réduction modulo $p \Longrightarrow (T^p - T)S(q,k) \equiv S(q,k-p) \operatorname{mod} p\mathbb{Z}$ $\square$

1.2.3 Transformation de Mellin-Barsky

Définition 19

L'application qui associe la suite u à la suite$\widetilde{u}$ définie par la série

$g_{\widetilde{u}}(X) = g_{uo\widetilde{\alpha}}(X)$

$$u \longrightarrow \widetilde{u}$$

est appelée la tranformation de Mellin-Barsky

cette transformation doit son nom à Mellin et à Barsky .

En effet chacun l'a utilisé mais differemment.

nous ferons appel à cette transformation dans la proposition 2 du chapitre3

Chapitre 2

Généralisation du théorème de Von Staudt -Claussen à des séries de Hurwitz

Dans ce chapitre nous allons généraliser le théorème de Von Staudt -Claussen qui traite les coéfficients de la série de Hurwitz $g_a(X)$,à une certaine classe de séries de Hurwitz linéaires

Le théorème deVON- STAUDT-CLAUSSEN

$$\text{Soit } \frac{x}{g_a(x)} = \frac{x}{e^x - 1} = \sum_{m>0} B_m \frac{x^m}{m!}, \text{ on a alors}$$

$$B_m = \begin{cases} a_{2\alpha} - \sum_{p-1\backslash 2\alpha} \frac{1}{p} & si \quad m = 2\alpha \quad (a_{2\alpha} \in \mathbb{Z}) \\ 0 & si \quad m = 2\alpha + 1 \end{cases} \qquad (\alpha \in \mathbb{N})$$

Théorème1

Soit u une suite de $\Omega_1(\mathbb{Z})$ telle que $u(1) = 1$ et $\overline{u}(m) = \epsilon_m (m-1)!$ où $\epsilon_m \in Z$

alors on a

$B_{n,p-1}(u) \equiv 0 \bmod p$ *pour* $n \in \mathbb{N}$ tq $n \nmid p-1$

$B_{n,p-1}(u) \equiv (-1)^{\alpha-1}\overline{u}^{\alpha-1}(p) \bmod p$ *pour* $n = \alpha(p-1)$ tq $\alpha \in \mathbb{N}$

Preuve :

$n = p-1$; $B_{p-1,p-1}(u) = 1 \equiv 1 \bmod p$

$p \leq n \leq 2p-3$; prouvons par récurrence que $B_{n,p-1}(u) \equiv 0 \bmod p$

lorsque $n = p$;calculons $B_{p,p-1}(u)$

$g_u^p(x) \equiv 0 \bmod p$ i.e $g_u^{p-1}(x).g_u(x) \equiv 0 \bmod p$

$$\sum_{m \geq p-1} (p-1)!\ B_{m,p-1}(u)\frac{x^m}{m!}\Psi \sum_{m \geq 1} u(m)\frac{x^m}{m!} \equiv 0 \bmod pZ_p[[x]]$$

$$\sum_{i=1}^{j} \binom{j}{i} u(i)(p-1)!\ B_{j-i,p-1}(u) \equiv 0 \bmod p$$

remplaçons avec $j = p+1$

$$\binom{p+1}{1}u(1)\ B_{p,p-1}(u) + \binom{p+1}{2}u(2)\ B_{p-1,p-1}(u) \equiv 0 \bmod p$$

$\binom{p+1}{2} \equiv 0 \bmod p$ implique $(p+1)B_{p,p-1}(u) \equiv 0 \bmod p$ i.e $B_{p,p-1}(u) \equiv 0 \bmod p$

supposons que $B_{n,p-1}(u) \equiv 0 \bmod p$ $\forall\, n \in \mathbb{N}$ tq $p+1 \leq n \leq 2p-4$ et prouvons

qu'elle reste vraie pour $n = 2p-3$

maintenant ,remplaçons avec $j = 2p-2$

$$\binom{2p-2}{1}u(1)\ B_{2p-3,p-1}(u) + \binom{2p-2}{p-1}u(2)\ B_{2p-2,p-1}(u) \equiv 0 \bmod p \qquad (1)$$

$(\binom{2p-2}{p-1} \equiv 0 \bmod p)$ et $(1) \Longrightarrow \binom{2p-2}{1}B_{2p-3,p-1}(u) \equiv 0 \bmod p$

$B_{2p-3,p-1}(u) \equiv 0 \bmod p$ □

$n = 2p-2$

posons $j = 2p-1$

$$\binom{2p-1}{1}u(1)\,B_{2p-2,p-1}(u) + \binom{2p-1}{p}u(p)\,B_{p-1,p-1}(u) \equiv 0 \bmod p \qquad (2)$$

$\binom{2p-1}{1} \equiv -1 \bmod p$ et $B_{p-1,p-1}(u) \equiv 1 \bmod p$

alors (2) devient $-B_{2p-2,p-1}(u) + u(p) \equiv 0 \bmod p$ i.e $B_{2p-2,p-1}(u) \equiv u(p) \bmod p$

$*n \geq 2p-1$

c'est ici que vont intervenir les hypothèses du théorème

$$x = g_u(x) o g_{\overline{u}}(x) = \sum_{m\geq 1} \overline{u}(m)\frac{g_u^m(x)}{m!} \equiv \sum_{m\geq 1}^{p} \epsilon_m \frac{g_u^m(x)}{m} \bmod pZ_p\,[[x]]$$

i.e $x \equiv \sum_{m\geq 1}^{p} \epsilon_m \frac{g_u^m(x)}{m} \bmod pZ_p\,[[x]]$

en dérivant les deux membres de la congruence ,on obtient

$$1 \equiv \sum_{m\geq 1}^{p} \epsilon_m g_u^{m-1}(x)\frac{d}{dx}g_u(x) \bmod pZ_p\,[[x]] \text{ donc}$$

$$\frac{1}{\frac{d}{dx}g_u(x)} \equiv \sum_{m\geq 1}^{p} \epsilon_m g_u^{m-1}(x) \bmod pZ_p\,[[x]]$$

i.e $\frac{d}{dx}g_u(x) \equiv \frac{1}{1+\epsilon_2 g_u(x) + \ldots + \epsilon_p g_u^{p-1}(x)} \bmod pZ_p\,[[x]]$

i.e $\frac{d}{dx}g_u(x) \equiv \sum_{m\geq 1}^{p} \eta_m g_u^{m-1}(x) \bmod pZ_p\,[[x]] \quad (\eta_m \in Z)$ (3)

remarquons que $D(g_u^{p-1}(x)) \equiv -g_u^{p-2}(x)\frac{d}{dx}g_u(x) \bmod pZ_p\,[[x]]$

ça (3) implique $D(g_u^{p-1}(x)) \equiv -g_u^{p-2}(x) \sum_{m\geq 1}^{p} \eta_m g_u^{m-1}(x) \bmod pZ_p\,[[x]]$

i.e $D(g_u^{p-1}(x)) \equiv -\eta_1 g_u^{p-2}(x) - \eta_2 g_u^{p-1}(x) \bmod pZ_p\,[[x]]$

alors $D^2(g_u^{p-1}(x)) \equiv a_0 g_u^{p-3}(x) + a_1 g_u^{p-2}(x) + a_2 g_u^{p-1}(x) \bmod pZ_p\,[[x]]$

en continuant ainsi la dérivation de $(g_u^{p-1}(x))$, on obtient :

$$D^{p-1}(g_u^{p-1}(x)) \equiv A_0 + A_1 g_u(x) + \ldots + A_{p-1} g_u^{p-1}(x) \bmod pZ_p\,[[x]] \quad (4)$$

d'autre part on a

$$D^{p-1}(g_u^{p-1}(x)) = D^{p-1}\Big(\sum_{m\geq p-1} (p-1)!B_{m,p-1}(u)\frac{x^m}{m!}$$

$$= \sum_{m > p-1} (p-1)!\ B_{m,p-1}(u) \frac{x^{m-(p-1)}}{(m-(p-1))!}$$
$$= \sum_{\alpha \geq 0} (p-1)!\ B_{\alpha+p-1,p-1}(u) \frac{x^{\alpha}}{\alpha!} \quad \text{où} \quad \alpha = m-(p-1)$$

et en considérant (4) on aura :

$$\sum_{\alpha \geq 0} (p-1)!\ B_{\alpha+p-1,p-1}(u) \frac{x^{\alpha}}{\alpha!} \equiv A_0 + A_1 g_u(x) + \ldots. + A_{p-1} g_u^{p-1}(x) \operatorname{mod} pZ_p\,[[x]] \quad (5)$$

en comparant les termes constants dans les deux membres de (5) on obtient

$(p-1)!\ B_{p-1,p-1}(u) \equiv A_0 \operatorname{mod} pZ_p$

i.e $\qquad -1 \equiv A_0 \operatorname{mod} pZ_p$

la comparaison des coéfficients de $\frac{x^{\alpha}}{\alpha!}$ $(1 \leq \alpha \leq p-2)$ dans les deux membres de la congruence (5) permet de déterminer de proche en proche les A_m, on aura

alors $(p-1)!\ B_{p,p-1}(u) \equiv A_1 \operatorname{mod} pZ_p$

et que $(p-1)!\ B_{\alpha+p-1,p-1}(u) \equiv A_{\alpha} \operatorname{mod} pZ_p$

mais sachant que $B_{\alpha,p-1}(u) \equiv 0 \operatorname{mod} pZ_p$; $p \leq \alpha \leq 2p-1$

on déduit alors $A_m \equiv 0 \operatorname{mod} pZ_p$; $1 \leq m \leq p-2$

reste la détermination de A_{p-1}

d'aprés (5), $A_{p-1} \equiv (p-1)!\ B_{2p-2,p-1}(u) \operatorname{mod} pZ_p$

i.e $A_{p-1} \equiv u(p) \operatorname{mod} pZ_p$ i.e $A_{p-1} \equiv u(p) \operatorname{mod}\ pZ_p$

en substituant les valeurs des A_i dans (5) on obtient

$$D^{p-1}(g_u^{p-1}) \equiv -1 + u(p) g_u^{p-1} \operatorname{mod} pZ_p$$

d'où $B_{m+p-1,p-1}(u) \equiv u(p)\ B_{m,p-1}(u) \operatorname{mod} pZ_p \qquad \forall m \geq p-1$

mais puisque $B_{m,p-1}(u) \equiv 0 \operatorname{mod} pZ_p \quad (p \leq m \leq 2p-3)$

alors $B_{m+p-1,p-1}(u) \equiv 0 \operatorname{mod} pZ_p$

en d'autres termes on a $B_{\alpha,p-1}(u) \equiv 0 \mod pZ_p \quad (2p-1 \leq \alpha \leq 3p-4)$

et $B_{3p-3,p-1}(u) \equiv u(p)(u(p) \mod pZ_p$

i.e $B_{3p-3,p-1}(u) \equiv u(p)^2 \mod pZ_p$

de proche en proche , on obtient $B_{m(p-1),p-1}(u) \equiv u(p)^{m-1} \mod pZ_p$

et $B_{m,p-1}(u) \equiv 0 \mod pZ_p$ pour tout m tq m non multiple de p et $m > p-1$

pour retrouver exactement le théoréme , il nous reste la preuve de

$$u(p) \equiv -\bar{u}(p) \mod pZ_p$$

pour cela nous aurons besoin de la preuve de la proposition suivante

Proposition1

Soit $g_u(x) = \sum_{m\geq 1} u(m) \dfrac{x^m}{m!}$ une série linéaire de$H_1(\mathbb{Z})$ alors

$$u(p) \equiv -\bar{u}(p) \mod p$$

Preuve :par récurrence sur n

Notons par $D_0^p\left(g_v^k\right)$ la quantité obtenue aprés dérivation de g_v^k et ce p fois

et ensuite en subtituant x par 0

vérifions que la propriète est vraie lorsque $k=2$

$$\begin{aligned} D_0^p\left(g_u^2\right) &= D_0^p \sum_{n\geq 2} \sum_{j=1}^{n-1} \binom{n}{j} \bar{u}(j)\, \bar{u}(n-j) \frac{X^n}{n!} \\ &= \sum_{n>p} \left(\sum_{j=1}^{n-1} \binom{n}{j} \bar{u}(j)\, \bar{u}(n-j) \right) \frac{X^{n-p}}{(n-p)!} \end{aligned}$$

le coéfficient constant de $D^p\left(g_u^2\right)$est$\sum_{j=1}^{p-1} \binom{p}{j} \bar{u}(j)\, \bar{u}(p-j)$, mais comme $\binom{p}{j} \equiv 0 \mod p$, on obtient $D^p\left(g_{\bar{u}}^2\right) \equiv 0 \mod p$ et donc la propriètè est vraie pour l'ordre $k=2$

Supposons que la propriètè est vraie pour l'ordre k i.e $D_0^p\left(g_{\bar{u}}^k\right) \equiv 0 \mod p$

Prouvons que la propriété est vraie pour l'ordre $k+1$

$$D_0^p\left(g_{\bar{u}}^{k+1}\right) = D_0^p\left(g_{\bar{u}}^k . g_{\bar{u}}\right) \tag{1}$$

développons (1) à l'aide de la formule de Leibnitz

$D_0^p\left(g_{\bar{u}}^k . g_{\bar{u}}\right) = \sum\limits_{\alpha=0}^{p} \binom{p}{\alpha} \left(g_{\bar{u}}\right)^{(\alpha)} \left(g_{\bar{u}}^k\right)^{(p-\alpha)}$

comme $\binom{p}{\alpha} \equiv 0 \bmod p \quad$ pour $1 \leq \alpha \leq p-1$

alors (1) impliquera $D_0^p\left(g_{\bar{u}}^{k+1}\right) = g_{\bar{u}}(0)\ D_0^p\left(g_{\bar{u}}^k\right) + g_{\bar{u}}^k(0)\ D_0^p g_{\bar{u}} \equiv 0 \bmod p$

d'où $D_0^p\left(g_{\bar{u}}^{k+1}\right) \equiv o \bmod p$ donc le résultat est établi $\square$

i.e $D_0^p\left(g_{\bar{u}}^k\right) \equiv 0 \bmod p\ \forall k > 1$

**] Calcul de $D_0^p\left(\frac{1}{p} g_{\bar{u}}^p\right)$

$D_0^p\left(\frac{1}{p} g_{\bar{u}}^p\right) = D_0^{p-1}\left(g_{\bar{u}}^{p-1} \frac{d}{dx} g_{\bar{u}}\right)$

$D_0^{p-1}\left(g_{\bar{u}}^{p-1} \frac{d}{dx} g_{\bar{u}}\right) = \binom{p-1}{0} \frac{d}{dx} g_{\bar{u}}(0)\ D_0^{p-1}\left(g_{\bar{u}}^{p-1}\right) + .. + \binom{p-1}{p-1} g_{\bar{u}}^{p-1}(0)\ D_0^{p-1} \frac{d}{dx} g_{\bar{u}}(0)$

alors

$D_0^{p-1}\left(g_{\bar{u}}^{p-1} . g'_{\bar{u}}\right) \equiv g'_{\bar{u}}(0)\ D_0^{p-1}\left(g_{\bar{u}}^{p-1}\right) \equiv 1\,(p-1)! \equiv -1 \bmod p$

on tire alors

$D_0^p\left(\frac{1}{p} g_{\bar{u}}^p\right) \equiv -1 \bmod p$

*] D'autre part puisque $x = g_u(g_{\bar{u}}(x)) = \sum_{m\geqslant 1} u(m)\dfrac{g_{\bar{u}}^m(x)}{m!}$

on déduit

$$0 = D_0^p(x) = D_0^p \sum_1^\infty u(m)\frac{g_{\bar{u}}^m(x)}{m!} = D_0^p \sum_1^p u(m)\frac{g_{\bar{u}}^m(x)}{m!} + D_0^p \sum_{p+1}^\infty u(m)\frac{g_{\bar{u}}^m(x)}{m!}$$

mais $D_0^p \sum_{p+1}^\infty u(m)\dfrac{g_{\bar{u}}^m(x)}{m!} = u(p+1)\dfrac{g_{\bar{u}}^{p+1}(x)}{(p+1)!} + D_0^p u(p+2)\dfrac{g_{\bar{u}}^{p+2}(x)}{(p+2)!} + \dots\dots\dots$
or $D_0^p \dfrac{g_{\bar{u}}^{p+1}(x)}{(p+1)!} = D_0^p\left((p+1)\,g_{\bar{u}}^{p-1}(x)\,g_{\bar{u}}^{/}(x)\right) = 0$
d'ailleurs $\forall m > p$, $D_0^p g_{\bar{u}}^m(x)$ sera un multiple de $g_{\bar{u}}(x)$ alors en remplacant $x = 0$

et sachant que $g_{\bar{u}}(x)$ est d'ordre1,

alors $\forall m > p$ $D_0^p \dfrac{g_{\bar{u}}^m(x)}{m!} \equiv 0 \bmod p$ d'où

$$0 = D_0^p \sum_1^\infty u(m)\frac{g_{\bar{u}}^m(x)}{m!} \tag{3}$$

en remplaçant (1)et (4) dans (5), on obtient

$$D_0^p g_u(x) + u(p)\, D_0^p\left(\frac{1}{p!} g_{\bar{u}}^p(x)\right) \equiv 0 \bmod p \tag{4}$$

en identifiant les coéfficients des deux membres de la congruence on obtient

$$\bar{u}(p) + u(p) \equiv 0 \bmod p$$

d'où

$$-\bar{u}(p) \equiv +u(p) \bmod p$$

donc

$$u(p) \equiv -\epsilon_p (p-1)! \bmod p$$

c.a.d

$$u(p) \equiv \epsilon_p \bmod p$$

$$\frac{g_u^{p-1}(x)}{(p-1)!} \equiv -\sum_1^{\infty} \epsilon_p^{m-1} \frac{x^{m(p-1)}}{(m(p-1))!} \bmod p$$

et le résultat du théorème 1 est donc obtenu.

Le lemme suivant n'est au départ qu'une application du théorème 1, mais on verra que le cas $p = 2$ donne des résultats qui seront nécessaires pour la démonstration des théorèmes principaux de ce chapitre.

Lemme1

$$\frac{g_u^3(x)}{(3-1)!} \equiv \frac{x^3}{3!} + \epsilon_2 \sum_2^{\infty} \frac{x^{2m+1}}{(2m+1)!} \bmod 2$$

Preuve

D'aprés le théorème 1de ce chapitre, on a $g_u = g_u^{2-1} \equiv -\sum_1^{\infty} \epsilon_2^{m-1} \dfrac{x^m}{m!} \bmod 2$

or $\epsilon_2^{\alpha} \equiv \epsilon_2 \bmod 2 \quad (\forall \alpha \in \mathbb{N} - \{0\})$

donc $g_u(x) \equiv x + \epsilon_2 \sum_2^{\infty} \dfrac{x^m}{m!} \bmod 2 \quad car\ \epsilon_2 \equiv -\epsilon_2 \bmod 2$

étudions les deux cas :1er /$\epsilon_2$impair; 2/^{ème} $\epsilon_2 pair$

1] le cas $\epsilon_2$impair:

$$\begin{aligned} g_u(x) &\equiv x + \sum_2^{\infty} \frac{x^m}{m!} \bmod 2 \\ &\equiv \sum_1^{\infty} \frac{x^m}{m!} \bmod 2 \end{aligned}$$

alors

$$\begin{aligned} g_u^2(x) &\equiv \left(\sum_1^{\infty} \frac{x^m}{m!} \right)^2 \bmod 2 \\ &\equiv \sum_2^{\infty} \left(\sum_{j=1}^{m-1} \binom{m}{j} \right) \frac{x^m}{m!} \bmod 2 \\ &\equiv \sum_2^{\infty} (2^m - 2) \frac{x^m}{m!} \bmod 2 \end{aligned}$$

sachant que $2^m \equiv 0 \bmod 4 \quad \forall m \geq 2$ et que $-2 \equiv 2 \bmod 4$

on déduit alors

$$g_u^2(x) \equiv 2 \sum_2^{\infty} \frac{x^m}{m!} \bmod 4$$

alors on a

$$\frac{g_u^2(x)}{2} \equiv \sum_2^\infty \frac{x^m}{m!} \bmod 2$$
$$\equiv g_u(x) - x \bmod 2$$
$$\equiv g_u(x) + x \bmod 2$$

d'où

$$\frac{g_u^3(x)}{2} \equiv g_u^2(x) + xg_u(x) \bmod 2$$
$$\equiv xg_u(x) \bmod 2 \qquad (\textit{voir} \quad \text{propositon } 1)$$

donc

$$\frac{g_u^3(x)}{2} \equiv x\sum_1^\infty \frac{x^m}{m!} \bmod 2$$
$$\equiv \sum_{m\geq 1}^\infty (m+1)\frac{x^{m+1}}{(m+1)!} \bmod 2$$
$$\equiv \sum_{m\geq 2}^\infty m\frac{x^m}{m!} \bmod 2$$

comme $m \equiv 0 \bmod 2$ si m est pair

et $\quad m \equiv 1 \bmod 2$ si m est impair

on déduit alors

$$\frac{g_u^3(x)}{2} \equiv \sum_1^\infty \frac{x^{2m+1}}{(2m+1)!} \bmod 2 \qquad (1)$$

2] le cas $c_2$pair:

$$\begin{aligned} g_u(x) &\equiv x \bmod 2 \\ \text{d'où } \frac{g_u^3(x)}{2} &\equiv \frac{x^3}{2} \bmod 2 \qquad (2) \end{aligned}$$

maintenant aprés étude de chaque cas à part , assemblons les formules (1) et (2) dans une seule

$$\frac{g_u^3(x)}{2} \equiv \frac{x^3}{2} + \epsilon_2 \sum_1^{\infty} \frac{x^{2m+1}}{(2m+1)!} \bmod 2$$

Théorème2(carlitz)

Soient u une suite de $\Omega_1(\mathbb{Z})$ qui satisfait les hypothèses du théorème 1

Soit $\dfrac{x}{g_u(x)} = \sum_{m=0}^{\infty} v(m) \dfrac{x^m}{m!}$ alors on a:

1] si m pair $\quad v(m) = G_m - \sum_{p-1\backslash m} \dfrac{1}{p} \epsilon_p^{\frac{m}{p-1}}$; $G_m \in \mathbb{Z}$

2] si m impair $\quad v(1) = \dfrac{\epsilon_2}{2}$

$$v(3) = G_3 + \frac{\epsilon_2}{2} + \frac{\epsilon_4}{2}$$

$$v(m) = G_m + \frac{\epsilon_2}{2} + \frac{\epsilon_2\epsilon_4}{2} \qquad \text{(pour tout } m > 3\text{)}, \ G_m \in \mathbb{Z}$$

Preuve:

Comme $x = g_u o g_u(x)$, alors $\dfrac{x}{g_u(x)} = \sum_{m=0}^{\infty} \dfrac{\epsilon_m}{m} g_u^{m-1}(x)$

puisque $g_u^{m-1}(x) \equiv 0 \bmod (m-1)!$ et

$(m-1)! \equiv 0 \bmod m$; (pour tout $m \geq 4$ et non premier) (voir cf[10])

il résulte

$$\frac{x}{g_u(x)} = g_\alpha(x) + \sum_{p-1\backslash m} \frac{\epsilon_p}{p} g_u^{p-1}(x) + \frac{\epsilon_4}{4} g_u^3(x) \text{ avec } g_\alpha(x) \in H(\mathbb{Z}) \qquad (1)$$

utilisons le théorème 1 pour calculer $\frac{\epsilon_p}{p} g_u^{p-1}(x)$,on a alors

$$\frac{\epsilon_p}{p} g_u^{p-1}(x) = -\frac{\epsilon_p}{p} \sum_1^\infty \epsilon_p^{m-1} \frac{x^{m(p-1)}}{(p-1)!} + p \sum_{m\geq 0} F_m^{(p)} \frac{x^m}{m!} \text{ (où } F_m^{(p)} \in \mathbb{Z}) \qquad (2)$$

le remplacement de (2)dans (1)donne

$$\sum_{m=0}^\infty v(m) \frac{x^m}{m!} = g_\alpha(x) + \left(-\sum_{m=0}^\infty \frac{\epsilon_2^m}{2} \frac{x^m}{m!} + 2\sum_{m>1} F_m^{(2)} \frac{x^m}{m!} \right) + \dots\dots\dots\dots + .$$

$$+. \left(-\sum_{m=0}^\infty \frac{\epsilon_p^m}{p} \frac{x^{(p-1)m}}{((p-1)m)!} + p\sum_{m\geq 0} F_m^{(p)} \frac{x^m}{m!} \right) + \dots\dots +$$

$$+\dots + \frac{\epsilon_4}{4} [\frac{x^3}{3!} + \epsilon_2 (\sum_{m=0}^\infty \frac{x^{2m+1}}{(2m+1)!} + 2\sum_{m=0}^\infty l_m \frac{x^m}{m!})] \; (l_m \in \mathbb{Z})$$

en comparant les deux membres de cette égalité , on obtient

si m est pair

$$v(m) = G_m - \sum_{p-1\backslash m} \frac{1}{p} \epsilon_p^{\frac{m}{p-1}}$$

si m est impair

$$\begin{aligned} v(1) &= \frac{-\epsilon_2}{2} = \frac{\epsilon_2}{2} \\ v(3) &= G_3 + \frac{\epsilon_2^3}{2} + \frac{\epsilon_4}{2} \qquad \textit{comme} \quad \epsilon_2^3 = \epsilon_2 \quad \textit{alors } v(3) = G_3 + \frac{\epsilon_2^3}{2} + \frac{\epsilon_4}{2} \\ v(m) &= G_m + \frac{\epsilon_2}{2} + \frac{\epsilon_2\epsilon_4}{2} \qquad \forall \quad m > 3 \; \square \end{aligned}$$

Une application du théorème2

considérons la suite a définie dans l'exemple 1(page31) et déterminons les coéfficients

de la série $\frac{x}{g_a(x)} = \sum_{m\geq 0} B_m \frac{x^m}{m!}$

D'aprés l'exemple la suite $\bar{a}$ vérifie les hypotèses du théorème 2.

tel que $\epsilon_m = (-1)^{m-1}$d'où

$$B_1 = \frac{\epsilon_2}{2} = -\frac{1}{2}$$

si m impair $\qquad B_m = G_m + \frac{-1}{2} + \frac{(-1)(-1)}{2} = G_m \qquad$ i.e

$$B_m = G_m; \text{ où } G_m \text{ est entier}$$

si m pair $\qquad B_m = G_m - \sum_{p-1\backslash m} \frac{1}{p} \epsilon_p^{\frac{m}{p-1}}$ i.e

$$B_m = G_m - \sum_{p-1\backslash m} \frac{1}{p}; \text{ où } G_m \text{ est entier}$$

ça coincide exactement avec le théorème de Von -Staudt-Claussen où les $B_m$sont les nombres de Bernoulli

Théorème 3

Soit u une suite vérifiant les hypothèses du théorème 2 et

supposons que $u(2) = 0$

Définissons δ_m par:

$\frac{x^2}{g_u^2(X)} = 1 + \sum_2^\infty (m-1)\, \delta_m \frac{x^m}{m!}$

alors on a :$\delta_m + v_m$ est entier $\forall m \geq 1$

Preuve:

Posons $\dfrac{x^2}{g_u^2(x)} = \sum_{m>0} \gamma_m \dfrac{x^m}{m!} = 1 + \sum_{m>1} \gamma_m \dfrac{x^m}{m!} \quad (\gamma_0 = 1)$

$u(2) = 0$ implique que:

1] $\epsilon_2 = 0$ car $\epsilon_2 = \bar{u}(2) = -u(2)$ qui est dû à l'identification des coéfficients des deux séries $g_{\bar{u}} o g_u(x)$ et x

2] $\gamma_1 = 0$ car

$$\left(\frac{x}{g_u(x)}\right)^2 = \left(\frac{x}{x + u(2)\frac{x^2}{2!} + ..}\right)^2 = \left(\frac{1}{1 + u(2)\frac{x}{2!}} + ..\right)^2$$

$$= 1 + u(2)\frac{x^2}{2!} - 2u(2)\frac{x^2}{2!} - 2u(3)\frac{x^2}{6}$$

$$= \sum_{m\geq 1} \gamma_m \frac{x^m}{m!} \text{ d'où } \gamma_1 = u(2) = 0$$

Afin d'obtenir le résulat de ce théorème on établira une identité qui relie $\dfrac{x}{g_u(x)}$ et $\dfrac{x^2}{g_u^2(x)}$ en suivant les étapes suivantes:

*] calcul de $x \displaystyle\int_0^x \frac{1}{g_u^2(x)} - \frac{1}{x^2} dx$:

$$\frac{1}{g_u^2(x)} - \frac{1}{x^2} = \frac{x^2 - g_u^2(x)}{x^2 g_u^2(x)} = \frac{x^2}{g_u^2(x)} - \frac{1}{x^2} - \frac{1}{x^2} = \sum_{m\geq 1} \gamma_m \frac{x^{m-2}}{m!} - \frac{1}{x^2}$$

i.e $\dfrac{1}{g_u^2(x)} - \dfrac{1}{x^2} = \left(\dfrac{1}{x^2} + \dfrac{\gamma_2}{2!} + \dfrac{\gamma_3}{3!} X + ...\right) - \dfrac{1}{x^2}$

d'où $x \displaystyle\int_0^x \frac{1}{g_u^2(x)} - \frac{1}{x^2} dx = x \int_0^x \sum_{m\geq 2} \gamma_m \frac{x^{m-2}}{m!} dx = \sum_{m\geq 2} \frac{\gamma_m}{m-1} \frac{x^m}{m!}$

i.e $x \displaystyle\int_0^x \frac{1}{g_u^2(x)} - \frac{1}{x^2} dx = \sum_{m\geq 1} \delta_m \frac{x^m}{m!}$ (selon l'énoncé du théorème) (1)

**] calcul de $x \displaystyle\int_0^x \frac{1}{g_u^2(x)} - \frac{1}{x^2} dx$ à partir de l'identité $x = \sum_{m\geq 1} \epsilon_m \dfrac{g_u^m}{m}$:

En dérivant et en la divisant par g_u^2 l'égalité $x = \sum_{m\geq 1} \epsilon_m \dfrac{g_u^m}{m}$

devient $\dfrac{1}{g_u^2(x)} = \displaystyle\sum_{m\geq 1} \epsilon_m g_u^{m-3} (g_u)'$ (2)

prouvons $\int\limits_0^x \frac{1}{g_u^2(x)} - \frac{1}{x^2} dx = \frac{1}{x} - \frac{1}{g_u(x)} + \sum_{m>2} \epsilon_m \frac{g_u^{m-2}}{m-2}$ (3)

ce qui revient à prouver : $\frac{1}{g_u^2(x)} - \frac{1}{x^2} = \left(\frac{1}{x} - \frac{1}{g_u(x)} + \sum_{m>2} \epsilon_m \frac{g_u^{m-2}}{m-2}\right)'$

c'est à dire $\frac{1}{g_u^2(x)} = \frac{g_u'}{g_u^2(x)} + \sum_{m\geq 2} \epsilon_m g_u^{m-3} (g_u(x))'$

or ceci est déjà demontré en (2)

***] Aprés multiplication de(3)par x comparons les formules $x \times 3$ et (1)

on a alors $\sum_{m\geq 2} \delta_m \frac{x^m}{m!} = x\left(\frac{1}{x} - \frac{1}{g_u(x)} + \sum_{m>2} \epsilon_m \frac{g_u^m}{m-2}\right)$

remplaçons avec $\frac{x}{g_u(x)} = \sum_{m\geq 0} v(m) \frac{x^m}{m!}$ on trouve alors

$\sum_{m>2} \delta_m \frac{x^m}{m!} + \sum_{m\geq 0} v(m) \frac{x^m}{m!} = 1 + X \sum_{m>2} \epsilon_m \frac{g_u^m}{m-2}$

comme le membre droit de cette égalité est une série de $H(\mathbb{Z})$ on conclut que

$$\delta_m + v(m) \in \mathbb{Z} \ ; \forall m \geq \square$$

Corollaire

Soient $k(k^m - 1) v(m) = v(m,k)$

$$k(k^m - 1)\delta_m = \delta_{m,k}$$

alors $v(m,k)$ et $\delta_{m,k}$ sont entiers

Preuve :

1] prouvons que $k(k^m - 1) v(m) \in Z$

on a $k(k^m - 1) v(m) = k(k^m - 1)\left(G_m - \sum_{p-1\backslash m} \frac{1}{p} \epsilon_p^{\frac{m}{p-1}}\right)$

comme $k(k^m - 1) G_m \in Z$; alors la preuve de 1] revient à prouver $\frac{k(k^m - 1)}{p} \epsilon_p^{\frac{m}{p-1}} \in Z$

remarquons que

a] si $k \equiv 0 \operatorname{mod} p$, alors le résultat est établi

b] si on arrive à prouver $k\left(k^{m}-1\right) \equiv 0 \operatorname{mod} p \forall k, \forall m$ tel que $p-1 \backslash m$, alors le résultat sera établi.

donc on suppose que k n'est pas congrue à $0 \operatorname{mod} p$ *et* prouvons que

$k\left(k^{m}-1\right) \equiv 0 \operatorname{mod} p$

pour cela distinguons deux cas :/ m pair ; /m impair

1^{er} *cas* (m pair) :alors $\exists\ l \in Z$ tel que $m = 2l$

$p-1 \backslash 2l \Longrightarrow \exists\ c \in Z$ tel que $2l = (p-1)c$

donc $k^{m}-1 = k^{(p-1)c}-1$

mais d'aprés le petit théorème de Fermat

$\left(k^{c}\right)^{p-1}-1 \equiv 0 \operatorname{mod} p$, d'où $k\left(k^{m}-1\right) \equiv 0 \operatorname{mod} p$

$2^{ème}$*cas* (m impair)

si $m=1$, $k(k-1)v(1) = k(k-1)\frac{\epsilon_2}{2} \in Z$car $k(k-1) \equiv 0 \operatorname{mod} 2$, pour tout k

si $m=3$, $k\left(k^{3}-1\right)$ $k\left(k^{m}-1\right)\left[G_{m}+\frac{\epsilon_2}{2}+\frac{\epsilon_2\epsilon_4}{2}\right]$cst entier car

$k\left(k^{3}-1\right) \equiv 0 \operatorname{mod} 2$,

si $m>3$, $k\left(k^{m}-1\right)\left[G_{m}+\frac{\epsilon_2}{2}+\frac{\epsilon_2\epsilon_4}{2}\right]$ est entier ;et ainsi $k\left(k^{m}-1\right)v(m) \in Z$

II] prouvons que $k\left(k^{m}-1\right)\delta_{m} \in Z$

d'aprés le théorème 3 on a $\delta_{m}+v(m) \in Z$

d'où $k\left(k^{m}-1\right)\delta_{m}+ k\left(k^{m}-1\right)v(m) \in Z$

et donc $k\left(k^{m}-1\right)\delta_{m} \in Z$ car $k\left(k^{m}-1\right)v(m) \in Z$ $\square$

Dans le théorème suivant ,on ne va plus considérer l'hypothèse des théorèmes

2 et 3

Théorème4

Soit $k \in \mathbb{N} - \{0\}$

Soient les séries $f(X) = \sum\limits_{m \geq 0} c_m \dfrac{X^{km+1}}{(km+1)!}$ $(c_0 = 1)$et sa réciproque

$\lambda(X) = \sum\limits_{m \geq 0} e_m \dfrac{X^{km+1}}{(km+1)!}$ $(e_1 = 1)$

telles que c_m et e_m sont des entiers modulo$k$

posons $\dfrac{X}{f(X)} = \sum\limits_{m > 0} \beta_m \dfrac{X^{km}}{(km)!}$

on a alors $\beta_m \equiv c_m \bmod k$

Preuve :

$$\frac{x}{f(x)} = \frac{x}{\sum_{m \geq 0} c_m \frac{x^{km+1}}{(km+1)!}} = \frac{1}{1 + c_1 \frac{x^k}{(k+1)!} + c_2 \frac{x^{2k}}{(2k+1)!} + \dots\dots}$$

$$= \sum_{i \geq 0} (-1)^i \left(\sum_{\alpha > 0} c_\alpha \frac{x^{k\alpha}}{(k\alpha+1)!} \right)^i = \sum_{m \geq 0} \beta_m \frac{x^{km}}{(km)!} \quad (1)$$

d'autre part $\dfrac{x}{f(x)} = \sum_{m \geq 0} e_m \dfrac{f^{km+1-1}}{(km+1)!} = \sum_{m > 0} e_m \dfrac{f^{km}}{(km+1)(km)!}$

d'où $\quad \dfrac{x}{f(x)} \equiv \sum_{m > 0} e_m \dfrac{f^{km}}{(km)!} \bmod k \qquad$ car $(km+1)! \equiv 1 \bmod k \quad (2)$

(1) et (2) impliquent $\sum_{m > 0} \beta_m \dfrac{x^{km}}{(km)!} \equiv \sum_{m > 0} e_m \dfrac{f^{km}}{(km)!} \bmod k$

donc si on arrive à établir que $\qquad \dfrac{f^{km}}{(km)!} \equiv \dfrac{X^{km}}{(km)!} \bmod k$, on obtiendra alors

facilement le résultat du théorème

à cette fin procédons comme suit

on a $f = \sum_{m \geq 0} c_m \dfrac{x^{km+1}}{(km+1)!} = x \sum_{m \geq 0} c_m \dfrac{x^{km}}{(km+1)!}$

$$f = x + \sum c_m \frac{x^{km}}{(km+1)!} \bmod k,$$

i.e $f = x(1 + f_1)$, $\quad$ où $\quad f_1 \equiv \sum c_m \dfrac{x^{km}}{(km)!} \bmod k$

soit p un nombre premier et soit s une puissance de p qui divise k

$$\begin{aligned}
\frac{f^{p^S}}{p^s} &= \frac{x^{p^S}}{p^s!}(1+f)^{p^S} \\
\frac{f^{p^S}}{p^s!} &\equiv \frac{x^{p^S}}{p^s\,!} + \frac{x^{p^S}}{p^s\,!}\sum_{\alpha=1}^{p-1}\binom{p^S}{\alpha}\left(f_1^{p^S}\right)^{\alpha} + \frac{x^{p^S}}{p^S!}f_1^{p^S} \bmod p^s \text{d'où} \\
\frac{f^{p^S}}{p^s!} &\equiv \frac{x^{p^S}}{p^s\,!} \bmod p^S \text{ car } \binom{p^s}{\alpha} \equiv 0 \bmod p^S \text{et} \\
\frac{x^{p^S}}{p^s\,!}f_1^{p^S} &\equiv 0 \bmod p^S, \text{puisque } f_1^{p^S} \equiv 0 \bmod p^S \text{ et } \frac{x^{p^S}}{p^s\,!} \in H(\mathbb{Z}) \\
\text{donc } \frac{f^{p^S}}{p^s!} &\equiv 0 \bmod p^S \qquad (2.1)
\end{aligned}$$

plus généralement pour tout $m \geqslant 1$, on a

$$\frac{f^{p^S m}}{(p^s\,m)!} = \frac{x^{p^S m}}{(p^s m)\,!}(1+f_1)^{p^S m} \equiv \frac{x^{p^S m}}{(p^s\,m)\,!} \bmod p$$

d'où on conclut que si p parcourt l'ensemble des diviseurs premiers de k , on obtient

$$\frac{f^{km}}{(km)!} \equiv \frac{x^{km}}{(km)!} \bmod k \text{donc}$$

$$\sum_{m>0}\beta_m\frac{x^{km}}{(km)!} \equiv \sum_{m\geq 0}e_m\frac{x^{km}}{(km)!} \bmod k$$

i.e $\qquad \beta_m \equiv e_m \bmod k \qquad \square$

Chapitre 3

Congruences de Kummer pour les cofficients des séries Hurwitz

3.1 Généralites

Introduction

Kummer a obtenu la congruence sur les nombres d'Euler E_m

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} \; E_{n+s(p-1)} \equiv 0 \bmod p^r$$

grâce au résultat général suivant

Théorème1

soient $p > 2$ un nombre premier et r un entier positif

soit u une suite de $S_0(Z_p)$ tel que $\forall n \in \mathbb{N}$ on a $\frac{uo\bar{a}}{n!}\,(n) \in Z_p$

alors on a

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} \; u(n+s(p-1)) \equiv 0 \bmod p^r \quad \text{pour tout } n \geqslant r$$

pour la preuve on aura besoin du théorème suivant

Théorème2

soit u une suite de $S_0(Z_p)$,

on a $\sum\limits_{s=0}^{r}(-1)^s\binom{r}{s}\ u(n+r+s(p-1)) \equiv 0 \bmod p^r \iff (T^p-T)^r u(n) \equiv 0 \bmod p^r$

Preuve:

$$\begin{aligned}(T^p-T)^r u(n) &= \textstyle\sum_{s=0}^{r}(-1)^{r-s}\dbinom{r}{s}T^{r+s(p-1)}u(n)\\ &= \textstyle\sum_{s=0}^{r}(-1)^{r-s}\dbinom{r}{s}u(n+r+s(p-1))\end{aligned}$$

posons $m=n+r$,alors

$(T^p-T)^r u(n) = (-1)^r \sum_{s=0}^{r}(-1)^{-s}\dbinom{r}{s}u(n+s(p-1)) \quad m \geqslant r$

donc $\sum\limits_{s=0}^{r}(-1)^s\binom{r}{s}\ u(n+r+s(p-1)) \equiv 0 \bmod p^r \iff (T^p-T)^r u(n) \equiv 0 \bmod p^r$

Preuve du théorème1

d'aprés le théorème 2 la preuve revient à démontrer que

$(T^p-T)^r u(n) \equiv 0 \bmod p^r$

$u(n) = uo\bar{a}oa(n)$

$$\begin{aligned}(T^p-T)^r u(n) &= (T^p-T)^r uo\bar{a}oa(n)\\
&= (T^p-T)^r \sum_{k=1}^{n} uo\bar{a}(k)S(n,k)\\
&= (T^p-T)^r \sum_{k=1}^{n}\left(\frac{uo\bar{a}(k)}{k!}\right)k!S(n,k)\\
&= \sum_{k=1}^{n}\left(\frac{uo\bar{a}(k)}{k!}\right)(T^p-T)^r k!S(n,k)\\
&= \sum_{k=1}^{n}\left(\frac{uo\bar{a}(k)}{k!}\right)\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}T^{r+s(p-1)}k!S(n,k)\\
&= \sum_{k=1}^{n}\left(\frac{uo\bar{a}(k)}{k!}\right)\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}T^{r+s(p-1)}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n\\
&= \sum_{k=1}^{n}\left(\frac{uo\bar{a}(k)}{k!}\right)\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}j^{n+r+s(p-1)}\end{aligned}$$

$$= \sum_{k=1}^{n} \left(\frac{uo\bar{a}(k)}{k!}\right) \sum_{j=0}^{k} (-1)^r (-1)^{k-j} \binom{k}{j} j^{n+r} \sum_{s=0}^{r} (-1)^s \binom{r}{s} j^{s(p-1)}$$
$$= \sum_{k=1}^{n} \left(\frac{uo\bar{a}(k)}{k!}\right) \sum_{j=0}^{k} (-1)^r (-1)^{k-j} \binom{k}{j} j^{n+r} (1 - j^{p-1})^r \equiv 0 \bmod p^r \square$$

Il est naturel de se demander si les hypothèses peuvent être affaiblies, la réponse est donnée dans le théorème 3.1.6

propositon1

$$v_p(k!) = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \ldots\ldots.$$

Preuve :voir[1]

notons $\gamma(k) = \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \left[\frac{k}{p^4}\right] + \ldots\ldots = v_p(k!) - \left[\frac{k}{p}\right]$

Théorème 3(théorème 1de Carlitz)

$$(T^p - T)^r k! S(n,k) \equiv 0 \bmod p^{r+\gamma(k)}$$

Preuve :

$1^{er} cas \quad r \leq \left[\frac{k}{p}\right]$

$\left(e^X - 1\right)^k = \sum_{n \geq k} k! S(n,k) \frac{X^n}{n!}$

on a $\left(e^X - 1\right)^k \equiv 0 \bmod k!$ (prpos.1chap1)

alors $k! S(n,k) \equiv 0 \bmod p^{v_p(k!)}$i.e $k! S(n,k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]+\gamma(k)}$

puisque $r \leq \left[\frac{k}{p}\right]$ alors $k! S(n,k) \equiv 0 \bmod p^{r+\gamma(k)}$

$2^{ème} cas \quad r > \left[\frac{k}{p}\right]$

$(T^p - T)^r k! S(n,k) \equiv 0 \bmod p^{r+\gamma(k)} \iff (T^p - T)^r S(n,k) \equiv 0 \bmod p^{r-\left[\frac{k}{p}\right]}$

posons

$k = mp + \tau$ où $0 \leq \tau \leq p - 1 \Longrightarrow \left[\frac{k}{p}\right] = m$

$t = r - m$

on aura $(T^p - T)^r S(n,k) = (T^p - T)^{m+t} S(n,k)$

$(T^p - T) S(n,k) \equiv S(n, k - p) \bmod p$

par composition m fois de l'opérateur $(T^p - T)$ on a

$(T^p - T)^m S(n,k) \equiv S(n, k - mp) \bmod p = S(n,\tau) \bmod p$

il résulte alors $(T^p - T)^{m+t} S(n,k) \equiv (T^p - T)^t S(n,\tau) \bmod p$

or sachant que $S(n,\tau) = \frac{1}{\tau!} \sum\limits_{j=1}^{\tau} (-1)^{\tau-j} \binom{\tau}{j} j^n$,

on déduit que $(T^p - T)^t S(n,\tau) = \frac{1}{\tau!} \sum\limits_{j=1}^{\tau} (-1)^{\tau-j} \binom{\tau}{j} (T^p - T) j^n$

donc ça revient à étudier l'application de l'opérateur $T^p - T$ à la suite $v = \lambda\alpha^q$,

$(T^p - T) v = \lambda (T^p - T) \alpha^q = \lambda (T^p\alpha^q - T\alpha^q) = (\alpha^p - \alpha) v \equiv 0 \bmod p$

d'où $(T^p - T)^t v = (\alpha^p - \alpha)^t v \equiv 0 \bmod p^t$

par linéarité pour $0 \leq \tau < p$ *i.e* pour $\lambda\tau^q$, on obtient

$(T^p - T)^t S(n,k) \equiv 0 \bmod p^t$

$(T^p - T)^{m+t} S(n,k) \equiv 0 \bmod p^t \Box$

Théorème4(théorème de Carlitz)

Soit une suitede $S_0(\mathbb{Z}_p)$

$(T^p - T)^r u(n) \equiv 0 \bmod p^r \quad \Longleftrightarrow u o \bar{a}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$

Preuve

1] $\Leftarrow$

on suppose que $u o \bar{a}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$

i.e ($(T^p - T)^r k! S(n,k)) \left(\frac{uo\bar{a}(k)}{k!}\right) \equiv 0 \bmod p^r$ $\quad (**)$

En remplaçant $(**)$ dans $(*)$ on obtient

$\left(\frac{uo\bar{a}(n)}{n!}\right)(T^p - T)^r n! S(n,n) \equiv 0 \bmod p^r$

or d'aprés le théorème4 on a $(T^p - T)^r n! S(n,n) \equiv 0 \bmod p^{r+\gamma(n)}$

et comme $\frac{1}{n!} \equiv 0 \bmod p^{-v_p(n!)}$ alors $uo\bar{a}(n) \equiv 0 \bmod p^{\left[\frac{n}{p}\right]}$ □

Théorème 5

Soit u une suite de $\Omega_1(Z_p)$ telle que $u(n) \equiv 0 \bmod p^{\left[\frac{n}{p}\right]}$

alors $k! B_{n,k}(u) \equiv 0 \bmod p^{\left[\frac{n}{p}\right]+\gamma(k)}$

Théorème6

Soit u une suite de $\Omega_1(Z_p)$ telle que $uo\bar{a}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$

alors $\sum_{s=0}^{r} (-1)^s \binom{r}{s} B_{n+s(p-1),k} \equiv 0 \bmod p^{r+\gamma(k)}$

i.e $(T^p - T)^r k! B_{n,k}(u) \equiv \bmod p^{r+\gamma(k)}$

Preuve :

$$\begin{aligned}
(T^p - T)^r k! B_{n,k}(u) &= (T^p - T)^r k! B_{q,k}(u) o\bar{a} o a(n) \\
&= (T^p - T)^r \sum_{\alpha=0}^{n} k! B_{q,k}(u) o\bar{a}(\alpha) S(n,\alpha) \\
&= (T^p - T)^r \sum_{\alpha=0}^{n} \frac{k! B_{q,k}(u) o\bar{a}}{\alpha!}(\alpha)\ \alpha! S(n,\alpha) \\
&= \sum_{\alpha=0}^{n} \frac{k! B_{q,k}(u) o\bar{a}}{\alpha!}(\alpha)(T^p - T)^r\ \alpha! S(n,\alpha)
\end{aligned}$$

or

$(T^p - T)^r \alpha! S(n,\alpha) \equiv \bmod p^{r+\gamma(\alpha)}$

$\alpha! \equiv \bmod p^{\left[\frac{\alpha}{p}\right]+\gamma(\alpha)}$

$(k! B_{q,k}(u) o\bar{a}) = k! B_{\alpha,k}(uo\bar{a}) \equiv 0 \bmod p^{\left[\frac{\alpha}{p}\right]+\gamma(k)}$

d'où $(T^p - T)^r k! B_{n,k}(u) \equiv 0 \bmod p^{r+\gamma(\alpha)-\gamma(\alpha)+\left[\frac{\alpha}{p}\right]-\left[\frac{\alpha}{p}\right]+\gamma(k)}$

$(T^p - T)^r k! B_{n,k}(u) \equiv 0 \bmod p^{r+\gamma(k)}$ □

notons Θ_p l'ensemble des suites $u(n)$ de $S_0(Z_p)$ tel que

$(T^p - T)^r u(n) \equiv 0 \bmod p^r \ \forall n \geq r$

Théorème7

Soit u une suite de Θ_p tel que $u(1) = 1$ et soit v une suite de $S_0(Z_p)$

alors on a

$$v \in \Theta_p \Longleftrightarrow vo\overline{u}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$$

Preuve:

1]

$(T^P - T)^r v(n) = (T^p - T)^r vo\overline{u}ou(n)$

$$= \sum_{k=1}^{n} \frac{vo\overline{u}}{k!}(k)\ (T^p - T)^r k! B_{n,k}(u)$$

or $u \in \Theta_p \Longleftrightarrow (T^p - T)^r u(n) \equiv 0 \bmod p^r$

$$\Longleftrightarrow uo\overline{a}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]} \qquad \text{(voir thm 4)}$$

$$\Longrightarrow (T^p - T)^r k! B_{n,k}(u) \equiv 0 \bmod p^{r+\gamma(k)} \qquad \text{(voir thm 6)}$$

et comme $vo\overline{u}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$ alors $(T^p - T)^r v(n) \equiv 0 \bmod p^r$

2]

soient u , v deux suites de Θ_p ;prouvons que $vo\overline{u}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$

la preuve est similaire à celle du théorème 4.

Par analogie au théorème de Carlitz(thm4), et au lieu de supposer que $uo\overline{a}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$

nous supposerons désormais que $\tilde{u}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$ i.e $uo\overline{\alpha}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]}$

et nous calculerons la classe de $(T^p - T)^r u(n)$modulop^r

la réponse fera l'objet de la prposition2

Proposition 2

soit u une suite de $S_0(\mathbb{Z}_p)$, alors

$\tilde{u}(k) \equiv 0 \bmod p^{\left[\frac{k}{p}\right]} \Longrightarrow \sum_{s=0}^{r}(-1)^s\binom{r}{s}u(n+s(p-1)) \equiv 0 \bmod p^r$

Preuve :

dire que $(T^p - T)^r u(n) \equiv 0 \bmod p^r \Longleftrightarrow (T^p - T)^r uo\overline{\alpha}o\alpha(n) \equiv 0 \bmod p^r$

$(T^p-T)^r uo\overline{\alpha}o\alpha(n) = (T^p-T)^r \sum_{k=1}^{n} uo\overline{\alpha}(k)s(n,k) = (T^p-T)^r \sum_{k=1}^{n} uo\overline{\alpha}(k)(-1)^{n+k}S(n,k)$

si on arrive à prouver que $(T^p - T)^r(-1)^{n+k}S(n,k) \equiv 0 \bmod p^{r-\left[\frac{k}{p}\right]}$ le problème serait résolu

posons

$k = mp + \tau$ où $0 \leq \tau \leq p-1$; d'où $\left[\frac{k}{p}\right] = m$

$t = r - m$

on aura $(T^p - T)^r \left(-1\right)^{n+k} S\left(n,k\right) = \left(T^p - T\right)^{m+t} \left(-1\right)^{n+k} S\left(n,k\right)$ on a

$T(-1)^{n+k}S\left(n,k\right) = (-1)^{n+k+1}S\left(n+1,k\right)$

par itération on obtient

$T^p(-1)^{n+k}S\left(n,k\right) = (-1)^{n+k+p}S\left(n+p,k\right)$

d'autre part sachant que $S\left(n+1,k\right) = S\left(n,k-1\right) + kS\left(n,k\right)$

et en multipliant les deux membres par $(-1)^{n+k+1}$ on obtient

$(-1)^{n+k+1}S\left(n+1,k\right) = (-1)^{n+k+1}S\left(n,k-1\right) + (-1)^{n+k+1}kS\left(n,k\right)$

et comme $(-1)^{-1} = (-1)^1$, on déduit alors

$(T+k)\,(-1)^{n+k}S(n+1,k)=(-1)^{n+k-1}S(n,k-1)$

par itération

$(T+k)(T+k-1).....(T+k-p+1)(-1)^{n+k}S(n,k)=(-1)^{n+k-p}S(n,k-p)$

d'où $(T^p-T)\,(-1)^{n+k}S(n,k)\equiv(-1)^{n+k-p}S(n,k-p)\bmod p$

et donc $(T^p-T)^m\,(-1)^{n+k}S(n,k)\equiv(-1)^{n+k-mp}S(n,k-mp)\bmod p$

i.e $(T^p-T)^{m+t}\,(-1)^{n+k}S(n,\tau)\equiv(T^p-T)^t\,(-1)^{n+\tau}S(n,\tau)\bmod p$

mais on a $(T^p-T)^t\,S(n,\tau)\equiv 0\bmod p^t$ ce qui impliquera que

$(T^p-T)^t\,(-1)^{n+\tau}S(n,\tau)\equiv 0\bmod p^t$

car $(T^p-T)^t\,S(n,\tau)\equiv 0\bmod p^t\iff\sum\limits_{j=0}^{t}\binom{t}{j}T^{pj}(-1)^{t-j}T^{t-j}S(n,\tau)\equiv 0\bmod p^t$

$$\begin{aligned}\sum_{j=0}^{t}\binom{t}{j}T^{pj}(-1)^{t-j}T^{t-j}S(n,\tau)&=\sum_{j=0}^{t}\binom{t}{j}T^{pj+t-j}(-1)^{t-j}S(n,\tau)\\&=\sum_{j=0}^{t}\binom{t}{j}(-1)^{t-j}S(n+pj+t-j,\tau)\end{aligned}$$

et d'autre part on a

$$\begin{aligned}(T^p-T)^t(-1)^{n+\tau}S(n,\tau)&=\sum_{j=0}^{t}\binom{t}{j}(-1)^{t-j}(-1)^{n+pj+t-j}S(n+pj+t-j,\tau)\\&=(-1)^{n+t}\sum_{j=0}^{t}\binom{t}{j}(-1)^{t-j}(-1)^{j(p-1)}S(n+pj+t-j,\tau)\end{aligned}$$

or $(-1)^{j(p-1)}=1$ pour tout p premier $\neq 2$

et donc on a le résultat recherché $\square$

3.2 Congruence de Kummer pour des séries linéaires spéciales

Théorème 8

Soit p un nombre premier

soit $f(x) = \sum_{m\geq 1} c_m \frac{x^m}{m!}$ une série linéaire de $H(\mathbb{Z})$ $(resp. H(\mathbb{Z}_p))$

soit $\lambda(x) = \sum_{m\geq 1} e_m \frac{x^m}{m!}$ la série réciproque de $f(X)$

si $p \not| e_m$ $\forall\, m > p$ alors $c_{m+p-1} \equiv c_m c_p \mod p; \forall m \geq 1$

remarquons que pour prouver ce théorème , il suffit de prouver que $f(x) = \sum_{m\geq 1} c_m \frac{f_1^m(x)}{m!} \mod p$

où $\frac{f_1^m(x)}{m!}$ est une série dont les coefficients sont des puissances de c_p $(\forall 1 \leq m \leq p-1)$

Preuve

$$x = \lambda o f(x) = \sum_{m\geq 1} e_m \frac{f^m(x)}{m!} \equiv \sum_{m=1}^{p} c_m \frac{f^m(x)}{m!} \mod p \quad \text{car } p \not| e_m \quad \forall m > p$$

notons $f_1(x) = x - c_p \frac{f^p(x)}{p!}$

$$\equiv \sum_{m=1}^{p} e_m \frac{f^m(x)}{m!} - e_p \frac{f^p(x)}{p!} \mod p$$

$$\equiv \sum_{m=1}^{p-1} e_m \frac{f^m(x)}{m!} \mod p$$

développons $\frac{f_1^m(x)}{m!}$ en série (pour tout $1 \leq m \leq p-1$)

on aura recours aux résultats suivants qui seront démontrés ultérieurement.

Proposition3

$$f_1^{p-1}(x) \equiv f^{p-1}(x) \mod p$$

Proposition4

$$f'(x) \equiv \sum_{m=0}^{\infty} d_m f^m(x) \mod p \text{ avec } d_m \in Z \ , \ d_0 = 1$$

Proposition5

$$\frac{f_1^p(x)}{p} \equiv \frac{f^p(x)}{p} \mod p$$

***Détermination de la série $f_1(X) \bmod p$**

$$\begin{aligned} f_1(x) &= x - e_p \frac{f^p(x)}{p!} \\ &= x - c_p \int \frac{f^{p-1}(x)}{(p-1)!} f'(x)\,dx \\ &\equiv x - c_p \int \frac{f^{p-1}(x)}{(p-1)!} \textstyle\sum_{m=0}^{\infty} d_m f^m(x) dx \qquad \text{(voir propo 4)} \\ &\equiv x + c_p \int \frac{f^{p-1}(X)}{(p-1)!} dx \bmod p \qquad \text{car } c_p \equiv -e_p \bmod p \end{aligned}$$

$$(\forall m > p, p \backslash e_m) \Rightarrow \frac{f^{p-1}(x)}{(p-1)!} \equiv \sum_{m=1}^{\infty} c_p^{m-1} \frac{x^{m(p-1)}}{m(p-1)!} \qquad \text{(voir thm.1chap2)}$$

on obtient alors

$$\begin{aligned} f_1(x) &\equiv x + c_p \int \sum_{m=1}^{\infty} c_p^{m-1} \frac{x^{m(p-1)}}{m(p-1)!} dx \bmod p \\ &\equiv x + \sum_{m=0}^{\infty} c_p^{m-1} \frac{x^{m(p-1)+1}}{(m(p-1)+1)!} \bmod p \\ &\equiv \sum_{m=0}^{\infty} c_p^{m-1} \frac{x^{m(p-1)+1}}{(m(p-1)+1)!} \bmod p \end{aligned}$$

***Détermination de la série$\frac{f_1^k}{k!} \bmod p \quad (1 \leq k \leq p-1)$**

En fait , nous allons prouver par récurrence sur l'ordre de dérivation que

$$\frac{f_1^k}{k!} \equiv \sum_{m=0}^{\infty} c_p^m \frac{x^{m(p-1)+k}}{(m(p-1)+k)!} \bmod p \qquad (1)$$

et ce en dérivant les deux membres de la congruence de la proposition3

la propriété est vraie pour l'ordre $k-1$ (voir thm 2.1)

prouvons que (1) est vraie pour $k = p-2$

or $\left(f_1^{p-1}(x) \equiv f^{p-1}(x) \bmod p\right) \Longrightarrow \frac{f_1^{p-1}(x)}{(p-1)!} \equiv \frac{f^{p-1}(x)}{(p-1)!} \bmod p$

aprés dérivation des deux membres de $\frac{f_1^{p-1}(x)}{(p-1)!} \equiv \frac{f^{p-1}(x)}{(p-1)!} \bmod p$,on obtient

$$\frac{f_1^{p-2}(x) f_1'(x)}{(p-2)!} \equiv \left(\frac{f^{p-1}(x)}{(p-1)!}\right)' \bmod p$$

i.e $f_1^{p-2}(x) \dfrac{[1 + e_p f^{p-1} f']}{(p-2)!} \equiv \left(\dfrac{f^{p-1}(x)}{(p-1)!}\right)' \bmod p$

i.e $f_1^{p-2}(x) \dfrac{[1 + e_p f^{p-1} f']}{(p-2)!} \equiv \left(\displaystyle\sum_{m=1}^{\infty} c_p^{m-1} \frac{x^{m(p-1)}}{(m(p-1))!}\right) \bmod p$

d'où $\dfrac{f_1^{p-2}(X)}{(p-2)!} \equiv \sum\limits_{m=1}^{\infty} c_p^{m-1} \dfrac{x^{m(p-1)-1}}{(m(p-1)-1)!} \bmod p$

soit le changement d'indice $n = m-1$,alors

$\dfrac{f_1^{p-2}(X)}{(p-2)!} \equiv \sum\limits_{m=0}^{\infty} c_p^{n} \dfrac{x^{n(p-1)+p-2}}{(n(p-1)+p-2)!} \bmod p$

et ainsi le résultat est vraie pour $k = p-2$

Supposons que la propriété est vraie pour $k \leq p-1$

assurons nous qu'elle reste vraie jusqu'à l'ordre $k-1$

puisque $\dfrac{f_1^k}{k!} \equiv \sum\limits_{m=1}^{\infty} c_p^{m} \dfrac{x^{m(p-1)+k}}{(m(p-1)+k)!} \bmod p$

alors aprés dérivation des deux membres de cette congruence , on aura

$\dfrac{f_1^{k-1}}{(k-1)!} \equiv \sum\limits_{m=0}^{\infty} c_p^{m} \dfrac{x^{m(p-1)+k-1}}{(m(p-1)+k-1)!} \bmod p$

d'où la preuve par récurrence est achevée.

détermination de $f(x)$ en fonction de$\dfrac{f_1^m}{m!}(x)$

On a $f_1(x) = \sum\limits_{m=1}^{p-1} c_m \dfrac{f^m(x)}{m!}$

i.e $f_1(x) = c_1 f(x) + c_2 \dfrac{f^2(x)}{2!} + \dots\dots\dots + c_{p-1} \dfrac{f^{p-1}(x)}{(p-1)!}$

en calculant la puissance $m^{ième}$de chaque membre de cette égalité, on obtient

un système de $p-1$ équations à $p-1$ variables

$$f_1(x) = c_1 f(x) + c_2 \frac{f^2(x)}{2!} + \dots + c_{p-1} \frac{f^{p-1}(x)}{(p-1)!}$$
$$\frac{f_1^2(x)}{2!} = \alpha_1^{(2)} f(x) + \alpha_2^{(2)} \frac{f^2(x)}{2!} + \dots + c_{p-1}^{(2)} \frac{f^{p-1}(x)}{(p-1)!}$$

$$\frac{f_1^{p-1}(x)}{(p-1)!} = \alpha_1^{(p-1)} f(x) + \alpha_2^{(p-1)} \frac{f^2(x)}{2!} + \dots + c_{p-1}^{(p-1)} \frac{f^{p-1}(x)}{(p-1)!}$$

système obtenu par la considération de $f_1^k(x) \equiv 0 \bmod p$, $\forall k > p$ et que

2!,3! .$(p-1)!$ sont tous premiers avec p

comme ce système admet la solution $f_1(x)$ ceci implique que son déterminant

est inversible dans Q $(resp.Q_p)$

d'où la solution inverse existe i.e $f(x)$ s'exprime en fonction de $f_1(X)$ d'où

$$f(x) \equiv \sum_{m=1}^{p-1} \gamma_m \frac{f_1^m(x)}{m!} \bmod p$$

Détermination de γ_m

comparons entre $\left(f_1(x) \equiv \sum_{m=1}^{p-1} c_m \frac{f^m(x)}{m!} \bmod p\right)$ et
$\left(\sum_{m\geq 1} c_m \frac{x^m}{m!} \text{ est l'inverse de } \sum_{m\geq 1} c_m \frac{x^m}{m!}\right)$
on déduit que $f(x) \equiv \sum_{m=1}^{p-1} c_m \frac{f_1^m(x)}{m!}$ i.e $\gamma_m \equiv c_m \bmod p$

Etablissement du résultat du théorème8&

$$\sum_{m\geq 1} c_m \frac{x^m}{m!} \equiv \sum_{m\geq 1} c_m \sum_{m=1}^{p-1} c_p^i \frac{x^{i(p-1)+m}}{(i(p-1)+m)!} \bmod p$$

en comparant les coefficients de $\frac{x^{i(p-1)+m}}{(i(p-1)+m)!}$ dans les deux membres de la

congruence , on déduit que

$$c_{m+i(p-1)} \equiv c_m c_p^i \qquad \left(1 \leq m \leq p-1\right)$$

prouvons par récurrence que

$$\left(c_{m+i(p-1)} \equiv c_m c_p^i \bmod p; 1 \leq m \leq p-1\right) \Longrightarrow \left(c_{m+p-1} \equiv c_m c_p \bmod p; \forall m \geq 1\right)$$

pour cela spécifions deux cas :$1^{er}cas : m \leq p-1$; $2^{ème}cas : m > p-1$

$\diamond$*pour le*1^{er}*cas*: il suffit de remplaçer $i = 1$ dans $c_{m+i(p-1)} \equiv c_m c_p^i \operatorname{mod} p$,

on retouve $c_{m+p-1} \equiv c_m c_p \operatorname{mod} p$

$\diamond$ *pour le* $2^{ème}$ *cas* : étudions d'abord le cas où $m = p$

$c_{p+p-1} = c_{1+2(p-1)} \equiv c_1 c_p^2 \operatorname{mod} p$ d'aprés l'hypothèse de récurrence

d'où effectivement ,on a $c_{p+p-1} = c_p c_p \operatorname{mod} p$

maintenant prouvons que c'est vrai quel que soit $m > p-1$

posons $m = i(p-1) + \alpha$ *avec* $0 \leq \alpha < p-1$

d'où $c_{m+p-1} = c_{i(p-1)+\alpha+p-1} = c_{\alpha+(i+1)(p-1)}$

d'aprés l'hypothèse on a $c_{m+p-1} = c_{\alpha+(i+1)(p-1)} \equiv c_\alpha c_p^{i+1} \operatorname{mod} p$ (1)

d'autre part on a $c_m c_p = c_{\alpha+i(p-1)} c_p \equiv c_\alpha c_p^i c_p \equiv c_\alpha c_p^{i+1} \operatorname{mod} p$ (2)

en comparant (1) et (2) on constate que $c_m c_p \equiv c_{m+p-1} \operatorname{mod} p$ $\square$

Preuve de la propositon 3

$f_1(x) \equiv \sum_{m=1}^{p-1} e_m \frac{f^m(x)}{m!} \operatorname{mod} p$

alors $f_1^{p-1}(x) \equiv \left(\sum_{m=1}^{p-1} e_m \frac{f^m(x)}{m!} \right)^{p-1} \operatorname{mod} p$

$\equiv f^{p-1} + \sum_{m=p}^{(p-1)^2} \beta_m f^m(X) \operatorname{mod} p$ où $\beta_m \in Z_p$

comme $f^m(x) \equiv 0 \operatorname{mod} p$ $\forall m > p$, on déduit $f_1^{p-1}(x) \equiv f^{p-1}(x) \operatorname{mod} p$ $\square$

Preuve de la proposition 4

$$x \equiv \sum_{m=1}^{p-1} e_m \frac{f^m(x)}{m!} \operatorname{mod} p$$

en dérivant les deux membres de cette congruence , on obtient

$1 \equiv f'(x) + 2\frac{e_2}{2!} f'(x) f(x) + 3\frac{e_3}{3!} f'(x) f^2(x) + -- + p\frac{e_p}{p!} f'(x) f^{p-1}(x) \operatorname{mod} p$

d'où

$$1 \equiv f'(x)\left[1+2\frac{e_2}{2!}f(x)+3\frac{e_3}{3!}f^2(x)+----+p\frac{e_p}{p!}f^{p-1}(x)\right] \bmod p$$

i.e

$$f'(X) \equiv \frac{1}{1+2\frac{e_2}{2!}f(x)+3\frac{e_3}{3!}f^2(x)+----+p\frac{e_p}{p!}f^{p-1}(x)} \bmod p$$

puisque $2\frac{e_2}{2!}f(x)+3\frac{e_3}{3!}f^2(x)+----+p\frac{e_p}{p!}f^{p-1}(x) \in H(\mathbb{Z}_p)$

alors on a

$1+2\frac{e_2}{2!}f(x)+3\frac{e_3}{3!}f^2(x)+----+p\frac{e_p}{p!}f^{p-1}(x)$ est une unité de$H(\mathbb{Z}_p)$

d'où

$$\frac{1}{1+2\frac{e_2}{2!}f(x)+3\frac{e_3}{3!}f^2(x)+----+p\frac{e_p}{p!}f^{p-1}(x)} \in H(\mathbb{Z}_p)$$

et donc $\quad f'(X) \equiv \sum_{i=0}^{p-1}(-1)^i \alpha_i f^i(x) \bmod p \quad (\alpha_i \text{ entier})$ □

Preuve de la proposition5

on a $f_1^{p-1}(x) \equiv f^{p-1}(x) \bmod p \qquad$ (voir proposition 3)

d'où $f_1^{p-1}(x)\, f_1'(x) \equiv f^{p-1}(x)\, f_1'(x) \bmod p$

i.e $f_1^{p-1}(x)\, f_1'(x) \equiv f^{p-1}(x)\left[1+e_p f^{p-1}(x)\right]$

i.e $f_1^{p-1}(x)\, f_1'(x) \equiv f^{p-1}(x) \bmod p$ (1)

mais d'autre part on a $f^{p-1}(x)\, f'(x) \equiv f^{p-1}(x) \bmod p$ (2)

(1) et (2) impliquent $f_1^{p-1}(x)\, f_1'(x) \equiv f^{p-1}(x)\, f'(x) \bmod p$

d'où $\displaystyle\int f_1^{p-1}(x)\, f_1'(x)\, dx \equiv \int f^{p-1}(x)\, f'(x)\, dx \bmod p$

et donc $\dfrac{f_1^{p}(x)}{p} \equiv \dfrac{f^{p}(x)}{p} \bmod p$

Chapitre 4

Théorèmes de Barsky

4.1 Théorème 1

Dèfinition 1

Soit $\tilde{F}(X) = \sum_{n\geq 0} a_n \frac{X^n}{n!} \in K[[X]]$ où K est une extension de Q

On appelle Transformation de Laplace formelle de $\tilde{F}(X)$ l'application L tel que

$$L\left(\tilde{F}(X)\right) = \sum_{n>0} a_n X^n = F(X)$$

Définition2

Soit $D \subset \mathbb{C}_p$.

on dit que la fonction $F = \sum_{n>0} a_n X^n$ est un élément analytique p-adique sur D

si et seulement si F est limite uniforme d'une suite de fractions rationnelles

$(F_n(X))_{n\geq 0} \in \mathbb{C}_p(X)$ sans pôles dans D

Notation

On note $H(D)$ l'ensemble des éléments analytiques sur D

Lemme(cf[12])

Une condition nécéssaire et suffisante pour que $F(X) = \sum_{n>0} a_n X^n \in \mathbb{C}_p[[X]]$ soit un élément analytique p-adique sur $D(0,1)^-$ est que la suite $(a_n)_{n\in\mathbb{N}}$ soit p- presque périodique

i.e $\forall h > 0, \exists N \in \mathbb{N}, \exists M \in \mathbb{N}$ tel que $\forall n \geq N$, $|a_{n+M} - a_n| \leq p^{-h}$

Théorème 1 de BARSKY

Soit $\tilde{F}(X) = \sum_{n>0} a_n \frac{X^n}{n!}$ une série de $\mathbb{C}_p[[X]]$ telle que

$\tilde{F}(X) = \sum_{n>0} b_n (e^X - 1)^n = \sum_{n>0} b_n T^n = \tilde{G}(T)$ où $T = e^X - 1$

alors les deux propositions suivantes sont équivalentes :

i] $F(X) = L\left(\tilde{F}(X)\right) = \sum_{n\geq 0} a_n X^n \in H\left(D(0,1)^-\right)$

ii] $G(T) = L\left(\tilde{G}(T)\right) = \sum_{n>0} n! b_n T^n \in H\left(D(0,1)^-\right)$

Remarque

Dans la suite on notera $D(0.1)^-$par D

Preuve :

$i \Longrightarrow ii$

avant d'entamer la preuve de cette implication on commence par en donner ses grandes lignes .

$F(X) \in H(D) \Longleftrightarrow \exists (F_n(X))_{n\geq 0}$ de $\mathbb{C}_p(X)$ sans pôles dans D qui converge uniformément vers $F(X)$.

$F_n(X)$ est une fraction rationnelle alors elle se décompose en éléments simples de $1^{ère}$ éspèce, sous la forme suivante

$F_n(X) = \sum_{finie} \alpha_k f_k(X) + \sum_{finie} \beta_k h_k(X)$

où $f_k = \dfrac{1}{(1-aX)^k}$ avec $|a| \leq 1$

et $h_k = X^k$

ainsi tout revient à étudier les f_k et les h_k

grâce au changement de variable $T = e^X - 1$ précisé dans le théorème de Barsky,

on transforme les fonctions $f_k(X)$ en fonctions $g_{f_k}(T)$ et les $h_k(X)$ en fonction

$g_{h_k}(T)$ et on démontrera que $g_{f_k}(T)$, $g_{h_k}(T) \in H(D)$ pour tout k

aprés on démontrera que $G(T)$ est approchée uniformement par

$(G_n(T))_{n\geq 0}$où $G_n(T) = \sum_{finie} \alpha_k g_{f_k}(T) + \sum_{finie} \beta_k g_{h_k}(T)$

i.e $\forall h \geq 0, \exists N_h, \forall T \in D, \forall n > N_h, G(T) \equiv G_n(T) \mod p^h$ et ce sachant

que $F(X) \equiv F_n(X) \mod p^h$

prouvons le tout de suite

notons la série $F(X) - F_n(X)$ par $F(X) - F_n(X) = \sum\limits_{n\geq 0} u_n X^n$

mais comme $F(X) - F_n(X) \equiv 0 \mod p^h$ (1)

on déduit que $u_n \equiv 0 \mod p^h$ $(\forall n \geqslant 0)$ (2)

en appliquant aux deux membres de (1) la fonction réciproque de la transforma

-tion de Laplace; on obtient

$\tilde{F}(X) - \tilde{F}_n(X) = \sum\limits_{n\geq 0} u_n \dfrac{X^n}{n!} = \sum\limits_{n\geq 0} b'_n (e^X - 1)^n = \sum\limits_{n>0} n! b'_n \dfrac{(e^X-1)^n}{n!}$

i.e $\sum\limits_{n\geq 0} u_n \dfrac{X^n}{n!} = \sum\limits_{n\geq 0} n! b'_n \dfrac{(e^X-1)^n}{n!}$ (3)

tel que $\sum\limits_{n\geq 0} n! b'_n \dfrac{(e^X-1)^n}{n!} = g_v o g_a$

où $v(n) = n! b'_n$

et $a(n) = \begin{cases} 0 & \text{si } n = 0 \\ 1 & \text{si } n \geq 1 \end{cases}$

de (3) on tire $u_n = voa(n) = \sum_{k=1}^{n} v(k) S(n,k)$

d'où $v(n) = uo\bar{a}(n) = \sum_{k=1}^{n} u_k s(n,k)$ (4)

comme $s(n,k)$ est entier (voir propriété1.3.21)

et comme $u_n \equiv 0 \bmod p^h$ (de(2))

(4) nous permet de déduire que $v(n) \equiv 0 \bmod p^h$ et ce $\forall n \geq 0$ (5)

d'autre part on a $\sum_{n\geq 0} v(n) \frac{(e^X - 1)^n}{n!} = \sum_{n\geq 0} v(n) \frac{T^n}{n!} = \tilde{G}(T) - \tilde{G}_n(T)$

d'où $\sum_{n\geq 0} v(n) T^n = G(T) - G_n(T)$ (6)

de (5) et (6) on déduit $G(T) - G_n(T) \equiv 0 \bmod p^h$ (7)

il en résulte de (7) que $G(T)$ est approchée uniformément par une suite de fractions rationnelles sans pôles dans D.

précisons exactement cette suite

sachant que $G_n(T) = \sum_{finie} \alpha_k g_{f_k}(T) + \sum_{finie} \beta_k g_{h_k}(T)$ et que $g_{f_k}(T)$ et $g_{h_k}(T)$ sont dans $H(D)$(ce qui va être prouvé plus tard) on déduit $G_n(T) \in H(D)$

alors $\exists (G_{n,\alpha}(T))_{\alpha \geqslant 0} \in C_p.(X)$ sans pôles dans D qui vérifie

$\forall h > 0, \exists N_h \in \mathbb{N}, \forall n > N_h, \forall T \in D \; |G_n(T) - G_{n,\alpha}(T)| \leq p^{-h}$

et ainsi on tire

$$|G(T) - G_{n,\alpha}(T)| = |G(T) - G_n(T) - (G_{n,\alpha}(T) - G_n(T))|$$
$$\leq \max(|(G(T) - G_n(T))|, |G_{n,\alpha}(T) - G_n(T)|)$$

d'où $G(T)$ est approchée uniforement par$\left(G_{n,\alpha}(T)\right)_{\alpha\geqslant 0}$ et donc $G(T) \in H(D)$

ainsi s'achève la donnée des grandes linges de la preuve

prouvons par récurence que $g_{f_k}(T) \in H(D)$

afin d'alleger l'écriture notons $g_{f_k}(T)$ par $g_k(T)$

pour $k = 1$ $\qquad f_1(X) = \dfrac{1}{1 - aX}$

d'où
$$\begin{aligned}\tilde{f}_1(X) &= e^{aX} = \left(e^X - 1 + 1\right)^a \\ &= \sum_{n>0} \binom{a}{n} \left(e^X - 1\right)^n \\ &= \sum_{n>0} \binom{a}{n} T^n \\ &= \tilde{g}_1(T)\end{aligned}$$

alors
$$\begin{aligned}g_1(T) &= \sum_{n>0} n! \binom{a}{n} T^n \\ &= \sum_{n>0} a(a-1)........(a-n+1)\, T^n\end{aligned}$$

suposons $n = rp^h + q \qquad$ où $0 \leq q \leq p^h - 1$

on a $a(a-1).......(a-n+1) = a(a-1)..........\left(a - \left(rp^h + q\right) + 1\right)$

$= a(a-1)........\left(a - \left(p^h - 1\right)\right) \times \left(a - p^h\right)\left(a - p^h - 1\right)\left(a - p^h - 2\right)...\left(a - 2p^h + 1\right) \times$

$\times.......\left(a - rp^h\right)\left(a - rp^h + 1\right)....\left(a - \left(rp^h + q\right) + 1\right) \bmod p^h$

$\equiv \underbrace{a(a-1)..\left(a - \left(p^h - 1\right)\right) \times .. \times a(a-1)..\left(a - \left(p^h - 1\right)\right)}_{r \text{ fois}} \times$

$\times\; a(a-1)...(a-q+1) \bmod p^h$

$\equiv \left\{a(a-1)....\left(a - \left(p^h - 1\right)\right)\right\}^r a(a-1)....(a-q+1) \bmod p^h$

d'où modulo p^hon a

$$g_1(T) \equiv \sum_{q=0}^{p^{h-1}} \sum_{r\geq 0} \left\{a(a-1)....\left(a - \left(p^h - 1\right)\right)\right\}^r a(a-1)....(a-q+1)\, T^{rp^h+q} \bmod p^h$$

$$\equiv \sum_{q=0}^{p^h-1} a(a-1)\ldots.(a-q+1)T^q \sum_{r\geq 0} \{a(a-1)\ldots.(a-(p^h-1))\}^r \left(T^{p^h}\right)^r$$
$$\equiv \sum_{q=0}^{p^h-1} a(a-1)\ldots.(a-q+1)T^q \frac{1}{1-a(a-1)\ldots.(a-p^h+1)T^{p^h}}$$

or $\frac{1}{1-a(a-1)\ldots.(a-p^h+1)T^{p^h}} \in H(D)$car

$$\left(1-a(a-1)\ldots\ldots.(a-p^h+1)\right)T^{p^h}=0 \Longleftrightarrow 1=a(a-1)\ldots\ldots.(a-p^h+1)\,T^{p^h}$$
$$\Longleftrightarrow \frac{1}{a(a-1)\ldots.(a-p^h+1)}=T^{p^h}$$

d'où $\frac{1}{|a|\,|a-1|\ldots\ldots\ldots.|a-p^h+1|}=\left|T^{p^h}\right|$

les données suivantes $\begin{cases} |a|\leq 1 \\ \text{et} \\ |i|\leq 1 \qquad \forall i=1,\ldots\ldots\ldots,p^h-1 \\ \text{et} \\ |a-i|\leq \max(|a|,|i|), \end{cases}$

impliquent $|T|\geq 1$ donc $\frac{1}{1-a(a-1)\ldots.(a-p^h+1)T^{p^h}} \in H(D)$

il en résulte alors que $g_1(T)\in H(D)$

Maintenant supposons que $g_m \in H\left(D(0,1)^-\right)$ pour tout $0\leq m\leq k-1$

prouvons que $g_k \in H\left(D(0,1)^-\right)$

on a $f_k(X)=\frac{1}{(k-1)a}\frac{d}{dX}f_{k-1}(X)$

en utilisant la propriété(2) de la transformation de laplace,on obtient:

$$f_k(X) = \frac{1}{(k-1)a} L\left(\frac{d}{dX} X \frac{d}{dX} \tilde{f}_{k-1}(X)\right)$$

aprés avoir appliquer la transformation réciproque de Laplace aux deux membres

de cette égalité ,il résulte

$$\tilde{f}_k(X) = \frac{1}{(k-1)a} \frac{d}{dX} X \frac{d}{dX} \tilde{f}_{k-1}(X) \qquad (1)$$

posons $\tilde{f}_{k-1}(X) = \sum\limits_{n\geq 0} b_n(k-1)\left(e^X - 1\right)^n$ (2)

d'où $\tilde{g}_{k-1}(T) = \sum\limits_{n\geq 0} b_n(k-1)T^n$

on remplaçe (2) dans (1)

$$\begin{aligned}\tilde{f}_k(X) &= \frac{1}{(k-1)a}\left[\frac{d}{dX}\left(X\frac{d}{dX}\sum_{n>0} b_n(k-1)\left(e^X-1\right)^n\right)\right] \\ &= \frac{1}{(k-1)a}\left[\sum_{n>0} A_n\left(e^X-1\right)^n + X\sum_{n>0} B_n\left(e^X-1\right)^n\right]\end{aligned}$$

où $A_n = (n+1)\, b_{n+1}(k-1) + nb_n(k-1)$

et $B_n = (n+1)(n+2)\, b_{n+2}(k-1) + \left((n+1)^2 + n(n+1)\right) b_{n+1} + n^2 b_n(k-1)$

d'où $\tilde{g}_k(T) = \dfrac{1}{(k-1)a}\left[\sum\limits_{n\geq 0} A_n T^n + \log(1+T)\sum\limits_{n\geq 0} B_n' T^n\right]$

on développe $\log(1+T)\sum\limits_{n>0} B_n' T^n$ en série

$$\log(1+T)\sum_{n\geq 0} B_n' T^n = \sum_{n\geq 0}(-1)^{n-1}\frac{T^n}{n}\sum_{n\geq 0} B_n' T^n$$
$$= \sum_{n\geq 0}\left(\sum_{k=0}^{n}\frac{(-1)^{n-k-1}}{n-k}B_k\right)T^n$$

on déduit $g_k(T) = \sum\limits_{n\geq 0} n! A_n T^n + \sum\limits_{n\geq 0} T^n n! \sum\limits_{k=0}^{n}\dfrac{(-1)^{n-k-1}}{n-k}B_k$

$$(4.1)$$

comme $n!\sum\limits_{k=0}^{n}\dfrac{(-1)^{n-k-1}}{n-k}B_k = n!\sum\limits_{k=0}^{n}\dfrac{(n-k-1)!\,k!}{(n-k-1)!\,k!}\dfrac{(-1)^{n-k-1}}{n-k}B_k$

$$= \sum_{k=0}^{n}\frac{(-1)^{n-k-1}}{(n-k)!k!}n!\,(n-k-1)!k!B_k$$

$$= \sum_{k=0}^{n}(-1)^{n-k-1}\binom{n}{k}(n-k-1)!k!B_k$$

donc $g_k(T) = \sum\limits_{n>0} n! A_n T^n + \sum\limits_{n>0} T^n \sum_{k=0}^{n}(-1)^{n-k-1}\binom{n}{k}(n-k-1)!k!B_k$

notons $\sum_{k=0}^{n}(-1)^{n-k-1}\binom{n}{k}(n-k-1)!k!B_k = C_k$

pour prouver que $g_k(T) \in H(D)$ il suffit de prouver que les suites $(n!A_n)_{n\geq 0}$ *et* $(C_n)_{n\geq 0}$ sont p.presque périodiques

$n!A_n = n![(n+1)b_{n+1} + nb_n](k-1) = [(n+1)!b_{n+1} + nn!b_n](k-1)$

or $(n!b_n(k-1))_{n\geq 0}$ sont les coéfficients de la série $g_{k-1}(T) = \sum n!b_n(k-1)T^n$ qui est par hypothése un élément de$H(D)$ donc$(n!b_n(k-1))_{n\geq 0}$ est une suite p présque périodique d'où $((n+1)!b_{n+1}(k-1))_{n\geq 0}$ l'est aussi.

prouvons maintenant que $(nn!b_n)_{n\geqslant 0}$ est p présque périodique $(p.p.p)$

on a $(n!b_n)_{n\geq 0}$ est $p.p.p$ par hypothése

si on arrive à prouver que $(n)_{n\geq 0}$ est $p.p.p$ et aprés démontrer que le produitè de deux suites $p.p.p$ $(u_n), (v_n)$ est aussi une suite $p.p.p$

le résultat $(nn!b_n)$ est $p.p.p$ découle immédiatement .

Pour cette fin on aura besoin des deux propositions suivantes

Proposition1

Soit $(a_n)_{n\geq 0}$ une suite $p.p.p$ de $\mathbb{C}_p$ alors la suite $(|a_n|)_{n\geq 0}$ est bornée.

Preuve:

(a_n) est $p.p.p \Leftrightarrow \forall h \geq 0, \exists N, \exists M$ tq $\forall n \geq N \Longrightarrow |a_{n+M} - a_n| \leq p^{-h}$

considérons l'ensemble $I = \{|a_N|, |a_{N+1}|, |a_{N+2}|, \ldots\ldots\ldots, |a_{N+M-1}|\}$

I est un ensemble fini de Z; donc il est borné i.e $\exists \alpha \in Z$; $\forall i = \overline{N, N+M-1}$, on a $|a_i| \leq \alpha$

si $n = N + M$ on a
$$\begin{aligned} |a_{N+M}| &= |a_{N+M} - a_N + a_N| \\ &\leq |a_{N+M} - a_n| + |a_N| \\ &\leq p^{-h} + \alpha \end{aligned}$$

si $n = N + M + 1$ on a $$\begin{aligned}|a_{N+M+1}| &= |a_{N+M+1} - a_{N+1} + a_{N+1}| \\ &\leq |a_{N+M+1} - a_{N+1}| + |a_{N+1}| \\ &\leq p^{-h} + \alpha\end{aligned}$$

de manière similaire en itérant les calculs d'un pas on trouvera que $(|a_n|)_{n\geq 0}$ est bornée .□

Proposition2

soient (u_n) , (v_n) deux suites de $\mathbb{C}_p$

si (u_n) , (v_n) sont p-presque périodiques

alors leur produit $(u_n v_n)_{n\geq 0}$ est aussi une suite p-presque périodique

Preuve:

(u_n) $p.p.p.$ $\Leftrightarrow \forall h > 0, \exists N_1, \exists M_1$ tel que$\forall n \geq N_1$ $|u_{n+M_1} - u_n| \leq p^{-h}$

(v_n) $p.p.p$ $\Leftrightarrow \forall h > 0, \exists N_2, \exists M_2$ tel que $\forall n \geq N_2$ $|v_{n+M_2} - v_n| \leq p^{-h}$

soit $h > 0$, soit $N = Max(N_1, N_2)$ et $M = M_1 M_2$

pour tout $n > N$ calculons

$$\begin{aligned}|u_{n+M}v_{n+M} - u_n v_n| &= |u_{n+M}v_{n+m} - u_n v_{n+m} + u_n v_{n+m} - u_n v_n| \\ &= |(u_{n+M} - u_n)\, v_{n+M} + u_n\,(v_{n+M} - v_n)| \\ &\leq \max\left(|u_{n+M} - u_n|\,|v_{n+M}|\,, |u_n|\,|v_{n+M} - v_n|\right)\end{aligned}$$

or$|u_{n+M} - u_n| \leq p^{-h}$car M est une période de (u_n) puisque M est multiple de M_1

de même $|v_{n+M} - v_n| \leq p^{-h}$

d'autre part d'aprés la proposition1, $\exists \alpha, \gamma \in Z$ tel que$|v_{n+M}| \leq \alpha$ et $|u_n| \leq \gamma$

d'où

$\max\left(|u_{n+M}-u_n|\,|v_{n+M}|\,,|u_n|\,|v_{n+M}-v_n|\right)\leq \max\left(p^{-h}.\alpha,\gamma\, p^{-h}\right)$

et ainsi on aura $|u_{n+M}v_{n+M}-u_nv_n|\leq \max\left(p^{-h}.\alpha,\gamma\, p^{-h}\right)$

supposons $\alpha>\gamma$,si $\alpha<1$ alors on aura $|u_{n+M}-v_{n+M}|\leq p^{-h}$

sinon nous choisissons le N et M de façon que $\alpha.p^{-h}$ soit inferieur à p^{-h} (ce qui est possible)

d'où $(u_nv_n)_{n\geq 0}$ est *p.p.p* □

démontrons que la suite $(n)_{n\geq 0}$ est *p.p.p*

soit $h>0$, cherchons un rang N et une période M tels que $\forall n\geq N$ on ait

$|n+M-n|\leq p^{-h}$

il suffit de prendre $N=0, M=p^h$, on trouve $(n)_{n\geq 0}$ est *p.p.p*

En conclusion nous avons la suite $(n)_{n\geq 0}$ est *p.p.p* et$(n!b_n)_{n\geq 0}$ est *p.p.p*

d'où grâce à la proposition 2 leur produit $(n.n!b_n)_{n\geq 0}$ est *p.p.p.*

démontrons que la suite $\left(C_n=\sum_{k=0}^{n}(-1)^{n-k-1}(n-k-1)!\binom{n}{k}k!\beta_{k.}\right)_{n>0}$

est *p.p.p.*

la suite $(-1)^{n-k-1}$est *p.p.p.*

et la suite $((n-k-1)!)_{n\geq 0}$ est *p.p.p* car la suite $(n!)_{n\geq 0}$est *p.p.p* prouvons le

soit $h \geq 0$,trouvons$N$ et M tel que $\forall n \geq N$ on a$|(n+M)! - n!| \leq p^{-h}$

nous aurons besoin de la proposition suivante

Proposition3

toute suite convergente est *p.p.p*

Preuve

soit $(a_n)_{n>0}$une suite convergente

or toute suite $(a_n)_{n\geq 0}$ convergente est une suite de Cauchy

i.e $\forall h > 0,\ \exists N_1 \geq 0, \forall n > N_1, \forall m > N_1 \Rightarrow |a_n - a_m| \leq p^{-h}$

démontrons que c'est une suite *p.p.p*

soit $h > 0$ cherchons un rang N et une période M , tel que$\forall n \geq N$ on ait

$|a_n - a_{n+M}| \leq p^{-h}$

posons $N = N_1$; $M = 1$ alors on a $\forall n > N \Rightarrow |u_n - u_{n+M}| \leq p^{-h}$

d'où $(a_n)_{n>0}$ est p.p.p $\square$

nous déduisons de la proposition que la suite $(n!)_{n>0}$ est p.p.p et c'est dû au fait

que

$(n!)_{n\geq 0}$est convergente vers0 dans C_p

♦la suite $\left(\binom{n}{k}\right)_{n\geq 0}$ est aussi p.p.p ,en effet

soit $h > 0$, cherchons un rang N et une période M

tel que $\forall n \geq N$: $\left|\binom{n+M}{k} - \binom{n}{k}\right| \leq p^{-h}$ $\qquad (*)$

supposons qu'on ait $(*)$ et déduisons le N et M

posons

$$\binom{n+M}{k} = P(M) = (n+M)(n+M-1)(n+M-2)\ldots\ldots\ldots\ldots(n+M-k+1)$$
$$= c_k M^k + c_{k-1} M_{k-1} + \ldots\ldots + c_0$$

donc P c'est un pôlynome de variable M de degré k

remarquons que $\binom{n}{k} = n(n-1)\ldots\ldots\ldots\ldots(n-k+1) = P(0) = c_0$

d'où $(*) = |P(M) - P(0)| = \left|c_k M^k + c_{k-1} M^{k-1} + \ldots\ldots\ldots + c_0 - c_0\right|$

$$= \left|c_k M^k + c_{k-1} M^{k-1} + \ldots\ldots\ldots + c_1 M\right|$$

$$= |M| \left|c_k M^{k-1} + c_{k-1} M^{k-2} + \ldots\ldots\ldots + c_1\right|$$

en posant $M = p^{-h}$ et $N = 0$ on aura $(*) \leq p^{-h}$

et donc $\left(\binom{n}{k}\right)_{n\geq 0}$ est p.p.p

♦ $(k!B_k)_{k\geq 0}$ est p.p.p par hypothèse

donc on déduit que le produit $(-1)^{n-k-1}(n-k-1)!\binom{n}{k}k!B_k$ est p.p.p (voir propo.1)

d'où $C_n = \sum_{k=0}^{n}(-1)^{n-k-1}(n-k-1)!\binom{n}{k}k!B_k$ est p.p.p, et ainsi on déduit

que $\sum\limits_{n\geq 0} g_k(T) = \sum\limits_{n\geq 0} n!A_n T^n + \sum\limits_{n\geq 0} n!C_n T^n \in H(D)$ □

Similairement , prouvons par récurrence que $g_{h(k)}(T) \in H(D)$

notons $g_{h(k)}(T) = g_k(T)$

pour $k = 1$

on a $h(1) = X = \log\left(e^X - 1 + 1\right) = \sum\limits_{n>0} \frac{(-1)^n}{n}\left(e^X - 1\right)^n$

$$= \sum_{n\geq 0} \frac{(-1)^n}{n} T^n = \tilde{g}_1(T)$$

d'où $g_1(T) = \sum_{n\geq 0}(-1)^{n-1}(n-1)!T^n$

comme la suite$(-1)^{n-1}(n-1)!$ est convergente donc elle est p.p.p

d'où $g_1(T) \in H(D)$

supposons que la propriété est vraie jusqu'à l'ordre k

calculons l'ordre $k+1$

mais avant ça explicitons $g_k(T)$

on a $X^k = \log(e^X - 1 + 1)^k = (g_{\bar{a}} o g_a(X))^k = [\sum\limits_{n>1} \bar{a}(n) \frac{(g_a(X))^n}{n!}]^k$

$= \sum\limits_{n\geq k} k! B_{n,k}(\bar{a}) \dfrac{g_a(X)^n}{n!} = \sum\limits_{n\geq k} k! B_{n,k}(\bar{a}) \dfrac{T^n}{n!} = \widetilde{G}_k(T)$

d'où $g_k(T) = \sum\limits_{n\geq k} k! B_{n,k}(\bar{a}) T^n$

affirmer que $g_k(T) \in H(D(0,1)^-)$ signifie que $k! B_{n,k}(\bar{a})$ est *p.p.p* i.e $k! s(n,k)$ est *p.p.p*

maintenant passons à $k+1$

$$X^{k+1} = X.X^k = \sum_{n\geq 1} (-1)^{n-1}(n-1)! \frac{(e^X-1)^n}{n!} \sum_{n\geq k} k! B_{n,k}(\bar{a}) \frac{(e^X-1)^n}{n!}$$
$$= \sum_{n\geq 1} (-1)^{n-1}(n-1)! \frac{T^n}{n!} \sum_{n\geq k} k! B_{n,k}(\bar{a}) \frac{T^n}{n!}$$
$$= \sum_{n\geq k+1} (-1)^{n-1}(n-1)! \Psi k! B_{n,k}(\bar{a}) \frac{T^n}{n!}$$
$$= \sum_{m\geq k+1} \sum_{j=0}^{m} (-1)^{m-1-j}(m-1-j)! k! s(j,k) \frac{T^m}{m!} = \widetilde{g}_{k+1}(T)$$

d'où $g_{k+1}(T) = \sum\limits_{m\geq k+1} \sum\limits_{j=0}^{m} (-1)^{m-1-j}(m-1-j)! k! s(j,k) T^m$

dire qu'il est dans $H(D(0,1)^-)$ revient à dire que $\sum\limits_{j=0}^{m} (-1)^{m-1-j}(m-1-j)! k! s(j,k)$ est p.p.p

or c'est une somme finie de produit de suites p.p.p $\square$

Preuve de $ii \Longrightarrow i$

comme $G(T) = \sum_{k>0} k! b_k T^k \in H\left(D(0,1)^-\right)$

ceci implique que $(k! b_k)_{k\geq 0}$ est une suite *p.p.p.*

transformons $G(T)$ en $F(X)$ par le procédé inverse de celui donné dans le théoréme Barsky

$G(T) = \sum_{k\geq 0} k! b_k T^k = \sum_{k>0} b_k k! (e^x - 1)^k$

d'où $\tilde{G}(T) = \sum_{k\geq 0} b_k T^k = \sum_{k>0} b_k (e^x - 1)^k$

et $\tilde{F}(X) = \sum_{k\geq 0} b_k (e^x - 1)^k = \sum_{n\geq 0} a_n \frac{X^n}{n!}$ (1)

calculons a_n :

$\sum_{k\geq 0} b_k (e^x - 1)^k = \sum b_k k! \left(\frac{e^X - 1}{k!}\right)^k$

or $\sum_{k>0} b_k k! \left(\frac{e^X - 1}{k!}\right)^k = g_{v0a}$ où $v(k) = k! b_k$ et $a(n) = \begin{cases} 0 & n = 0 \\ 1 & n \geq 0 \end{cases}$

d'où la comparaison des deux membres de (1) permet de déduire

$a_n = \sum_{\alpha=1}^{n} b_\alpha \alpha! S(n, \alpha)$

prouvons que $F(X) = \sum_{n\geq 0} a_n X^n \in H(D)$

or

$$\begin{aligned}
F(X) &= \sum_{n\geq 0} a_n X^n \\
&= \sum_{n\geq 0} \sum_{k=0}^{n} b_k k! S(n, k) X^n \\
&= \sum_{k\geq 0} \sum_{n\geq k} b_k k! \sum_{j=0}^{k} \frac{(-1)^{k-j}}{k!} \binom{k}{j} j^n X^n \\
&= \sum_{k\geq 0} b_k k! \sum_{j=0}^{k} \lambda_j \sum_{n\geq k} j^n X^n; \text{ où } \lambda_j = \frac{1}{k!} (-1)^{k-j} \binom{k}{j} \\
&= \sum_{k\geq 0} b_k k! \sum_{j=0}^{k} \lambda_j \sum_{n\geq 1} j^n X^n \\
&= \sum_{k} b_k k! \sum_{j=0}^{k} \lambda_j \frac{jX}{1 - JX} \\
&= \sum_{k\geq 0} b_k k! \sum_{j=1}^{k} \lambda_j \frac{jX}{1 - JX} \\
&= \sum_{k>0} \frac{b_k k! X A_k(X)}{(1 - x) \ldots (1 - kX)}
\end{aligned}$$

où $X^k A_k(X) = X^k$car $\left(\begin{array}{c} S(q, k) \text{ cst une suite d'ordre } k \text{ alors } X A_k(X) \text{ est un polynome} \\ \text{d'ordre } k \text{ et au fait que } d^0 A(X) < k \end{array} \right)$

donc on a réussi à écrire $F(X)$ en fonction des coéfficients de $G(T)$ i.e des

$(n!b_n)_{n\geq 0}$

$F(X) = \sum_{n\geq 0} \frac{n!X^n}{(1-X)\ldots\ldots(1-nX)} b_n$

démontrons que $F(X) \in H(D)$ en utilisant la définition d'une fonction analytique sur D

Exploitons le fait que $(n!b_n)_{n\geq 0}$ est p-presque périodique

ie $\forall h > 0, \exists N$ et $\exists M$ tel que $\forall n \geq N \Rightarrow |n!b_n - (n+M)!b_{n+M}| \leq p^{-h}$

ou $n!b_n \equiv (n+M)!b_{n+M} \bmod p^h$

Comme tout multiple d'une période est aussi une période donc Mp^h est période de $(n!b_n)_{n\geq 0}$

soit $n = rMp^h + \gamma \qquad 0 \leq \gamma \leq Mp^h - 1$

$$F(X) = \sum_{n=0}^{N-1} \frac{n!X^n}{(1-X)\ldots\ldots(1-nX)} b_n + \sum_{n\geq N} \frac{n!X^n}{(1-X)\ldots\ldots(1-nX)} b_n$$

pour $n > N$ écrivons le sous la forme $n = N + n'$ tel que $n' = rMp^h + \gamma$; d'où

$n = rMp^h + \alpha \qquad N \leq \alpha \leq N + mp^h - 1$

$$\frac{n!X^n}{(1-X)\ldots\ldots(1-nX)} b_n = \frac{(rMp^h+\alpha)!X^{rMp^h+\alpha}}{(1-X)\ldots\ldots(1-(rMp^h+\alpha)X)} b_{rMp^h+\alpha}$$

modulo p^hnous avons $(Mp^h+n)!b_{Mp^h+n} \equiv n!b_n \bmod p^h$;

$$F(X) = \sum_{r\geq 0} \sum_{\alpha=N}^{N+Mp^h-1} \frac{\alpha! b_\alpha X^{rMp^h+\alpha}}{(1-X)..(1-(Mp^h-1)X)(1-X)..(1-(Mp^h-1)X)..(1-X)..(1-(Mp^h-1)X)..(1-X)..(1-(\alpha-1)X)}$$

i.c$F(X) \equiv \sum_{r\geq 0} \sum_{\alpha=N}^{N+Mp^h-1} \frac{\alpha!X^\alpha}{(1-X)\ldots\ldots 1-(rMp^h+\alpha)X} b_{rMp^h+\alpha}$

d'où $F(X) \equiv F_n(X) \bmod p^h$*où*

$F_n(X) = \sum_{n=0}^{s-1} b_n \frac{n!X^n}{(1-X)..(1-nX)} +$

$+ \sum_{n-s}^{s+Mp^k-1} b_n \frac{n!X^n}{(1-X)..(1-nX)} \sum_{r\geq 0} \frac{X^{rmp^h}}{(1-X)..(1-(mp^h-1)X)^r}$

$F_n(X) = \sum_{n=0}^{s-1} b_n \frac{n!X^n}{(1-X)..(1-nX)} +$

$+\sum_{n=s}^{s+Mp^k-1} b_n \frac{n!X^n}{(1-X)..(1-nX)} \times \frac{(1-X)..\left(1-\left(mp^h-1\right)X\right)}{(1-X)..\left(1-\left(mp^h-1\right)X\right)-X^{mp^h}}$

et donc $F_n(X)$ est une fraction rationnelle sans pôles dans $D(0,1)^-$, d'où le résultat $\square$

4.2 Théorème 2

Soit $X = \sum_{n\geq 1} e_n \frac{Y^n}{n}$ une série de $C_p[[Y]]$ avec $e_1 = 1$ et $|e_n|_p \leq 1$,

Soit $Y = \sum_{n\geq 1} a_n \frac{X^n}{n!}$ la série réciproque de X

et $c \in C_p$ tel que $|c^{p-1} - e_p| \leq p^{-1}$, alors

$Y = \sum_{n\geq 1} b_n \left(e^{cX} - 1\right)^n$ où $b_n = b_n(c)$ avec

i] $b_1 = c^{-1}$

ii] $|b_n|_p \leq |c|_p^{-n}$ si $1 \leq n \leq 2p-1$

iii] $|b_n|_p \leq |c|_p^{-n} r_p^{n-1}$ si $n \geq 2p$ où $r_p = p^{1/(2p-2)}$ si $p \neq 2$ et 3, $r_3 = 3^{2/7}$,

$r_2 = 2^{3/4}$

formellement (i.e pour la topologie T-adique de $C_p[[T]]$) il est toujours possible de trouver $b_n \in C_p, n \in \mathbb{N}$ tel que $Y = \sum_{n\geq 1} a_n \frac{T^n}{n!} = \sum_{n\geq 1} b_n (e^{cT} - 1)^n$ et pour avoir les estimations sur les $|b_n|_p$, on se basera sur le théorème d'inversion de Lagrange Bürmann comme on aura recours à d'autres théorèmes, propositions et corollaires.

Théorème de Lagrange-Bürmann

Soient $T = \sum_{n\geq 0} c_n Y^n$ et $Y = \sum_{n\geq 0} b_n T^n$ deux séries formelles à coéfficients dans un corps supposons que T et Y soient l'une réciproque de l'autre, c'est à dire que

$T(Y(T)) = T$ et $Y(T(Y)) = Y$

supposons en outre que $c_1 \neq 0$

alors le coéfficient de T^ndans la série Y est égal au coéfficient de Y^{n-1} dans le développement en série de Taylor de $\left(\frac{Y}{T}\right)^{n+1} \frac{dT}{dY}$

Preuve:cf[9]

Théorème2

Soit $\exp\left(c\sum_{n\geq 1}\frac{e_n}{n}Y^n\right) = \Pi_{i\geq 1}\left(1-\alpha_i Y^i\right)$ avec

$e_n \in C_p$, $|e_n|_p \leq 1$ et $e_1 = 1$, $c \in C_p - \{0\}$

Soit $c \in C_p - \{0\}$ tel que $|e_p - c^{p-1}|_p \leq p^{-1}$ et $|c|_p \leq 1$, alors :

$i]\alpha_1 = c$,

$ii]$ $|\alpha_n|_p \leq |c|_p$si $1 \leq n \leq 2p-1$,

$iii]$ $|\alpha_n|_p \leq |c|_p .p^{(n/2p-2)-(1/p-1)}$ pour $p \neq 2$ et 3,

$|\alpha_n|_3 \leq |c|_3 .3^{(2n/7)-(1/2)}$ pour $p = 3$,

$|\alpha_n|_2 \leq |c|_2 .2^{(3n/4)-1}$ pour $p = 2$

Preuve :

formellement , on peut toujours trouver $\alpha_i \in C_p$, $i \in \mathbb{N}$ tels que

$$\exp\left(c\sum_{n\geq 1}\frac{e_n}{n}Y^n\right) = \Pi_{i\geq 1}\left(1-\alpha_i Y^i\right) \qquad (01)$$

en dérivant les logarithmes des deux membres de (01) , on obtient

$$\frac{d}{dy}\log(\exp\left(c\sum_{n\geq 1}\frac{e_n}{n}Y^n\right) = \frac{d}{dy}\log(\Pi_{i>1}\left(1-\alpha_i Y^i\right))$$

$$ce_n y^{n-1} = \sum_{i\geq 1} \frac{i\alpha_i Y^{i-1}}{1-\alpha_i Y^i}$$

$c\sum_{n\geq 1} e_n y^{n-1} = \sum_{i\geq 1} i\alpha_i Y^{i-1} \sum_{\gamma\geq 1}(a_i y^i)^{\gamma}$

$c\sum_{n\geq 1} e_n y^{n-1} = \sum_{i\geq 1} i\alpha_i \sum_{\gamma\geq 0} \alpha_i^{\gamma} y^{i(\gamma+1)-1}$

la comparaison des coéfficients de y^{n-1}dans les deux membres de cette égalité mène à déduire que la puissance $n-1$de y s'obtient par le parcours des γ , i tels que $i(\alpha+1)=n$, d'où $ce_n=\sum_{i/n} i\alpha_i^{n/i}$ (02)

Estimations des $|\alpha_i|_p$:

(02) implique que $1/\alpha_1 = c$

$2/\alpha_2 = 2^{-1}(ce_2 - c^2)$, si $p\neq 2$; $|\alpha_2|_p \leq |c|_p \sup(|e_2|_p, |c|_p)$

on a $|e_2|_p \leq 1$,(par donnée)

et $|c|_p \leq 1$,car on a $|c^{p-1}-e_p|_p \leq p^{-1}$

et comme $|c^{p-1}|_p = |c^{p-1}-e_p+e_p|_p$

$\leq \sup(p^{-1},1)=1$

donc $|c^{p-1}|_p \leq 1$,d'où $|c|_p \leq 1$

et ainsi $|\alpha_2|_p \leq |c|_p$

3/ prouvons que $|\alpha_n|_p \leq 1$ pour tout $1\leq n\leq p-1$

supposons que la propriété est vraie pour tout $i\leq n$ et estimons $|\alpha_n|_p$

$$|\alpha_n|_p = |n^{-1}|_p \left|ce_n - \sum_{i/n, i\neq n} i\alpha_i^{n/i}\right|_p$$

$$= |n^{-1}|_p \left|ce_n - c^n - \sum_{i/n,i\neq n, i\neq 1} i\alpha_i^{n/i}\right|_p$$

$$\leq |n^{-1}|_p \sup(|c|_p |e_n|_p \quad , |c|_p^n, \sup\left|i a_i^{n/i}\right|_p (i/n, i\neq n, i\neq 1))$$

or $|n^{-1}|_p = 1$

$|c|_p\,|e_n|_p \leq |c|_p$

$|c^n|_p \leq |c|_p$

et $\left|i\alpha_i^{n/i}\right|_p = |i|_p\,|\alpha_i|_p^{\frac{n}{i}} \leq 1\,|c|_p^{\frac{n}{i}} \leq |c|_p$

car $|\alpha_i|_p \leq |c|_p$ (dû à l'hypothèse de récurrence)

et $|c|_p^{\frac{n}{i}} \leq |c|_p$ puisque $|c|_p \leq 1$

d'où $|\alpha_n|_p \leq 1\sup(\,|c|_p.1,\, |c|_p\,,\, |c|_p)$

et donc $|\alpha_n|_p \leq |c|_p$ pour tout n tel que$1 \leq n \leq p{-}1$ (03)

4/ lorsque $n = p$

$\alpha_p = p^{-1}(ce_p - c^p)$

alors $|\alpha_p|_p = |p^{-1}|_p\,|c|_p\,|e_p - c^{p-1}|_p$

or par hypothèse , on a $|e_p - c^{p-1}| \leq p^{-1}$d'où

$|\alpha_p|_p \leq |p^{-1}|_p\,|c|_p\,p^{-1} = |c|_p$

donc $|\alpha_p|_p \leq |c|_p$ (04)

on déduit aussi par récurrence que $|\alpha_n|_p \leq |c|_p$ pour tout $p-1 \leq n \leq 2p-1$

5/-lorsque $n = 2p$,on aura

$$|\alpha_{2p}|_p = |2p^{-1}|\,\left|ce_{2p} - \alpha_1^{2p} - p\alpha_p^2 - 2\alpha_2^p\right|_p \leq \sup(|c|_p.1, |c|_p\,, p\,|c|_p),\, |c|_p^p\,,)$$

$$\leq p\,|c|_p$$

d'où $|\alpha_{2p}|_p \leq p\,|c|_p$ (05)

de (02) et de l'inégalité ultramétrique, on déduit pour $n > 2p$

$$|\alpha_n|_p \leq \sup(\,|ce_n n^{-1}|_p\ ,\ \sup(\left|in^{-1}\alpha_i^{\frac{n}{i}}\right|_p) \quad \text{telque } 1 \leq i \leq n \text{ et } i/n$$

$$\leq \sup(|ce_n n^{-1}|_p\,, \sup(\sup_{1\leq i\leq n, i/n, i<2p}(\left|in^{-1}\alpha_i^{\frac{n}{i}}\right|_p), \sup_{2p\leq i\leq n, i/n}(\,\left|in^{-1}\alpha_i^{\frac{n}{i}}\right|))$$

$$\leq \sup(|c|_p\,|n^{-1}|_p\,, \sup(\sup_{1\leq i\leq n, i/n, i<2p}(\left|in^{-1}\alpha_i^{\frac{n}{i}}\right|_p), \sup_{2p\leq i\leq n, i/n}(\left|in^{-1}\alpha_i^{\frac{n}{i}}\right|))$$

car $|c_n|_p \leq 1, |c|_p^{n/i} \leq |c|$

or d'aprés les hypothèses de récurrence on a

$\sup_{1\leq i\leq n, i/n, i<2p}(\left|in^{-1}\alpha_i^{\frac{n}{i}}\right|_p \leq \sup|in^{-1}|\,|c|^{\frac{n}{i}} \leq \sup|in^{-1}c|_p$

et donc le tout revient à prouver que

$|\alpha_n|_p \leq \sup(|c|_p\,|n^{-1}|_p\,, \sup(\sup_{1\leq i\leq n, i/n, i<2p}(|in^{-1}c|_p) \quad , \quad \sup_{2p\leq i\leq n, i/n}(\left|in^{-1}\alpha_i^{\frac{n}{i}}\right|))$

et puisque $\sup_{1\leq i\leq n}\ |cin^{-1}|_p = |c|_p\,|n^{-1}|_p$ alors

$|\alpha_n|_p \leq \sup(|cn^{-1}|_p\,, \sup_{2p\leq i\leq n, i/n}\left|n^{-1}i\alpha_i^{n/i}\right|_p)$

on a $|cn^{-1}|_p = |c|_p\,p^{v_p(n)}$

et $\sup_{2p\leq in, i/n}(\ \left|in^{-1}\alpha_i^{\frac{n}{i}}\right| = \sup_{2p\leq i\leq n, i/n}(\ \left|n^{-1}i\alpha_i^{\frac{n}{i}}\right| \leq p^{v_p(\frac{n}{i})}\,|c|_p^{\frac{n}{i}}\,p^{\frac{n}{i}(\frac{i}{2p-2}-\frac{1}{p-1})})$

et ce d'aprés les hypothèses de récurrence:

$|a_i|_p \leq |c|_p\,p^{\frac{i}{2p-2}-\frac{1}{p-1}}$ pour tout $2p < i < n$

d'où $\sup\left|in^{-1}a_i^{\frac{n}{i}}\right|_p = \left|n^{-1}a_i^{\frac{n}{i}}\right|_p = p^{v_p(\frac{n}{i})}\,|a_i|_p^{n/i} \leq p^{v_p(\frac{n}{i})}\,|c|_p^{\frac{n}{i}}\,p^{\frac{n}{i}(\frac{i}{2p-2}-\frac{1}{p-1})}$

à la fin , on déduit que

$|a_n|_p \leq \sup(|c|_p\,p^{v_p(n)},\ |c|_p\,p^{v_p(\frac{n}{i})+\frac{n}{i}(\frac{i}{2p-2}-\frac{1}{p-1})})$

si on arrive à prouver que

a/$v_p(\frac{n}{i}) + \frac{n}{i}(\pi)\ \leq\ \frac{n}{2p-2} - \frac{1}{p-1}$ (06)

b/$v_p(n) \leq \frac{n}{2p-2} - \frac{1}{p-1}$ (07)

alors le résultat sera vite établi

Proposition1

pour tout entier n on a

$$v_p(n) < \left[\frac{\log n}{\log p}\right]$$

Preuve :

écrivons n dans la base p

$n = a_l p^l + a_{l+1} p^{l+1} + \ldots\ldots + a_r p^r$

$v_p(n) = l$

$p^r \leq n < p^{r+1}$

$\log p^r \leq \log n$

donc $r \leq \left[\dfrac{\log n}{\log p}\right]$

comme

$v_p(n) = l < r$, on déduit $v_p(n) < \left[\dfrac{\log n}{\log p}\right]$ $\square$

en combinant (06) et la proposition , on constate que la preuve de (06) se ramène

à la preuve de $\left[\dfrac{\log n}{\log p}\right] \leq \frac{n}{2p-2} - \frac{1}{p-1}$ (08)

avant de procéder de même pour (07) , on constate que

$$(07) \Longleftrightarrow \left[v_p(\tfrac{n}{i}) + \tfrac{n}{i}(\tfrac{i}{2p-2} - \tfrac{1}{p-1}) \leq \tfrac{n}{2p-2} - \tfrac{1}{p-1}\right]$$

$$\Longleftrightarrow \left[v_p(\tfrac{n}{i}) + \tfrac{n}{2p-2} - \tfrac{n}{i}\left(\tfrac{1}{p-1}\right) \leq \tfrac{n}{2p-2} - \tfrac{1}{p-1}\right]$$

$$\Longleftrightarrow \left[v_p(\tfrac{n}{i}) \leq (\tfrac{n}{i} - 1)\tfrac{1}{p-1}\right] \qquad (07)'$$

d'aprés la combinaison de(07) et $(07)'$ et la proposition, la preuve de (07) découle

directement de la preuve de

$$\left[\dfrac{\log \frac{n}{i}}{\log p}\right] \leq (\tfrac{n}{i} - 1)\tfrac{1}{p-1} \qquad (09)$$

i.e la preuve de (06) et (07) revient à la preuve de

$$\text{pour } \; n \geq 2p : \begin{cases} \frac{n}{2p-2} - \frac{1}{p-1} \geq \left[\dfrac{\log n}{\log p}\right] & (\;08) \\ (\frac{n}{i} - 1)\frac{1}{p-1} \geq \left[\dfrac{\log \frac{n}{i}}{\log p}\right] & (09) \end{cases}$$

Preuve de (08)

soient p un nombre premier , $p \neq 2$ et 3 et $x \geq 2p$, étudions la fonction

$$f(x) = \tfrac{x}{2p-2} - \tfrac{1}{p-1} - \left[\frac{\log x}{\log p}\right]$$

on a $f(x) \geq \frac{x}{2p-2} - \frac{1}{p-1} - \frac{\log x}{\log p} = g(x)$

pour $2p \leq x \leq p^2 - 1$, on a

$$\left[\frac{\log 2p}{\log p}\right] \leq \left[\frac{\log x}{\log p}\right] \leq \left[\frac{\log(p^2-1)}{\log p}\right]$$

i.e $\left[\dfrac{\log 2 + \log p}{\log p}\right] \leq \left[\dfrac{\log x}{\log p}\right] \leq \left[\dfrac{\log(p-1) + \log(p+1)}{\log p}\right]$

donc $1 \leq \left[\dfrac{\log x}{\log p}\right] \leq 1$ i.e $\left[\dfrac{\log x}{\log p}\right] = 1$

et alors on aura $f(x) = \frac{x}{2p-2} - \frac{1}{p-1} - 1 \geq 0$

i.e (08) est vraie pour $2p \leq x \leq p^2 - 1$

si $x \geq p^2$ montrons que $g(x) \geq 0$

en effet $g'(x) = \frac{1}{2(p-1)} - \frac{1}{x \log p}$

$g'(x) = 0 \Longleftrightarrow x = \frac{2(p-1)}{\log p} \leq p^2$ si $p \geq 3$

d'autre part , on a $g(p^2) = \frac{p^2}{2p-2} - \frac{1}{p-1} - 2 \geq \frac{p+1}{2} - 2 - \frac{1}{p-1} \geq 0$ si $p \geq 5$

donc (08) est vraie pour $p \neq 2, p \neq 3$ $\forall x \geq 2$

Preuve de (09)

soit p premier ; $p \neq 2, p \neq 3$

étudions la fonction $f(x) = \frac{x}{p-1} - \frac{1}{p-1} - \left[\dfrac{\log x}{\log p}\right]$ pour $x \geq 2$ (car $\frac{n}{i} \geq 2$)

$$f(x) \geq \frac{x-1}{p-1} - \frac{\log x}{\log p} = g(x)$$

pour $2 \leq x \leq p-1$ on a $\dfrac{x-1}{p-1} - \left[\dfrac{\log x}{\log p}\right] = \dfrac{x-1}{p-1}$

de même pour $p \leq x \leq p^2 - 1$,on a

$$\frac{\log p}{\log p} \leq \frac{\log x}{\log p} \leq \frac{\log(p^2-1)}{\log p}$$

i.e $1 \leq \left[\frac{\log x}{\log p}\right] \leq \left[\frac{\log(p-1)+\log(p+1)}{\log p}\right]$

d'où$1 \leq \left[\frac{\log x}{\log p}\right] \leq 1$ $i.e$ $\left[\frac{\log x}{\log p}\right] = 1$

et donc $f(x) = \dfrac{x-1}{p-1} - 1 = \dfrac{x-p}{p-1} \geq 0$

pour $x \geq p^2$ constatons que $g'(x) = \dfrac{1}{p-1} - \dfrac{1}{x\log p}$

$g'(x) = 0 \Longleftrightarrow x = \dfrac{p-1}{\log p} \leq p^2$

$g(p^2) = \dfrac{p^2-1}{p-1} - \dfrac{\log p^2}{\log p} = p + 1 - 2 \geq 0 \ \ \forall p \geq 2,$

et ainsi (08) et (09) sont démontrées pour $p \neq 2, 3$

le cas $p = 2$

$\alpha_4 = 4^{-1}(cc_4 - c^4 - 2\alpha_2^2)$

$|\alpha_4| = |4^{-1}|_2 \, |cc_4 - c^4 - 2\alpha_2^2|_2$

$\leq 2^2 \sup(|cc_4|_2 \, , |c^4|_2 \, , |2\alpha_2^2|_2)$

$\leq 4 \sup(|c|_2 \, , |c|_{2,} \, 2^{-1} \, |c|_2^2)$

$\leq 4 \, |c|_2$

supposons que la propriété $|\alpha_i| \leq 2^{\frac{3i}{4} - \frac{1}{2}} \, |c|_2$ soit vraie pour tout $4 \leq i \leq n$

alors en estimant $|\alpha_n|_2$, on obtient une inégalité similaire au cas $p \neq 2$

i.e $|\alpha|_2 \leq \sup(|c|_2 \, 2^{v_2(n)}, |c|_2 \, 2^{v_2(\frac{n}{i}) + \frac{n}{i}(\frac{3i}{4} - 1)}$

alors la démonstration de $|a_n|_2 \leq |c|_2 \, 2^{\frac{3n}{4} - 1}$ revient à la démonstration de:

$$\begin{cases} \left[\dfrac{\log n}{\log 2}\right] \leq \frac{3n}{4} - 1 & (10) \\ \dfrac{n}{i} - 1 - \left[\dfrac{\log \frac{n}{i}}{\log 2}\right] \geq 0 & (11) \end{cases}$$

Preuve de (10) :

étudions la fonction $f_2(x) = \frac{3x}{4} - 1 - \left[\frac{\log x}{\log 2}\right]$

$f_2(x) \geq \frac{3x}{4} - 1 - \frac{\log x}{\log 2} = g_2(x)$

or $g_2'(x) = \frac{3}{4} - \frac{1}{x \log 2}$

$g_2'(x) = 0 \Longleftrightarrow x = \frac{4}{3\log 2} \leq 3$ et $g_2(4) = 0$

d'où $g_2'(x) \geq 0 \; \forall x \geq 4$ et ainsi (10) est prouvé

Preuve de (11) :

étudions la fonction $f(x) = x - 1 - \left[\frac{\log X}{\log 2}\right]$ pour $x \geq 2$

$f(x) \geq x - 1 - \frac{\log x}{\log 2} = g(x)$

$g'(x) = 1 - \frac{x}{\log 2} \geq 0 \forall x \geq 2$ et $g'(4) = 4 - 1 - 2 \geq 0$ d'où (11) est prouvé

le cas $p = 3$

$n = 3 \quad a_3 = 3^{-1}(ce_3 - c^3)$

d'où $|a_3|_3 = |3^{-1}|_3 \, |c|_3 \, |e_3 - c^2| \leq 3\, |c|_3 \, 3^{-1} = |c|_3$

i.e $|a_3|_3 \leq |c|_3$

$$
\begin{aligned}
n = 6, |a_6| &= |6^{-1}|_3 \, |ce_3 - c^6 - 2a_2^3 - 3a_3^2|_3 \\
&= 3\, |ce_3 - c^6 - 2a_2^3 - 3a_3^2|_3 \\
&\leq 3 \sup(|c|_3 \, , |c|_3 \, , |c|_3 \, , 3^{-1} \, |c|_3) \\
&\leq 3\, |c|_3 \, 3^{2 \cdot \frac{6}{7} - \frac{1}{2}}
\end{aligned}
$$

soit $n \geq 6$ et supposons que la propriété

$|a_\alpha|_3 \leq |c|_3 \, 3^{\frac{2\alpha}{7} - \frac{1}{2}}$ est vraie pour tout $\alpha < n$ et vérifions la pour l'ordre n

en suivant le procédé du cas $p = 2$ et $p \neq 2, 3$ on déduit les formules

$$\begin{cases} \dfrac{2n}{7} - \dfrac{1}{2} \geq \left[\dfrac{\log n}{\log 3}\right] & (12) \\ (\dfrac{n}{i} - 1)\dfrac{1}{2} - \left[\dfrac{\log \frac{n}{i}}{\log 3}\right] \geq 0 & (13) \end{cases}$$

Preuve de (12) :

soit $f_3(x) = \dfrac{2x}{7} - \dfrac{1}{2} - \left[\dfrac{\log x}{\log 3}\right]$

si $6 \leq x \leq 9$ $\left[\dfrac{\log x}{\log 3}\right] = 1$; alors $f_3(x) = \dfrac{2x}{7} - \dfrac{1}{2} - 1 > 0$

si $x > 9$, soit la fonction $g_3(x) = \dfrac{2x}{7} - \dfrac{1}{2} - \dfrac{\log x}{\log 3}$

alors $g_3'(x) = \dfrac{2}{7} - \dfrac{1}{x \log 3}$

$g_3'(x) = 0 \Leftrightarrow x = \dfrac{7}{2 \log 3} \leq 9$

et $g_3(9) = 3 - \frac{1}{2} - 1 \geq 0$ d'où $g_3(x) \geq 0$ $\forall x \geq 9$

et donc $f_3(x) \geq 0$ $\forall x \geq 9$ et (12) est établi

Preuve de (13) :

étudions la fonction $f(x) = \dfrac{x-1}{2} - \left[\dfrac{\log x}{\log 3}\right]$

soit$6 \leq x \leq 9$ $f(x) = \dfrac{x-1}{2} - 1 = \dfrac{x-3}{2} \geq 0$

soit $x \geq 9$ et $g(x) = \dfrac{x-1}{2} - \dfrac{\log x}{\log 3}$

alors $g'(x) = \dfrac{1}{2} - \dfrac{1}{x \log 3}$

d'où $g'(x) = 0 \Longleftrightarrow x = \dfrac{2}{\log 3}$ et $g(9) = \dfrac{9-1}{2} - 2$

d'où $f(x) \geq 0$ et (13) est établi.

Corollaire 1

Soit $\exp\left(c \sum_{n \geq 1} \dfrac{e_n}{n} Y^n\right) = \Pi_{i \geq 1}(1 - \alpha_i Y^i) = 1 + \sum_{n \geq 1} B_n Y^n$,

où $e_n \in C_p - \{0\}$, $|e_n|_p \leq 1, e_1 = 1$, et $c \in C_p - \{0\}$ tel que $|c^{p-1} - e_p|_p \leq p^{-1}$,

alors :

$i]$ $B_0 = 1, B_1 = c$ et $|B_n|_p \leq |c|_p$ si $n \leq 2p - 1$

$ii]$ $|B_n|_p \leq |c|_p \rho_p^n r_p$ pour $n \geq 2p$ où $\rho_p = p^{\frac{1}{2p-2}}$, $r_p = p^{\frac{-1}{p-1}}$, $r_3 = 3^{\frac{2}{7}}$et $r_2 = 2^{-1}$

Preuve :

on a $B_n = \sum_{i((1)>i(2)>...>i(k))} (-1)^k a_{i(1)}a_{i(2)}......a_{i(k)}$

la sommation portant sur les k-uples $(i(1), i(2)........i(k)) \in \mathbb{N}^k$ tels que

$i(1) + i(2) + ... + i(k) = n$, $i(1) > i(2) > .... > i(k) > 0$, $i \leq k \leq n$.

donc d'aprés l'inégalité ultramétrique;

$$|B_n|_p \leq \sup_{1\leq k<n} \left(\left|a_{i(1)}\right|_p, \left|a_{i(2)}\right|_p, ..., \left|a_{i(k)}\right|_p\right) \leq \sup_{1\leq k<n} \left(\left|c^k\right|_p \rho_p^{i(1)+...+i(k)} r_p^k\right)$$

$$= \sup \leq \left(|c|_p^k \rho_p^n r_p^k\right) \leq |c|_p \rho_p^n r_p$$

d'où le résultat □

Corollaire2:

avec les notations du corollaire 1 , les coéfficients $(c_n)_{n\geq 0}$ de

la série$\sum\limits_{n\geq 0} c_n T^n = (\sum\limits_{n\geq 1} B_n T^{n-1})^{-1}$vérifient les inégalités

$i]$$c_0 = c^{-1}$

$ii]$ $|c_n|_p \leq |c|_p^{-1}$ si $1 \leq n \leq 2p-1$

$iii]$ $|c_n|_p \leq |c|_p^{-1} \rho_p^n$ si $n \geq 2p$

Preuve:

l'identité $\sum\limits_{n\geq 0} c_n T^n = (\sum\limits_{n\geq 1} B_n T^{n-1})^{-1}$ implique$\sum\limits_{n\geq 0} c_n T^n . \sum\limits_{n\geq 1} B_n T^{n-1} = 1$

l'identification des coéfficients des deux membres de cette égalité mène au

système d'équations :

$$\begin{cases} c_0 B_1 = 1 \\ c_0 B_2 + c_1 B_1 = 0 \\ ------ \\ c_0 B_{n+1} + c_1 B_n + c_2 B_{n-1} + \dots + c_n B_1 = 0 \end{cases}$$

d'où $c_n = \dfrac{-1}{c}(c_0 B_{n+1} + c_1 B_n + c_2 B_{n-1} + \dots + c_{n-1} B_2)$

alors $|c_n|_p = \left|\dfrac{-1}{c}\right|_p |c_0 B_{n+1} + c_1 B_n + c_2 B_{n-1} + \dots + c_{n-1} B_2|_p$

$$\leq \left|\frac{-1}{c}\right|_p \max(|c_0 B_{n+1}|_p, |c_1 B_n|_p, \dots, |c_{n-1} B_2|_p) \qquad (*)$$

en utilisant la récurrence $|c_n|_p \leq |c|_p^{-1}$ pour tout $n \leq 2p-2$, on obtient

$|c_n|_p \leq \left|\dfrac{-1}{c}\right|_p \max(|c|_p^{-1}|c|_p, |c|_p^{-1}|c|_p, \dots, |c|_p^{-1}|c|_p)$

i.e $|c_n|_p \leq \left|\dfrac{-1}{c}\right|_p \max(1, 1, \dots, 1)$

d'où $|c_n|_p \leq |c|_p^{-1}$ pour tout $n \leq 2p-2$

lorsque $n = 2p-1$

$|c_{2p-1}|_p \leq \left|\dfrac{-1}{c}\right|_p \max(|c|_p^{-1}|B_{2p}|_p, |c|_p^{-1}|c|_p, \dots, |c|_p^{-1}|c|_p)$

$$\leq \left|\frac{-1}{c}\right|_p \max(|c|_p^{-1}|c|_p p^{\frac{2p}{2p-2}-\frac{1}{p-1}}, 1, 1, \dots, 1) = \left|\frac{-1}{c}\right|_p \max(p, 1, 1, \dots, 1)$$

d'où $|c_{2p-1}|_p \leq \left|\dfrac{-1}{c}\right|_p p \leq \left|\dfrac{-1}{c}\right|_p \rho_p^{2p-1}$

et donc le théorème est vrai pour $n = 2p-1$

$iii]$ pour $n \geq 2p$

considérons la série $\sum\limits_{n>0} B_n T^{n-1}$ dans la boule ouverte $B(o, \rho_p^{-1})$

$$\left|\sum_{n>0} B_n T^{n-1}\right|_p \leq \max_{n>1} |B_n T^{n-1}|_p \leq \max(|B_n|_p \rho_p^{-n+1})$$

$$\leq \max(|B_n|_p \rho_p^n p^{\frac{-1}{p-1}} \rho_p^{-n+1})$$

$$\leq \max(|B_n|_p p^{\frac{-1}{p-1}}) \leq |c|_p \qquad (01)$$

retrouvons la borne inférieure de $\left|\sum_{n>0} B_n T^{n-1}\right|_p$

sachant que $\left|\sum_{n>0} B_n T^{n-1}\right|_p = \dfrac{1}{\left|\sum_{n>0} c_n T^{n-1}\right|_p}$

$$\geq \frac{1}{\max_{n>1}\left|c_n T^n\right|_p} \geq \frac{1}{\max_{n>1}\left(|c|_p^{-1}\rho_p^n \rho_p^{-n}\right)} = \frac{1}{|c|_p^{-1}}$$

d'où $\left|\sum_{n>0} B_n T^{n-1}\right|_p \geq |c|_p$ (02)

de (01) et (02) , on déduit $\left|\sum_{n>0} B_n T^{n-1}\right|_p = |c|_p$

dans le disque $B(o,\rho_p)$ on déduit que la série $\sum_{n>1} B_n T^{n-1}$ n'a pas de zéros , d'où

l'existence de la série inverse $(\sum_{n>0} B_n T^{n-1})^{-1}$

i.e la série $(\sum_{n>0} B_n T^{n-1})^{-1}$ est convergente dans ce disque et en outre

$\sup_{T\in B(o,\rho_p)}\left|(\sum_{n>0} B_n T^{n-1})^{-1}\right|_p \leq |c|_p^{-1}$

et donc d'aprés les inégalités de Cauchy les inégalités $iii]$ seront évidentes

Corollaire3

Si $Z(T) = \sum_{n>1} b_n T^n \in C_p[[t]]$ vérifie les inégalités $i], ii], iii]$ du corollaire 1

et si $T(Z) = \sum_{n>1} d_n Z^n$ est la série réciproque de $Z(T)$ i.e $T(Z(T)) = T$

et $(T(Z)) = Z$

alors :

$i]$ $d_1 = c^{-1}$

$ii]$ $|d_n|_p \leq |c|_p^{-n}$ si $n \leq 2p-1$

$iii]$ $|d_n|_p \leq |c|_p^{-n}\ \rho_p^{n-1}$si $n \geq 2p$

Preuve

d'aprés le théorème de Lagrange Bürmann d_n est le coéfficient de T^{n-1} dans le développement en série de Taylor de

$$(\frac{T}{Z})^{n+1}(\frac{dZ}{dT}) = ((\sum_{n>0} B_n T^{n-1})^{-1})^{n+1}(\sum_{n>0} nB_n T^{n-1})$$

puisque les B_n vérifient les inégalités du corollaire 1 alors en posant

$(\sum_{n>0} B_n T^{n-1})^{-1} = \sum_{m>0} c_m T^m$ on obtient

$|c_m|_p \leq |c|_p^{-1} \rho_p^m$ si $m \geq 2p$ et

$|c_m|_p \leq |c|_p^{-1}$ si $1 \leq m \leq 2p-1, \quad c_0 = c^{-1}$ $\qquad (*)$

posons $(\sum_{n>0} B_n T^{n-1})^{-n} = \sum_{m>0} c_m^{(n)} T^m$

alors de $(*)$ on déduit que

$\left|c_m^{(n)}\right| \leq |c|_p^{-n} \rho_p^m$ si $m \geq 2p$ et $\left|c_m^{(n)}\right| \leq |c|_p^{-n}$ si $1 \leq m \leq 2p-1$

en posant $((\sum_{n>0} B_n T^{n-1})^{-1})^{n+1}(\sum_{n>0} nB_n T^{n-1}) = \sum_{m>0} g_m^{(n+1)} T^m$

on alors $\left|g_m^{(n+1)}\right|_p \leq |c|_p^{-n} \rho_p^m$ si $m \geq 2p$

et $\left|g_m^{(n+1)}\right|_p \leq |c|_p^{-n}$ si $m \leq 2p-1$

or d'aprés le théorème de Lagrange Bürmann $d_m = g_{m-1}^{(n+1)}$

d'où $|d_n|_p \leq |c|_p^{-n} \rho_p^{n-1}$ si $n \geq 2p$ et $|d_n|_p |c|_p^{-n}$ si $n \leq 2p-1$

maintenant on est en mesure de démontrer le théorème principal

Preuve

Les deux séries $Z = \exp c \sum_{n>1} c_n \frac{y^n}{n} - 1$, $y = \sum_{n>1} b_n Z^n$ sont l'une est réciproque de l'autre.

D'autre part la série Z vérifie les conditions du théorème 1, alors son développement en série de Taylor vérifie les conditions du corollaire 2 et donc les deux séries Z et y vérifient les conditions du corollaire 3 ,d'où les estimations sur les $|b_n|_p$

Bibliographie

[1] :Y.Amice, Nombres p-adiques , P.U.F, collection sup, Le Mathématicien, Paris 1975

[2] :D.Barsky, Congruences pour les nombres de Schröder, Groupe d'étude d'Analyse ultramétrique, $6^{ème}$année, n°2 1978/1979, 14p

[3] :D.Barsky, Différentielles et Congruences , Groupe d'étude d'Analyse ultramétrique, $4^{ème}$année, n°12 1976/1977, 10p

[4] :D.Barsky, Analyse p-adique et suites classiques de nombres , Institut Galilée, Université Paris13, 1995

[5] :B.benzaghou , Algèbre de Hurwitz et calcul ombral, Prépublication, Institut de Math.U.S.T.H.B, 1999

[6] : L.Carlitz , some properties of Hurwitz series, Duke Math.j.t , 1949, p285.295

[7] :L.Carlitz ,The coefficient of the reciprocal of a series , Duke Math.j.t , 1941, p689.700

[8] :L.Carlitz ,Criteriafor Kummer congruences, Acta Arithmetica (1961)

[9] :L.Comtet, Analyse Combinatoire , tome1 et 2 , P.U.F, collection sup

[10] :D.Parent , Exercices de Théorie de Nombres

[11] G.Polya .G.Szegö, Problems and Theorems in Analysis, Volume2, Springer-Verlag, Berlin Heidlberg NewYork1976

[12] :Ph.Robba,Fonctions analytiques sur les corps valués ultramétriques complets, Astérique n°10, 1973, p.109-220