PROPRIETES p-ADIQUES DE POLYNOMES CLASSIQUES

THESE
présentée à la faculté des sciences, pour obtenir
le grade de docteur ès sciences, par

Maxime ZUBER

UNIVERSITE DE NEUCHATEL
Institut de Mathématiques
Chantemerle 20
2000 NEUCHATEL (Suisse)

IMPRIMATUR POUR LA THÈSE

Propriétés p-adiques de polynômes classiques

de Monsieur Maxime Zuber

UNIVERSITÉ DE NEUCHÂTEL

FACULTÉ DES SCIENCES

La Faculté des sciences de l'Université de Neuchâtel
sur le rapport des membres du jury,

MM. les professeurs A. Robert, U. Suter et
D. Barsky (Paris)

autorise l'impression de la présente thèse.

Neuchâtel, le 3 décembre 1992

Le doyen :

A. Robert

A Claudia, Valentin et Marina

" On n'est pas vieux tant que l'on cherche. "

Jean Rostand

Ô mathématiques sévères, je ne vous ai pas oubliées, depuis que vos savantes leçons, plus douces que le miel, filtrèrent dans mon coeur, comme une onde rafraichissante.

Comte de Lautréamont

Avant-propos

Au printemps 1989, dans le cadre du colloque de l'Institut de mathématiques, Daniel Barsky nous présenta les remarquables propriétés de congruences que vérifient les polynômes de Legendre. Etablies à l'aide de la théorie des groupes formels par T. Honda, les congruences en question trouvaient, dans cet exposé, une preuve élémentaire qui fut le point de départ de nos recherches. Comprise, puis généralisée, la démonstration de Barsky constitua l'outil de premières investigations visant d'autres familles classiques de polynômes.

Au travers des résultats établis pour les polynômes de Tchebychev, de Bernoulli et d'Euler, nous vîmes bientôt nos efforts récompensés. Toutefois, le caractère calculatoire des méthodes utilisées rendaient nos démonstrations particulièrement indigestes. Celles-ci se décantèrent à la lumière de deux théorèmes: *le Lemme de l'équation fonctionnelle* et *le Théorème des accroissements finis p-adiques*. Le premier, emprunté à la théorie des groupes formels, est un résultat purement algébrique (voire combinatoire) de Hazewinkel, qui permet d'impressionnants raccourcis dans certaines manipulations de séries formelles. Comme son nom l'indique, le second énonce le succédané p-adique du principe des accroissements finis (réel). On le doit à Alain Robert. Aussi, les raisonnements exposés dans cette thèse se distinguent-ils souvent par l'alternance d'arguments algébriques et analytiques.

Outre certaines conventions de notation ainsi que la présentation d'éléments d'analyse p-adique et de théorie des groupes formels, le chapitre introductif a pour vocation essentielle de mettre en place et d'énoncer les deux résultats auquels nous venons de faire mention.

Nous consacrons le chapitre 1 à toutes les généralités qui concernent une famille de polynômes satisfaisant à la relation de congruence dite "de Honda". Dans ce contexte, la méthode mise à l'épreuve des polynômes de Legendre par Barsky, prend la forme d'un théorème (du même nom).

Le chapitre 2 traite du cas particulier d'une famille de polynômes d'Appell. Nous y développons une méthode s'appliquant, de façon concluante, aux polynômes de Bernoulli et d'Euler. Sans prétendre à une entière originalité, nous présentons des preuves p-adiques de certains résultats relatifs aux nombres de Bernoulli. Accessoirement, nos calculs nous donnent l'occasion d'améliorer sensiblement un théorème de J.-L. Brylinski sur les polynômes de Gegenbauer.

Le chapitre 3 est complètement dévolu à l'étude des polynômes de Tchebychev de première espèce. L'établissement de la fonction $\arcsin x$ en tant que limite d'une sous-suite particulière de ces polynômes en constitue le point fort.

Finalement, l'approche que nous faisons, dans le chapitre 4, des polynômes de Legendre par l'intermédiaire de ceux de Coster, apporte peut-être un nouvel éclairage aux travaux de Honda , Landweber et Yui.

La présente thèse a vu le jour grâce à un travail d'équipe. Toute son élaboration a bénéficié de l'émulation du Groupe d'analyse ultramétrique de l'Université de Neuchâtel. Je tiens à exprimer toute ma gratitude à Alain Robert, mon directeur de thèse. Ses précieux conseils, ses encouragements inconditionnels et sa disponibilité de tout instant m'ont permis d'effectuer quatre années de recherche dans des conditions optimales. Je n'oublierai pas son art d'agrémenter les pauses-café de petits exposés mathématiques, dont chacun valait bien une demi-journée de lecture attentive.

Mes remerciements vont aussi à Christian Vonlanthen: l'ami avec lequel j'ai commencé mes études et partagé quatre années de collaboration fructueuse, au cours desquelles je l'ai vu jouer les rôles d'auditeur, de correcteur, de conseiller et même parfois celui de psychanalyste.

Ma reconnaissance s'adresse particulièrement à Daniel Barsky, tout d'abord pour m'avoir inspiré le sujet de cette thèse, puis pour son invitation à présenter mes premiers résultats au Groupe parisien d'analyse ultramétrique et finalement pour avoir fonctionné en tant que membre du jury.

Je remercie également Ueli Suter de sa sollicitude et de l'intérêt qu'il a manifesté pour mon travail ainsi que Akimou Osse pour les indications bibliographiques et les remarques de styles qu'il m'a dispensées.

Je dédie cette thèse à Claudia, mon épouse. Sans sa compréhension et son abnégation, rien de tout ceci n'aurait été possible. Qu'elle trouve ici l'expression de ma très profonde gratitude.

Moutier, le 5 septembre 1992

Maxime Zuber

The theory of Groups is a branch of mathematics in which one does something to something and compares the result obtained from doing the same thing to something else, or something else to the same thing.

J. R. Newmann (The World of Mathematics)

INTRODUCTION

Quelques principes d'analyse p-adique

Soit p un nombre premier; en accord avec les notations de Y. Amice [2], $\mathbf{Z}_p$ désigne l'anneau topologique des entiers p-adiques, $\mathbf{Q}_p = Frac(\mathbf{Z}_p)$, le corps des nombres p-adiques et $\mathbf{C}_p$, le complété de la clôture algébrique de $\mathbf{Q}_p$. La valeur absolue sur $\mathbf{Z}_p$, $\mathbf{Q}_p$ et $\mathbf{C}_p$ est normalisée par $|p| = \frac{1}{p}$. Nous rappelons[1] ici, quelques principes fondamentaux qu'entraîne le caractère ultramétrique de cette valeur absolue.

Considérons une suite $(a_n)_{n\geq 0}$ dans K, corps valué ultramétrique complet. Le cas typique $K = \mathbf{C}_p$ va nous intéresser.
La suite $(a_n)_{n\geq 0}$ est convergente si et seulement si $|a_{n+1} - a_n| \to 0$ lorsque $n \to \infty$. De même, la série $\sum_{n\geq 0} a_n$ converge si et seulement si son terme général a_n tend vers 0, et si ceci est le cas, alors

$$\left|\sum_{n\geq 0} a_n\right| \leq \sup |a_n| = \max |a_n|.$$

Il en résulte que la série de puissances $f = \sum_{n\geq 0} a_n x^n$ possède un rayon de convergence r_f caractérisé par le fait que

$$\sum_{n\geq 0} a_n x^n \text{ converge pour } |x| < r_f \text{ et diverge pour } |x| > r_f.$$

Ce rayon de convergence est donné par

$$0 \leq r_f = \sup\{t : |a_n t^n| \to 0\} \leq \infty$$

ou par la formule de Hadamard

$$r_f = \frac{1}{\limsup |a_n|^{1/n}}.$$

Par exemple, la série de puissances

$$\log(1+x) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n$$

[1] Cf. par exemple [2], [33], [36].

converge pour $|x| < r_{log} = 1$, tandis que le rayon de convergence r_e de la série exponentielle

$$\exp(x) = \sum_{n\geq 0} \frac{x^n}{n!}$$

est égal à $r_e = |p|^{\frac{1}{p-1}}$.

Si le coefficient général a_n de la série de puissances $f = \sum_{n\geq 0} a_n x^n$ tend vers 0 lorsque $n \to \infty$ (on dit dans ce cas que $f \in \mathbf{C}_p\{x\}$ l'anneau des séries formelles restreintes), alors la norme uniforme $\|f\|$ de f est donnée par

$$\|f\| := \sup_{|x|\leq 1} |f(x)| = \max_{n\geq 0} |a_n|.$$

Le théorème des accroissements finis p-adiques, résultat dû à A. Robert [32], occupe une position centrale dans cette thèse, eu égard au nombre de simplifications techniques qu'il permet.

Théorème des accroissements finis p**-adiques.** - *Pour une série formelle restreinte* $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbf{C}_p\{x\}$, *on a*

$$|f(x) - f(y)| \leq \|f'\| \cdot |x - y|,$$

dès que

$$|x - y| \leq r_e = |p|^{\frac{1}{p-1}}.$$

Preuve[2].- Puisque $a_n \to 0$ lorsque $n \to \infty$ et que $|n| \leq 1$ pour tout entier n, on a

$$\|Df\| := \|f'\| = \sup |na_n| \leq \sup |a_n| = \|f\|.$$

L'opérateur de dérivation, $D : f \to f'$, est de norme 1. La formule de Taylor, centrée en $x = y - t$, s'écrit alors

$$f(x + t) = f(x) + f'(x) \cdot t + \cdots = \sum_{n\geq 0} D^n f(x) \cdot \frac{t^n}{n!}.$$

Ainsi

$$f(x + t) - f(x) = (e^{tD} - 1)f(x) = t \cdot \left(\frac{e^{tD} - 1}{tD}\right)(Df(x)) = t \cdot (Tf')(x).$$

On doit établir que l'opérateur

$$T := \frac{e^{tD} - 1}{tD} = \sum_{n\geq 1} \frac{t^{n-1}}{n!} D^{n-1},$$

[2]Nous reproduisons ici la preuve de [32].

bien défini sur $\mathbf{C}_p\{x\}$, a une norme ≤ 1. Pour $|t| \leq r_e$, on vérifie que

$$|t|^{n-1} \leq r_e^{n-1} \leq |p|^{\frac{n-S_p(n)}{p-1}} = |n!|,$$

de sorte que $|t^{n-1}/n!| \leq 1$ dans le disque fermé $|t| \leq r_e$. De plus, si $f \in \mathbf{C}_p\{x\}$ a tous ses coefficients entiers, alors $\|f\| \leq 1$ et il en est de même de $g = f'$. Ainsi

$$\|D^{n-1}g\| \leq 1, \quad \|D^{n-1}g\| \to 0,$$

ce qui achève la démonstration.
Alternativement, puisque

$$\frac{1}{k!}D^k x^n = \binom{n}{k} x^{n-k}, \quad (n \geq 0),$$

on en déduit $\|D^k/k!\| \leq 1$ et

$$\left\| \frac{t^{n-1}}{n!} D^{n-1} \right\| = \left\| \frac{t^{n-1}}{n} \cdot \frac{D^{n-1}}{(n-1)!} \right\| \leq \left| \frac{t^{n-1}}{n} \right|.$$

Pour montrer que $\|T\| \leq 1$, il suffit de montrer

$$\left| \frac{t^{n-1}}{n} \right| \to 0 \text{ et } \left| \frac{t^{n-1}}{n} \right| \leq 1.$$

L'inégalité pour $n = p$ requiert déjà $|t| \leq r_e$ et si elle est satisfaite, toutes les conditions sont remplies! ∎

Remarque.- L'application de ce théorème à la fonction $f(x) = x^p$, en $x = 1$, montre que

$$|(1+t)^p - 1| \leq |t| \cdot |p| \text{ dès que } |t| \leq r_e.$$

Mais cette inégalité doit être remplacée par

$$|(1+t)^p - 1| \leq |t|^p \text{ (avec égalité si } p = 2),$$

lorsque $r_e < |t| \leq 1$. En effet, il existe $s(t) \in \mathbf{Z}_p[t]$ tel que

$$(1+t)^p = 1 + t^p + pts(t);$$

si bien que, pour $r_e < |t| \leq 1$, on a

$$|(1+t)^p - 1| = \max\{|t^p|, |p| \cdot |s(t)|\} = |t|^p,$$

(avec égalité si $p = 2$, car dans ce cas, $s(t) = 1$).
Ceci montre que le rayon r_e de convergence de la série exponentielle limite le domaine de validité du théorème des accroissements finis p-adiques.

Eléments de théorie des groupes formels

Conjointement aux quelques principes élémentaires d'analyse p-adique exposés plus haut, nous utilisons des techniques purement algébriques empruntées à la théorie des groupes formels. Il convient donc de citer brièvement les définitions et exemples fondamentaux de cette théorie. A cet effet, nous nous inspirons du chapitre I du livre, très complet, de M. Hazewinkel [18] traitant du sujet[3].

Dans la suite, A désigne un anneau commutatif à élément unité $1 \neq 0$.

Définition. *Une* loi de groupe formel *de dimension* 1, *sur l'anneau* A, *est une série formelle* $F(x,y) \in A[[x,y]]$, *telle que*

a) $F(x,y) \equiv x + y$ *mod degré* 2 ;

b) $F(F(x,y),z) = F(x,F(y,z))$.

Si de plus, $F(x,y) = F(y,x)$, *alors* $F(x,y)$ *est une loi de groupe formel commutatif.*

De la propriété *a*), il suit que

$$F(x,0) = x \quad \text{et} \quad F(0,y) = y.$$

D'autre part, on peut facilement démontrer l'existence d'une unique série formelle

$$i(x) \equiv -x \ mod \ \deg 2,$$

telle que

$$F(x,i(x)) = 0.$$

Remarque.- Il faut voir dans le concept de loi de groupe formel, un procédé qui permet la construction de "vrais" groupes. A titre illustratif, considérons un anneau local A d' idéal maximal M. La filtration M-adique

$$A \supset M \supset M^2 \supset \ldots$$

munit A d'une structure d'anneau topologique. Supposons que $\bigcap_n M^n = \{0\}$ et qu'en plus, A soit complet. Dans ces conditions, $F(x,y)$ devient série convergente dès que $x, y \in M$. Ainsi, F définit une nouvelle loi de groupe sur M.
Dans un langage catégorique, cette "machine" de construction définit un *foncteur covariant* F : *le groupe formel* associé à la loi de groupe formel $F(x,y)$.
Nous commettrons l'abus, de ne pas opérer la distinction entre le groupe formel F et la série formelle $F(x,y)$ qui lui est associée.

[3] La lecture de l'appendice 2 (p. 354-379) de [31] est également à conseiller.

Exemples de lois de groupe formel

a) $G_a(x,y) := x + y$: la loi de groupe formel additive;

b) $G_m(x,y) := x + y + xy$: le groupe formel multiplicatif, pour lequel $1 + G_m(x,y) = (1+x)(1+y)$;

c) La formule d'addition de la tangente hyperbolique donne lieu à la loi de groupe formel

$$F(x,y) = \frac{x+y}{1+xy} = \tanh\left(\tanh^{-1}(x) + \tanh^{-1}(y)\right).$$

Définition. *Soit $F(x,y)$ et $G(x,y)$ deux lois de groupes formels sur A. Un* homomorphisme $F(x,y) \to G(x,y)$ *est une série formelle $h(x) = h_1x + h_2x^2 + \cdots \in A[[x]]$, sans terme constant, telle que*

$$h(F(x,y)) = G(h(x), h(y)).$$

L'homomorphisme $h(x) : F(x,y) \to G(x,y)$ est un isomorphisme, *s'il existe un homomorphisme $k(x) : G(x,y) \to F(x,y)$ tel que*

$$h(k(x)) = x = k(h(x)).$$

*Si, de plus, $h_1 = 1$, alors $h(x)$ est qualifié d'*isomorphisme strict. *Deux lois de groupes formels sont dites* (strictement) isomorphes *s'il existe entre elles un isomorphisme (strict).*

Remarque.- On établit aisément que l'homomorphisme $h(x) = h_1x + h_2x^2 + \cdots$ est un isomorphisme, si et seulement si h_1 appartient au groupe $A^\times := U(A)$ des unités de A.

Exemple.- Si l'on considère, sur $A = \mathbf{Q}$, les séries formelles

$$E(x) := \exp(x) - 1 = \sum_{n\geq 1} \frac{x^n}{n!},$$

$$L(x) := \log(1+x) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n,$$

alors

$$E(x) : G_a(x,y) \to G_m(x,y)$$

et

$$L(x) : G_m(x,y) \to G_a(x,y)$$

définissent deux isomorphismes stricts inverses l'un de l'autre. Autrement dit, les groupes formels additifs et multiplicatifs sont strictement isomorphes sur $A = \mathbf{Q}$

(remarquons que ce n'est plus le cas, par exemple si $A = K$ est un corps de caractéristique non nulle).

Nous avons souligné, plus haut, l'importance fondamentale que revêt *le théorème des accroissements finis p-adiques* dans notre propos. Parallèlement, *le lemme de l'équation fonctionnelle* de M. Hazewinkel [18] constitue notre second puissant outil. Il permet d'impressionnants raccourcis dans les manipulations formelles tendant à établir certains résultats d'intégralité, tels les théorèmes de Dieudonné-Dwork (proposition 1.2.2) et de Barsky (théorème 1.3.1).

Lemme de l'équation fonctionnelle de Hazewinkel. *Soient A un sous-anneau d'un anneau K, I un idéal de A, p un nombre premier, q une puissance de p, $\sigma : K \to K$ un homomorphisme d'anneaux et $(s_i)_{i\geq 1}$ une suite d'éléments de K. Supposons que ces "ingrédients" remplissent les conditions suivantes*

1) $p \in I$;

2) $s_i I \subset A$ *pour tout* $i \geq 1$;

3) $\sigma(a) \equiv a^q \bmod I$ *pour tout* $a \in A$;

4) $I^r b \subset I \Rightarrow I^r \sigma(b) \subset I$ *pour tout* $b \in K$ *et tout* r *entier.*

Pour $g(x) \in A[[x]]$, convenons de noter $f_g(x)$ la série formelle solution de l'équation fonctionnelle

$$f_g(x) = g(x) + \sum_{i\geq 1} s_i \sigma_*^i f_g\left(x^{q^i}\right).$$

(où $\sigma_*^i f(x) = \sum_{n\geq 1} \sigma^i(a_n) x^n$ si $f(x) = \sum_{n\geq 1} a_n x^n$).
Soient encore

$$g(x) = \sum_{n\geq 1} g_n x^n \in A[[x]], \text{ avec } g_1 \in A^\times \quad \text{et} \quad h(x) = \sum_{n\geq 1} h_n x^n \in A[[x]].$$

On a alors

(i) $F_g(x,y) := f_g^{-1}(f_g(x) + f_g(y)) \in A[[x,y]]$ *et donc, $F_g(x,y)$ définit une loi de groupe formel sur A ;*

(ii) $f_y^{-1}(f_h(x)) \in A[[x]]$;

(iii) Il existe $k(x) \in A[[x]]$ telle que $f_g(h(x)) = f_k(x)$;

(iv) Soit $\alpha(x) \in A[[x]]$, $\beta(x) \in K[[x]]$ et $r > 0$; alors
$\alpha(x) \equiv \beta(x) \bmod I^r A[[x]]$ si et seulement si $f_g(\alpha(x)) \equiv f_g(\beta(x)) \bmod I^r A[[x]]$.

Preuve.- Cf. [18], p. 9-15.

Remarque.- L'équation fonctionnelle

$$f_g(x) = g(x) + \sum_{i\geq 1} s_i \sigma_*^i f_g\left(x^{q^i}\right),$$

se traduit par une formule de récurrence pour les coefficients de sa solution $f_g(x)$. Plus précisément, si

$$g(x) = \sum_{n\geq 1} g_n x^n \quad \text{et} \quad f_g(x) = \sum_{n\geq 1} f_n x^n.$$

alors

$$f_n = \begin{cases} g_n \text{ si } q \text{ ne divise pas } n; \\ g_n + \sum_{i=1}^{r} s_i \sigma^i\left(f_{n/q^i}\right) \text{ si } n = mq^r \text{ avec } r \geq 1 \text{ et } q \text{ ne divisant pas } m. \end{cases}$$

Définition. *On appelle "type" de l'équation fonctionnelle, la donnée des ingrédients* K, A, I, q, $(s_i)_{i\geq 1}$, σ *apparaissant dans l'énoncé du lemme de l'équation fonctionnelle. Par abus de langage, on dit qu'une série formelle est du type de l'équation qu'elle vérifie.*

Corollaire. *Si* $f_1(x)$ *et* $f_2(x)$ *sont deux séries formelles de même type et si, de plus* $f_1'(0)$, $f_2'(0) \in A^\times$, *alors*

$$h = f_2^{-1} \circ f_1 \; : \; F_1(x,y) \to F_2(x,y)$$

(où $F_i(x,y) := f_i^{-1}(f_i(x) + f_i(y))$ *), est un isomorphisme de groupes formels, qui est strict si et seulement si* $f_2'(0) = f_1'(0)$.

Preuve.- Le point (ii) du *lemme de l'équation fonctionnelle* établit que $h(x) \in A[[x]]$. Comme $f_1'(0)$ et $f_2'(0)$ sont des unités de A, h est inversible, au sens de la composition, dans $A[[x]]$. En outre

$$\begin{aligned} h \circ F_1(x,y) &= f_2^{-1} \circ f_1 \circ f_1^{-1}(f_1(x) + f_1(y)) \\ &= f_2^{-1}(f_1(x) + f_1(y)) \\ &= F_2(h(x), h(y)). \end{aligned}$$

Finalement $h(x) \equiv x \; mod \; \deg 2$, si et seulement si $f_2'(0)^{-1} \cdot f_1'(0) = 1$. ∎

Bien que *le lemme de l'équation fonctionnelle* soit le fait de M. Hazewinkel, il convient de citer la contribution (parallèle et indépendante) de T. Honda. Dans son article: *"On the theory of commutative formal groups"* [20], T. Honda développe

une théorie basée sur des méthodes non commutatives de calcul de séries formelles. Il y démontre alors, pour le cas particulier d'un corps K de caractéristique 0 muni d'une valuation discrète, des résultats correspondant aux quatre points du *lemme de l'équation fonctionnelle*. Le mérite de M. Hazewinkel est d'avoir su établir un énoncé tout à fait général et, partant, d'application plus vaste.

Pour notre part, nous n'étudierons qu'un type bien particulier d'équation fonctionnelle (dont nous empruntons la dénomination à T. Honda) : le type $p - T$, qui fait l'objet du chapitre I.

Notation.- Lorsqu'il s'agira, dans la suite, de nous référer au "*Lemme de l'équation fonctionnelle*", nous le ferons à l'aide du sigle abréviatif: "LEF".

TABLE DES MATIÈRES

C'est la grande généralisation, limitée par un un heureux cas particulier, qui fait la conception fructueuse.

A. N. Whitehead

Chapitre 1

LES CONGRUENCES DE HONDA

1.1 Le type $p - T$

Dans toute la suite, les ingrédients I, q, $(s_i)_{i\geq 1}$, intervenant dans l'énoncé du LEF seront fixés ainsi

$$I = pA\,,\ q = p\,,\ s_1 = \frac{1}{p}\,,\ s_i = 0 \text{ pour tout } i \geq 2.$$

Définition 1.1.1 *Une série formelle $f_g(x) \in K[[x]]$ est* de type $p - T$ *(sur A), si elle vérifie l'équation fonctionnelle*

$$f_g(x) - \frac{1}{p}\sigma_* f_g(x^p) = g(x), \tag{1}$$

pour une certaine série formelle donnée $g(x) \in A[[x]]$.

Soit maintenant $A = \mathbf{Z}_{(p)}$, $K = \mathbf{Q}$ et $\sigma = id_K$. Considérons les séries formelles

$$h(x) = x,$$

$$\ell(x) = \begin{cases} \sum_{(n,p)=1} \frac{(-1)^{n+1}}{n} x^n & \text{si } p \text{ est impair;} \\ \sum_{n\ impair} \frac{1}{n}(x^n - x^{2n}) & \text{si } p = 2. \end{cases}$$

Proposition 1.1.1 *Si $f_\ell(x)$ et $f_h(x)$ désignent les solutions de l'équation fonctionnelle (1) de type $p - T$ avec second membre égal à $\ell(x)$, respectivement $h(x)$, alors*

$$f_\ell(x) = \log(1 + x)$$

et

$$f_h(x) = H(x) := \sum_{n\geq 0} \frac{x^{p^n}}{p^n}.$$

Preuve.- On a

$$\log(1+x) = \sum_{(n,p)=1} \frac{(-1)^{n+1}}{n} x^n + \sum_{n\geq 1} \frac{(-1)^{np+1}}{np} x^{np}, \tag{2}$$

$$\frac{1}{p}\log(1+x^p) = \sum_{(n,p)=1} \frac{(-1)^{n+1}}{np} x^{np} + \sum_{n\geq 1} \frac{(-1)^{np+1}}{np^2} x^{np^2}. \tag{3}$$

En effectuant la soustraction (2)−(3), on obtient

$$\begin{aligned}\log(1+x) - \frac{1}{p}\log(1+x^p) &= \sum_{(n,p)=1} \frac{(-1)^{n+1}}{n} x^n + \sum_{(n,p)=1} \frac{(-1)^{np+1} - (-1)^{n+1}}{np} x^{np} \\ &+ \sum_{n\geq 1} \frac{(-1)^{np^2+1} - (-1)^{np+1}}{np^2} x^{np^2}.\end{aligned}$$

Si p est impair, les coefficients des deux dernières séries du membre de droite de l'égalité ci-dessus s'annulent, de sorte que

$$\log(1+x) - \frac{1}{p}\log(1+x^p) = \sum_{(n,p)=1} \frac{(-1)^{n+1}}{n} x^n = \ell(x).$$

Par ailleurs, si p=2, alors

$$\log(1+x) - \frac{1}{2}\log(1+x^2) = \sum_{n\,impair} \frac{x^n}{n} - 2\sum_{n\,impair} \frac{x^{2n}}{2n} = \ell(x).$$

Finalement, pour la série formelle $H(x)$, on a

$$H(x) - \frac{1}{p}H(x^p) = \sum_{n\geq 0} \frac{x^{p^n}}{p^n} - \frac{1}{p}\sum_{n\geq 0} \frac{x^{p^{n+1}}}{p^n} = x = h(x).$$

■

La série formelle $L(x) := \log(1+x)$, qui joue bien plus que le rôle de simple exemple dans la suite de notre propos, engendre le groupe formel multiplicatif, par la formule

$$G_m(x,y) = L^{-1}(L(x) + L(y)).$$

Cette propriété motive la définition suivante.

Définition 1.1.2 *Si un groupe formel $F(x,y) \in A[[x,y]]$ et une série formelle $f(x) \equiv x$ mod* deg 2 *sont tels que*

$$F(x,y) = f^{-1}(f(x) + f(y)),$$

alors on dit que $f(x)$ est le logarithme *du groupe formel $F(x,y)$.*

Ainsi, le point (i) du LEF fournit, dans un même temps, le logarithme et la méthode de construction d'un groupe formel sur un anneau particulier A.

1.2 Applications du LEF relatives au type $p-T$

Les séries formelles $H(x)$ et $L(x)=\log(1+x)$ sont toutes deux de type $p-T$ et donnent lieu, en application du point (i) du LEF, aux groupes formels

$$G_m(x,y)=L^{-1}(L(x)+L(y)) \text{ et } H(x,y)=H^{-1}(H(x)+H(y)).$$

L'application du point (ii) du LEF montre alors que

$$L^{-1}(H(x))=f_i^{-1}(f_h(x))=\exp(H(x))-1\in \mathbf{Z}_{(p)}[[x]],$$

ce qui établit la proposition suivante.

Proposition 1.2.1 *L'exponentielle de Artin-Hasse*[1]

$$E_p(x):=\exp\left(x+\frac{x^p}{p}+\frac{x^{p^2}}{p^2}+\cdots\right),$$

a ses coefficients dans l'anneau $\mathbf{Z}_{(p)}$. *De plus*

$$E_p(x)-1\ :\ H(x,y)\longrightarrow G_m(x,y),$$

est un isomorphisme strict de groupes formels.

En vue d'illustrer, une fois encore, la puissance simplificatrice du LEF, démontrons une version particulière d'un autre "résultat d'intégralité": le théorème de Dieudonné-Dwork[2]

Proposition 1.2.2 (Théorème de Dieudonné-Dwork) *Soit* $A=\mathbf{Z}_p[[t]]$, $K=Frac(A)$ *et l'endomorphisme* σ *de* K *qui envoie* t *sur* t^p. *Alors pour*

$$F(x)=1+a_1x+a_2x^2+\ldots\in K[[x]];$$

série formelle à coefficients dans K, *les propriétés suivantes sont équivalentes*

(i) $$F(x)\in A[[x]],$$

(ii) $$\frac{F(x)^p}{\sigma_*F(x^p)}\in 1+pxA[[x]].$$

[1] Telle que définie dans [16].

[2] La version la plus générale est énoncée dans [18].

Preuve.- Les ingrédients A, K, σ (et comme fixés initialement $I = pA$, $s_1 = \frac{1}{p}$, $s_i = 0$ pour $i > 1$) satisfont aux hypothèses du LEF. Comme σ n'affecte pas les coefficients de la série formelle $L(x) = \log(1+x)$, celle-ci est de type $p - T$ sur A. Autrement dit

$$L(x) = f_\ell(x).$$

Supposons que $F(x) \in A[[x]]$. Par le point (iii) du LEF, il existe une série formelle $k(x) \in A[[x]]$, sans terme constant, telle que

$$f_\ell(F(x) - 1) = f_k(x).$$

Ceci se traduit par

$$L(F(x) - 1) - \frac{1}{p}\sigma_* L(F(x^p) - 1) = k(x);$$

ou encore, puisque $\sigma \in End(K)$, par

$$p\log(F(x)) - \log(\sigma_* F(x^p)) = pk(x) \in pA[[x]].$$

En prenant l'exponentielle de cette dernière expression, on obtient

$$\frac{F(x)^p}{\sigma_* F(x^p)} \in 1 + pxA[[x]];$$

ce qui établit l'implication $(i) \Rightarrow (ii)$.

Réciproquement, si l'on admet que

$$\frac{F(x)^p}{\sigma_* F(x^p)} \in 1 + pxA[[x]],$$

alors

$$p\log(F(x)) - \log(\sigma_* F(x^p)) = pk(x) \in pA[[x]],$$

où $k(x) \in A[[x]]$ est une série formelle sans terme constant. Il s'ensuit que

$$\log(F(x)) - \frac{1}{p}\log(\sigma_* F(x^p)) = k(x);$$

autrement dit, la série formelle

$$\log(F(x)) = L(F(x) - 1) = f_\ell(F(x) - 1)$$

est de type $p - T$ sur A. Ainsi $f_\ell(F(x) - 1) = f_k(x)$ et, de l'application du point (ii) du LEF, il ressort alors que

$$F(x) - 1 = f_\ell^{-1}(f_k(x)) \in A[[x]],$$

donc, $F(x)$ a bien ses coefficients dans A. ∎

1.3 Le théorème de Barsky

Soient p un nombre premier, $A = \mathbf{Z}_p[[t]]$, $I = pA$, $K = Frac(A)$, $q = p$, $s_1 = \frac{1}{p}$, $s_i = 0$ pour tout $i \geq 2$ et l'endomorphisme σ de K qui envoie t sur t^p.

Ces ingrédients qui, de façon évidente, remplissent les conditions énoncées dans le LEF, resteront ainsi fixés dans tout ce qui suit.

L'usage a été jusqu'ici, de résoudre l'équation fonctionnelle

$$f_g(x) - \frac{1}{p}\sigma_* f_g(x^p) = g(x).$$

relative à une série formelle donnée $g(x) \in A[[x]]$ et d'appliquer les différentes conclusions du LEF à la solution obtenue $f_g(x) \in K[[x]]$.

Renversons le raisonnement, en partant cette fois d'une série formelle "logarithmique"

$$f(x) = \sum_{n\geq 1} \frac{a_n}{n} x^n \in K[[x]].$$

La question se pose alors, de savoir quelles propriétés doivent posséder les coefficients a_n, pour que la série formelle $f(x)$ soit de type $p - T$. Le théorème suivant apporte un élément de réponse.

Théorème 1.3.1 (Barsky [4]) *Pour une série formelle*

$$f(x) = \sum_{n\geq 1} \frac{a_n}{n} x^n \in K[[x]],$$

les propositions suivantes sont équivalentes

(i) $f(x)$ *est de type* $p - T$;

(ii) $a_n \in A$ *si* p *ne divise pas* n *et*
$a_{np}(t) \equiv a_n^{\sigma}(t) = a_n(t^p) \ mod\ npA$, *pour tout* $n \geq 1$;

(iii) $\exp(f(x)) \in A[[x]]$.

Preuve.- En préambule, rappelons que la série formelle $L(x) = \log(1 + x)$ est de type $p - T$ puisque ses coefficients sont invariants par σ.

$(i) \Rightarrow (iii)$: Si $f(x)$ est de type $p - T$ (tout comme $L(x)$), alors du point (ii) du LEF, il suit que

$$L^{-1}(f(x)) = \exp(f(x)) - 1 \in A[[x]];$$

ce qui établit (iii).

$(iii) \Rightarrow (i)$: Puisque $h(x) := \exp(f(x)) - 1$ a ses coefficients dans A, alors en vertu du point (iii) du LEF, il existe une série formelle $k(x) \in A[[x]]$ telle que

$$f(x) = L(h(x)) = f_k(x).$$

Ceci signifie précisément que $f(x)$ est de type $p - T$.

$(i) \Leftrightarrow (ii)$: Si l'on pose $g(x) = \sum_{n\geq 1} g_n x^n$, alors l'équation fonctionnelle

$$f_g(x) - \frac{1}{p}\sigma_* f_g(x^p) = g(x),$$

s'écrit, in extenso

$$\sum_{n\geq 1} \frac{a_n}{n} x^n - \frac{1}{p} \sum_{n\geq 1} \frac{a_n^\sigma}{n} x^{np} = \sum_{n\geq 1} g_n x^n.$$

Par identification des coefficients des puissances de x, on obtient

$$\frac{a_n}{n} = g_n \quad \text{si } p \text{ ne divise pas } n \geq 1 \text{ et}$$

$$\frac{a_{np}}{np} - \frac{a_n^\sigma}{np} = g_{np} \quad \text{pour } n \geq 1.$$

Ou encore

$$a_n = n \cdot g_n \quad \text{si } p \text{ ne divise pas } n \geq 1 \text{ et}$$

$$a_{np} = a_n^\sigma + np \cdot g_{np} \quad \text{pour } n \geq 1.$$

Supposer que $f(x)$ est de type $p - T$ revient à imposer que $g_n \in A$ pour tout $n \geq 1$. Dans ce cas, $a_n \in nA = A$ si p ne divise pas n et $a_{np} \equiv a_n^\sigma \ mod\ npA$ pour $n \geq 1$. Réciproquement, si l'on admet (ii), alors de fait, $g_n \in A$ pour tout $n \geq 1$, ce qui, par définition, prouve que $f(x)$ est de type $p - T$. ∎

Définition 1.3.1 *Nous donnerons le nom de* congruence de Honda[3] *à la congruence*

$$a_{np}(t) \equiv a_n(t^p) \, mod \, npA$$

apparaissant dans l'énoncé du point (ii) du théorème de Barsky.

Définition 1.3.2 *[14] Deux suites $(a_n)_{n\geq 1}$ et $(e_n)_{n\geq 1}$ satisfont à* l'identité de Spitzer, *si*

$$\exp\left(\sum_{n\geq 1} \frac{a_n}{n} x^n\right) = 1 + \sum_{n\geq 1} e_n x^n.$$

[3]Par analogie avec les résultats concernant les polynômes de Legendre établis dans [21].

Proposition 1.3.1 *Si deux suites $(a_n)_{n\geq 1}$ et $(e_n)_{n\geq 1}$ satisfont à l'identité de Spitzer, alors*

1. $$ne_n = a_n + \sum_{k=1}^{n-1} e_k a_{n-k} \quad ,(n \geq 1);$$

2. $$e_n = \sum \frac{a_1^{m_1} \cdots a_n^{m_n}}{m_1! \cdots m_n! 1^{m_1} \cdots n^{m_n}},$$

où la sommation est étendue à tous les n-uples $(m_1, m_2, \ldots, m_n)$ d'entiers positifs tels que $m_1 + 2m_2 + \cdots + nm_n = n$.

Preuve[4].- Posons

$$f(x) = \sum_{n\geq 1} \frac{a_n}{n} x^n \quad \text{et} \quad g(x) = 1 + \sum_{n\geq 1} e_n x^n.$$

En dérivant l'identité de Spitzer

$$g(x) = \exp(f(x)),$$

on obtient

$$g'(x) = f'(x) \cdot \exp(f(x)),$$

ou encore

$$xg'(x) = xf'(x)g(x),$$

égalité dont le développement en séries s'écrit

$$\sum_{n\geq 1} ne_n x^n = \sum_{n\geq 1} a_n x^n \left(1 + \sum_{n\geq 1} e_n x^n\right).$$

La première relation s'obtient par identification des coefficients des puissances de x des deux membres de cette égalité.
On trouvera une preuve de 2. dans [14], p. 73-74. ∎

1.4 Pseudo-puissances

Définition 1.4.1 *On dit qu'un polynôme $P(t) \in \mathbf{Z}_p[t]$ est une* pseudo-puissance n *si sa dérivée $P'(t)$ appartient à $n\mathbf{Z}_p[t]$.*

Exemples

- Si $q(t) \in \mathbf{Z}_p[t]$, alors sa n-ième puissance $P(t) = q(t)^n$ est une pseudo-puissance n (c'est l'origine de la terminologie);

[4] Voir aussi [30]

- le polynôme de Tchebychev $T_n(t) := \cos(n \cdot \arccos t)$ est une pseudo-puissance n dans $\mathbf{Z}_p[t]$, quel que soit p (cf. chapitre 3) ;
- le n-ième polynôme de Legendre $P_n(t)$ est, simultanément, pseudo-puissance n et $n+1$ dans $\mathbf{Z}_p[t]$, pour tout p impair (cf. chapitre 4).

Proposition 1.4.1 *Soit une suite $(P_n(t))_{n\geq 1} \subset \mathbf{Z}_p[t]$ de polynômes vérifiant les congruences de Honda*

$$P_{np}(t) \equiv P_n(t^p) \ mod\ np\,\mathbf{Z}_p[t],\ (n \geq 1);$$

alors $P_n(t)$ est une pseudo-puissance n, quel que soit $n \geq 1$.

Preuve.- Ce résultat s'établit par induction sur l'ordre p-adique de n. Soit $\nu = ord_p(n)$; si $\nu = 0$, alors n est une unité p-adique. Comme $P_n(t) \in \mathbf{Z}_p[t]$, par hypothèse, alors

$$P_n'(t) \in n\mathbf{Z}_p[t] = \mathbf{Z}_p[t].$$

Supposons maintenant que $n = mp^\nu$, avec $\nu > 0$ et m premier à p. Après dérivation de la congruence de Honda

$$P_{mp^\nu}(t) \equiv P_{mp^{\nu-1}}(t^p) \ mod\ mp^\nu\mathbf{Z}_p[t],$$

on obtient

$$P'_{mp^\nu}(t) \equiv p \cdot P'_{mp^{\nu-1}}(t^p) \cdot t^{p-1} \ mod\ mp^\nu\,\mathbf{Z}_p[t].$$

Par hypothèse d'induction, $P'_{mp^{\nu-1}}(t) \in mp^{\nu-1}\mathbf{Z}_p[t]$, ainsi le second membre de la congruence précédente est nul modulo $p^\nu\mathbf{Z}_p[t]$, de sorte que

$$P'_{mp^\nu}(t) \in mp^\nu\mathbf{Z}_p[t].$$

■

1.5 Limite définie sur une lemniscate

Proposition 1.5.1 *Soit $(P_n(t))_{n\geq 1} \subset \mathbf{Z}_p[t]$ une famille de polynômes satisfaisant, pour tout $n \geq 1$, à la relation de congruence de Honda*

$$P_{np}(t) \equiv P_n(t^p) \ mod\ np\,\mathbf{Z}_p[t].$$

Si l'on considère, dans $\mathbf{C}_p$, le domaine D de convergence de la suite $(P_{mp^\nu}(a))_{\nu\geq 0}$ (m entier fixé) et si π_m désigne la fonction définie sur D par

$$\pi_m(a) := \lim_{\nu\to\infty} P_{mp^\nu}(a),$$

alors

a) Le domaine D contient la lemniscate p-adique

$$L_{r_e} = \{a \in \mathbf{C}_p \,:\, |a^p - a| \leq r_e\};$$

b) Si $a \in D$ et $|a| \leq 1$, alors les racines p-ièmes $a^{1/p}$ de a appartiennent aussi à D. De plus $\pi_m(a) = \pi_m(a^{1/p})$.

c) Si $a \in D$, alors la boule $B_{\leq r_e} = \{x \in \mathbf{C}_p \,:\, |x - a| \leq r_e\}$ est contenue dans D et π_m est constante sur cette boule.

Preuve.- *a)* Soit $a \in L_{r_e}$; pour montrer que $b_\nu := P_{mp^\nu}(a)$ définit une suite convergente dans $\mathbf{C}_p$, il suffit de voir que $b_{\nu+1} - b_\nu \to 0$ lorsque ν tend vers ∞. Mais

$$\begin{aligned} |b_{\nu+1} - b_\nu| &= |P_{mp^{\nu+1}}(a) - P_{mp^\nu}(a)| \\ &= |P_{mp^{\nu+1}}(a) - P_{mp^\nu}(a^p) + P_{mp^\nu}(a^p) - P_{mp^\nu}(a)| \\ &\leq \max\{|P_{mp^{\nu+1}}(a) - P_{mp^\nu}(a^p)|\,;\, |P_{mp^\nu}(a^p) - P_{mp^\nu}(a)|\} \\ &\leq \max\left\{|p^{\nu+1}|\,;\, |p^\nu|\right\} \\ &\leq |p^\nu| \to 0 \text{ lorsque } \nu \to \infty. \end{aligned}$$

En effet, d'une part

$$\begin{aligned} |P_{mp^{\nu+1}}(a) - P_{mp^\nu}(a^p)| &\leq \left|mp^{\nu+1} r_\nu(a)\right|, \ (r_\nu(t) \in \mathbf{Z}_p[t]) \\ &\leq \left|p^{\nu+1}\right|, \end{aligned}$$

grâce à la congruence de Honda; d'autre part, comme le polynôme $P_{mp^\nu}(t)$ est une pseudo-puissance mp^ν (cf. proposition 1.4.1), le *théorème des accroissements finis* fournit les inégalités

$$\begin{aligned} |P_{mp^\nu}(a^p) - P_{mp^\nu}(a)| &\leq |a - a^p| \cdot \|P'_{mp^\nu}(a)\| \\ &\leq |a - a^p| \cdot |mp^\nu| \\ &\leq |p^\nu|. \end{aligned}$$

Ainsi, $|b_{\nu+1} - b_\nu| \to 0$ lorsque ν tend vers ∞, si bien que la suite $b_\nu = P_{mp^\nu}(a)$ converge.

b) Si $a \in D$ est de valeur absolue $|a| \leq 1$, alors la congruence de Honda implique que

$$P_{mp^\nu}(a^{1/p}) = P_{mp^{\nu-1}}(a) + mp^\nu r_\nu\left(a^{1/p}\right),$$

avec $r_\nu(t) \in \mathbf{Z}_p[t]$ pour tout $\nu \geq 1$. Si $\nu \to \infty$, la dernière égalité devient

$$\pi_m(a^{1/p}) = \pi_m(a).$$

c) Si $|x - a| \leq r_e$, alors *le théorème des accroissements finis* montre que

$$|P_{mp^\nu}(x) - P_{mp^\nu}(a)| \leq |p^\nu| \to 0 \text{ lorsque } \nu \to \infty$$

et par conséquent, que $\pi_m(x) = \pi_m(a)$. ∎

Remarque.- La lemniscate L_{r_e} est réunion disjointe de p boules de rayon r_e. Plus précisément, si l'on considère l'ensemble

$$\mu_{p-1} = \left\{\zeta \in \mathbf{C}_p : \zeta^{p-1} = 1\right\} \subset \mathbf{Z}_p,$$

alors

$$L_{r_e} = \coprod_{\zeta \in \mu_{p-1} \cup \{0\}} B_{\leq r_e}(\zeta).$$

Ceci découle du lemme suivant.

Lemme 1.5.1 *Soient $r < 1$ et $L_r = \{x \in \mathbf{C}_p : |x^p - x| \leq r\}$ la lemniscate p-adique de paramètre r; alors*

$$L_r = \coprod_{\zeta \in \mu_{p-1} \cup \{0\}} B_{\leq r}(\zeta).$$

Preuve.- Pour $x \in L_r$, l'inégalité $|x^p - x| \leq r < 1$ montre que $|x| \leq 1$. Ecrivons la factorisation

$$|x^p - x| = |x| \cdot |x - \zeta_1| \cdot \cdots \cdot |x - \zeta_{p-1}|,$$

avec

$$\zeta_i \in \mu_{p-1} \subset \mathbf{Z}_p \text{ et } \zeta_i \equiv i \ mod\ p\mathbf{Z}_p.$$

Alors, ou bien $|x| < 1$, auquel cas $|x^p - x| = |x| \leq r$, et donc $x \in B_{\leq r}(0)$, ou bien $|x| = 1$. Dans ce cas, il existe $i \in \{1, \ldots p-1\}$, tel que $|x - \zeta_i| < 1$. Mais alors, pour $j \neq i$, on a

$$|x - \zeta_j| = |x - \zeta_i + \zeta_i - \zeta_j| = |\zeta_i - \zeta_j| = |i - j| = 1.$$

Ainsi $|x^p - x| = |x - \zeta_i| \leq r$, ce qui montre que $x \in B_{\leq r}(\zeta_i)$.

Réciproquement, si $x \in B_{\leq r}(0)$, alors $|x^p - x| = |x| \leq r$ et donc $x \in L_r$. Maintenant, si $x \in B_{\leq r}(\zeta_i)$, pour un $i \in \{1, 2, \ldots, p-1\}$ et si $\alpha \in \mathbf{C}_p$ est tel que $x = \zeta_i + \alpha$, alors

$$\begin{aligned} x^p - x &= \sum_{k=0}^{p} \binom{p}{k} \zeta_i^k \alpha^{p-k} - \zeta_i - \alpha \\ &= \sum_{k=0}^{p-1} \binom{p}{k} \zeta_i^k \alpha^{p-k} - \alpha \\ &= (p-1)\alpha + \sum_{k=0}^{p-2} \binom{p}{k} \zeta_i^k \alpha^{p-k}, \end{aligned}$$

de sorte que $|x^p - x| \leq |\alpha| \leq r$ et donc $x \in L_r$. ∎

1.6 Limite définie sur $\mathbf{Z}_p(1)$

Dans le paragraphe précédent, nous avons étudié la question de la convergence de la suite $(P_{mp^\nu}(a))_{\nu\geq 0}$ pour $a \in \mathbf{C}_p$ fixé. Une autre possibilité de construire une fonction limite, à partir de la suite de polynômes $(P_{mp^\nu}(t))_{\nu\geq 0}$, consistera à considérer une suite $(P_{mp^\nu}(\zeta_\nu))_{\nu\geq 0}$ en choisissant ζ_ν dans une partie adéquate de $\mathbf{C}_p$.

Définitions 1.6.1 *Pour k entier positif, considérons le groupe μ_{p^k} des racines p^k-ièmes de l'unité dans $\mathbf{C}_p$, i.e*

$$\mu_{p^k} = \left\{\zeta \in \mathbf{C}_p \,:\, \zeta^{p^k} = 1\right\} \subset \mu_{p^\infty} = \bigcup_{k\geq 0} \mu_{p^k}$$

et l'application $\varphi_k : \mu_{p^{k+1}} \to \mu_{p^k}$ qui envoie ζ sur ζ^p. On définit alors $\mathbf{Z}_p(1)$ comme la limite projective

$$\mathbf{Z}_p(1) := \varprojlim \mu_{p^k}.$$

En tant que tel, $\mathbf{Z}_p(1)$ est un groupe abélien, compact, totalement discontinu, dont les éléments consistent en les suites $[\zeta] = (\zeta_k)_{k\geq 0}$, avec $\zeta_k \in \mu_{p^k}$ et $\zeta_k = \varphi(\zeta_{k+1}) = \zeta_{k+1}^p$.

Proposition 1.6.1 *Si $(P_n(t))_{n\geq 1} \subset \mathbf{Z}_p[t]$ est une suite de polynômes vérifiant les congruences de Honda*

$$P_{np}(t) \equiv P_n(t^p) \ mod\ np\,\mathbf{Z}_p[t],\ (n \geq 1),$$

alors, quel que soit $m \geq 1$ et pour tout $[\zeta] \in \mathbf{Z}_p(1)$, la limite

$$\lim_{\nu\to\infty} P_{mp^\nu}(\zeta_\nu)$$

existe et définit ainsi une fonction continue sur $\mathbf{Z}_p(1)$.

Preuve.- Soient donc $m \geq 1$ et un élément $[\zeta] = (\zeta_\nu)_{\nu\geq 0}$ de $\mathbf{Z}_p(1)$. La suite définie par $b_\nu = P_{mp^\nu}(\zeta_\nu)$ est une suite de Cauchy car

$$\begin{aligned} |b_\nu - b_{\nu-1}| &= |P_{mp^\nu}(\zeta_\nu) - P_{mp^{\nu-1}}(\zeta_{\nu-1})| \\ &= |P_{mp^\nu}(\zeta_\nu) - P_{mp^{\nu-1}}(\zeta_\nu^p)| \\ &\leq |p^\nu| \cdot |r_\nu(\zeta_\nu)| \text{ avec } r_\nu(t) \in \mathbf{Z}_p[t] \text{ (congruence de Honda)} \\ &\leq |p^\nu|\,; \end{aligned}$$

elle est donc convergente. Posons

$$\tilde{\pi}([\zeta]) = \lim_{\nu\to\infty} P_{mp^\nu}(\zeta_\nu);$$

la majoration ci-dessus entraîne alors la suivante

$$|P_{mp^\nu}(\zeta_\nu) - P_{mp^r}(\zeta_r)| \leq |p^r| \ ,(\nu \geq r \geq 0).$$

Cette dernière reste valable à la limite $\nu \to \infty$ et fournit

$$|\,\tilde{\pi}([\zeta]) - P_{mp^r}(\zeta_r)\,| \leq |p^r|.$$

La continuité (relativement à la topologie de $\mathbf{Z}_p(1)$) de la fonction $\tilde{\pi}$ s'ensuit immédiatement. ∎

1.7 Polygones de Newton

Définition 1.7.1 *Soit* $P(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbf{Q}_p[t]$, *un polynôme de degré* $n \geq 1$ *à coefficients dans* $\mathbf{Q}_p$. L'ensemble représentatif *de* $P(t)$ *est formé des couples* $s_i = (i, ord_p(a_i))$ *où* $i \in \{0, 1, \ldots, n\}$.
On appelle polygone de Newton *de* $P(t)$, *l'ensemble* $\mathcal{N}_P$ *des segments* $[s_i, s_j]$ *qui constituent le bord de l'enveloppe convexe supérieure (dans* $\mathbf{R}^2$*) de l'ensemble représentatif de* $P(t)$.

Le polygone de Newton $\mathcal{N}_P$ recèle toute l'information concernant les valeurs absolues des zéros de $P(t)$ dans $\mathbf{C}_p$ (voir [25], [2]). Plus précisément, on a les résultats suivants.

Proposition 1.7.1 *Si* $[s_i, s_j]$ *est un segment du polygone de Newton* $\mathcal{N}_P$ *du polynôme* $P(t)$, *avec*

$$s_i = (i, v_i)\ ,\ s_j = (j, v_j),\ \ (j > i),$$

alors $P(t)$ *possède* $j - i$ *zéros (comptés avec leur multiplicité) de valeur absolue égale à* $p^{-\Delta_{ij}}$, *où* $\Delta_{ij} = \frac{v_j - v_i}{j - i}$ *est la pente de* $[s_i, s_j]$ *(avec la convention:* $p^{-\infty} = 0$*).*

Preuve.- cf. [25].

Définition 1.7.2 *Si* $[s_i, s_j]$ *est un segment de pente* Δ_{ij} *du polygone de Newton* $\mathcal{N}_P$, *alors* Δ_{ij} *est appelée* pente critique *de* $\mathcal{N}_P$ *et le nombre* $r_{ij} = p^{-\Delta_{ij}}$ *est* rayon critique *de* $\mathcal{N}_P$. *Par abus de langage, on parlera de rayon critique ou de pente critique du polynôme* $P(t)$.

Ainsi, r est rayon critique de $\mathcal{N}_P$ si et seulement s'il existe $a \in \mathbf{C}_p$, avec $P(a) = 0$ et $|a| = r$.

Exemple.- L'ensemble représentatif du polynôme

$$P(t) = (1 + t)^p - 1 = \sum_{k=1}^{p} \binom{p}{k} t^k$$

est formé des $p + 1$ couples $(0, +\infty)$, $(1, 1)$, $\ldots$, $(p - 1, 1)$ et $(p, 0)$. Il donne lieu à un polygone de Newton réduit à deux segments: l'un vertical de pente $-\infty$, l'autre oblique de pente $-\frac{1}{p-1}$ (cf. fig. 1.7.1).

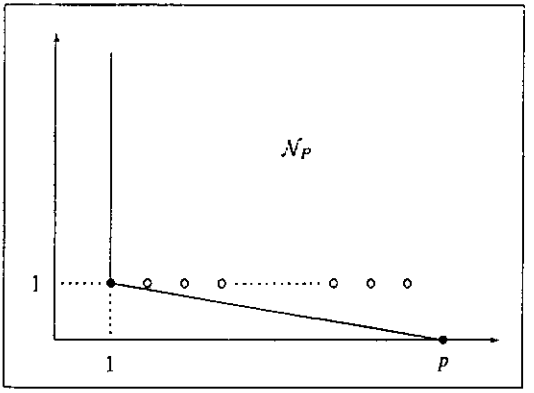

fig. 1.7.1

On en déduit, sans surprise, que $P(0) = 0$ et que, par ailleurs, les $p-1$ autres zéros de $P(t)$ sont situés sur la sphère de rayon critique $|p|^{\frac{1}{p-1}}$.
Par définition, $P(t) = 0$ si et seulement si $1 + t \in \mu_p$. Ainsi, les racines p-ièmes de l'unité (autres que 1) se trouvent sur la sphère $B_{=r_c}(1)$ de $\mathbf{C}_p$.

La proposition suivante montre comment la congruence de Honda peut, dans certains cas, fournir une information sur les zéros des polynômes qui la vérifient.

Proposition 1.7.2 *Si $(P_n(t))_{n\geq 1} \subset \mathbf{Z}_p[t]$ est un système de polynômes tels que, pour tout $n \geq 1$, les conditions suivantes soient remplies*

1. *la congruence de Honda est satisfaite, i.e*

$$P_{np}(t) \equiv P_n(t^p) \ mod\ np\,\mathbf{Z}_p[t];$$

2. *le coefficient dominant de $P_n(t)$ est une unité;*

3. $P_n(0) = 0$;

4. $P_n'(0) = n \cdot u_n$ *avec* $u_n \in \mathbf{Z}_p^\times$;

alors

$$\{\Delta : \Delta \text{ pente critique de } P_{np}(t)\} = \left\{\frac{\Delta}{p} : \Delta \text{ pente critique de } P_n(t)\right\} \bigcup \left\{-\frac{1}{p-1}\right\}.$$

Plus précisément, si $n = mp^\nu$ avec $\nu \geq 0$ et m premier à p, les rayons critiques du polynôme $P_n(t)$ sont

a) $r = 0$ *lorsque* $n = 1$;

b) $r = 0$ *et* $r = 1$ *lorsque* $n = m \geq 2$;

c) $r = 0$, $r_k = p^{-\frac{1}{p^k(p-1)}} = r_e^{1/p^k}$ $(k = 0, 1, \ldots, \nu - 1)$ *si* $m = 1$ *et* $\nu > 0$;

d) $r = 0$, $r = 1$ *et* $r_k = r_e^{1/p^k}$ $(k = 0, 1, \ldots, \nu - 1)$ *si* $m > 1$ *et* $\nu > 0$.

Preuve.-L'affirmation *a*) est évidente.

b) Si $n = m \geq 2$, alors le polynôme $P_n(t)$ s'écrit

$$P_n(t) = at + \cdots + bt^n$$

avec $a, b \in \mathbf{Z}_p^\times$. Son polygone de Newton est donc formé d'un segment vertical et d'un segment horizontal, qui fournissent les rayons critiques $r = 0$ et $r = 1$.

Le point *c*) s'établit par induction sur $\nu \geq 1$. La congruence de Honda

$$P_p(t) \equiv P_1(t^p) = bt^p \ mod\, p\,\mathbf{Z}_p[t] \ \ (b \in \mathbf{Z}_p^\times),$$

donne la construction suivante du polygone $\mathcal{N}_{P_p}$.

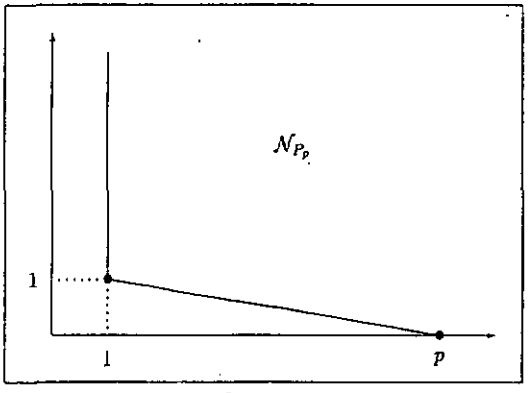

fig. 1.7.2

Les rayons critiques de $P_p(t)$ sont donc

$$r = 0 \ \text{ et } \ r_0 = p^{-\frac{1}{p-1}} = r_e.$$

Supposons (hypothèse d'induction) que le polynôme $P_{p^\nu}(t)$, $(\nu \geq 1)$, possède les $\nu+1$ rayons critiques $r = 0$ et r_k, $k = 0, \ldots, \nu - 1$, provenant du polygone de Newton $\mathcal{N}_{P_{p^\nu}}$.

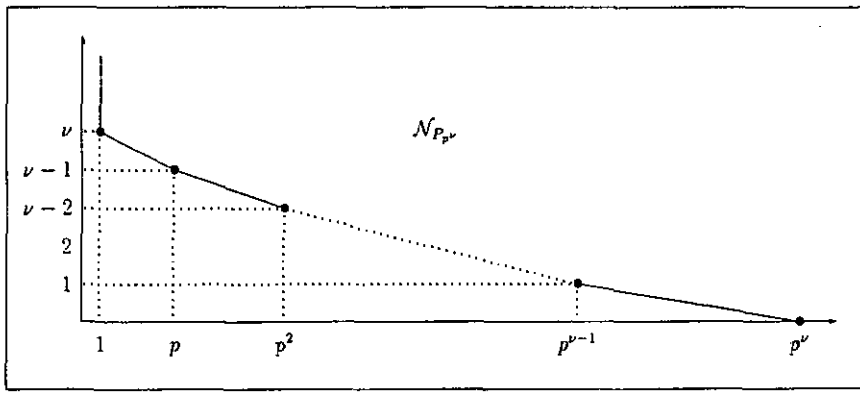

fig. 1.7.3

La congruence de Honda

$$P_{p^{\nu+1}}(t) \equiv P_{p^\nu}(t^p) \ mod\, p^{\nu+1}\mathbf{Z}_p[t],$$

permet de déduire le polygone de Newton de $P_{p^{\nu+1}}(t)$ de celui de $P_{p^\nu}(t)$. En effet, si $s_i = (i, v_i)$ et $s_j = (j, v_j)$ sont les extrémités d'un segment de $\mathcal{N}_{P_{p^\nu}}$, alors $\hat{s}_i = (ip, v_i)$ et $\hat{s}_j = (jp, v_j)$ sont celles d'un segment de $\mathcal{N}_{P_{p^{\nu+1}}}$. Autrement dit, si P_{p^ν} possède la pente critique Δ, alors $P_{p^{\nu+1}}$ admet $\frac{\Delta}{p}$ comme pente critique. En outre, les points $s_1 = (1, \nu+1)$ et $s_p = (p, \nu)$ sont les sommets d'un segment (de pente $-\frac{1}{p-1}$) du polygone de $P_{p^{\nu+1}}(t)$. Ainsi, le polynôme $P_{p^{\nu+1}}(t)$ possède les $\nu+2$ pentes critiques

$$\Delta = -\infty\ ,\ \Delta_k = -\frac{1}{(p-1)p^k}\ ,k = 0, \cdots, \nu.$$

d) Soit $m > 1$; le polynôme $P_m(t)$ possède la pente critique $\Delta = 0$: celle du segment d'extrémités $(1,0)$ et $(m,0)$. Il s'ensuit que $r = 1$ est rayon critique de $P_{mp^\nu}(t)$, quel que soit $\nu \geq 0$.
Le reste du point *d*) s'obtient de façon tout à fait analogue au point *c*). En fait, le polygone de Newton $\mathcal{N}_{P_{mp^\nu}}$ est constitué d'un segment horizontal $[(p^\nu, 0); (mp^\nu, 0)]$ et du polygone de Newton $\mathcal{N}_{P_{p^\nu}}$ de P_{p^ν} entre les indices 0 et p^ν. ∎

Exemple.- La famille de polynômes, $(Q_n(t))_{n\geq 1} \subset \mathbf{Z}_p[t]$, définie par

$$Q_n(t) = (1+t)^n - 1.$$

satisfait, de façon évidente, aux hypothèses 2, 3 et 4 de la proposition 1.7.2. Par ailleurs, ainsi que nous l'établirons dans le chapitre 2, la congruence de Honda

$$Q_{np}(t) \equiv Q_n(t^p) \ mod\, np\, \mathbf{Z}_p[t]$$

est vérifiée pour tout $n \geq 0$. Comme, par définition

$$Q_n(t) = 0 \iff \zeta = 1 + t \in \mu_{p^n},$$

la proposition 1.7.2 fournit la proximité à 1 de ζ, c'est-à-dire la distance

$$|t| = |1 - \zeta|.$$

Par exemple, si

$$\zeta \in \mu_{p^k} - \mu_{p^{k-1}},$$

pour un certain $k \geq 1$, alors

$$|\zeta| = |p|^{\frac{1}{(p-1)p^{k-1}}} = r^{\frac{1}{p^{k-1}}}.$$

Je crois que la réalité mathématique nous est extérieure, que notre rôle est de la découvrir ou de l'observer, et que les théorèmes que nous démontrons, en les qualifiant pompeusement de "créations", sont simplement des notes sur nos observations.

G. H. Hardy L'apologie d'un mathématicien

Chapitre 2

FAMILLES D'APPELL

2.1 Famille d'Appell et congruences de Honda

Considérons une suite $(P_n(t))_{n\geq 0} \subset \mathbf{Z}_p[t]$ telle que le polynôme $P_n(t)$ soit une pseudo-puissance n pour tout $n \geq 0$. D'après la définition donnée dans le chapitre précédent, ceci signifie que la dérivée $P_n'(t)$ appartient $n\mathbf{Z}_p[t]$. Autrement dit, pour tout $n \geq 0$, il existe un polynôme $r_{n-1}(t) \in \mathbf{Z}_p[t]$, défini par

$$P_n'(t) := nr_{n-1}(t).$$

Ce caractère d'intégralité est la seule condition imposée à la suite $(r_n(t))$; en particulier, il n'existe aucune relation entre les polynômes $P_n(t)$. L'exigence de compatibilité, exprimée ci-après, définit les suites particulières de pseudo-puissances que nous nous proposons d'étudier.

Définition 2.1.1 *Une* famille d'Appell[1] *est une suite* $(A_n(t))_{n\geq 0}$, *de polynômes liés par les conditions*

$$A_0'(t) = 0 \quad et \quad A_n'(t) = nA_{n-1}(t)\ ,\ (n \geq 1).$$

Remarque.- Avec cette définition, le terme A_k d'une suite d'Appell $(A_n(t)) \subset \mathbf{Z}_p[t]$ est une pseudo-puissance k de degré k.

Exemples.- Le présent chapitre se consacre, précisément, à l'étude de quelques exemples classiques de familles d'Appell. Les polynômes de Bernoulli et d'Euler font l'objet des sections 2.3 et 2.4, tandis que les polynômes $R_n(t) := (1+t)^n$ (rencontrés dans le chapitre précédent) sont traités en section 2.2.

Remarque.- Si deux polynômes $P_{np}(t)$ et $P_n(t)$ vérifient la congruence de Honda

$$P_{np}(t) \equiv P_n(t^p) \ mod\ np\,\mathbf{Z}_p[t], \qquad (1)$$

[1] Paul Appell, mathématicien français né à Strasbourg (1855-1930). L'essentiel de son oeuvre se situe en analyse.

alors, clairement, leur évaluation en un quelconque entier p-adique $a \in \mathbf{Z}_p$ amène la congruence

$$P_{np}(a) \equiv P_n(a^p) \ mod\ np\mathbf{Z}_p. \tag{2}$$

Evidemment, la réciproque est fausse. Même si la congruence (2) a lieu en tout $a \in \mathbf{Z}_p$, la congruence polynomiale (1) n'en découle pas pour autant.
A titre d'exemple, les polynômes $P_p(t) = 2t^p - t$ et $P_1(t) = t$ ne vérifient pas la congruence de Honda, bien que

$$P_p(a) - P_1(a^p) = a^p - a \equiv 0 \ mod\ p\mathbf{Z}_p,$$

pour tout entier p-adique $a \in \mathbf{Z}_p$.

En revanche, "la propriété d'Appell" entraîne le résultat suivant.

Théorème 2.1.1 *Pour une famille d'Appell $(A_n(t))_{n\geq 0}$ dans $\mathbf{Z}_p[t]$, les deux affirmations suivantes sont équivalentes*

(i) Il existe un entier $a \in \mathbf{Z}_p$ pour lequel

$$A_{np}(a) \equiv A_n(a^p) \ mod\ np\mathbf{Z}_p,$$

quel que soit $n \geq 0$;

(ii) La congruence de Honda

$$A_{np}(t) \equiv A_n(t^p) \ mod\ np\,\mathbf{Z}_p[t]$$

est vérifiée pour tout $n \geq 0$.

Remarque.- En tant qu'élément d'une famille d'Appell dans $\mathbf{Z}_p[t]$, le polynôme $A_n(t)$ est une pseudo-puissance n. Ainsi, *le théorème des accroissements finis p-adiques* (appliquable ici puisque $|a^p - a| \leq |p| \leq r_c$) fournit la congruence

$$A_n(a^p) \equiv A_n(a) \ mod\ np\mathbf{Z}_p.$$

Dès lors, la proposition (i) du théorème 2.1.1 équivaut à la suivante

$(i)'$ Il existe un entier $a \in \mathbf{Z}_p$ en lequel la congruence

$$A_{np}(a) \equiv A_n(a) \ mod\ np\,\mathbf{Z}_p$$

est vérifiée quel que soit $n \geq 0$.

Preuve du théorème 2.1.1.- L'implication $(ii) \Rightarrow (i)$ est évidente. La réciproque $(i)' \Rightarrow (ii)$ se démontre à l'aide du *théorème de Barsky* (théorème 1.3.1). Il s'agit de prouver que les polynômes $q_n(t)$ intervenant dans l'identité de Spitzer

$$\exp\left(\sum_{n\geq 1} A_n(t)\frac{x^n}{n}\right) = 1 + \sum_{n\geq 1} q_n(t)x^n, \tag{1}$$

sont à coefficients dans $\mathbf{Z}_p$. En dérivant chaque membre de (1) par rapport à la variable t, on obtient

$$\left(\sum_{n\geq 1} A_n'(t)\frac{x^n}{n}\right)\exp\left(\sum_{n\geq 1} A_n(t)\frac{x^n}{n}\right) = \sum_{n\geq 1} q_n'(t)x^n$$

ou encore, grâce à la propriété d'Appell

$$\left(\sum_{n\geq 1} A_{n-1}(t)x^n\right)\left(1+\sum_{n\geq 1} q_n(t)x^n\right) = \sum_{n\geq 1} q_n'(t)x^n.$$

L'identification des coefficients relatifs à la même puissance de x, fournit la formule (avec $q_0(t)=1$)

$$q_n'(t) = \sum_{k=0}^{n-1} A_{n-k-1}(t)q_k(t)\ .\ (n\geq 1). \tag{2}$$

Ainsi

$$\begin{aligned} q_{n+1}'(t) &= \sum_{k=0}^{n} A_{n-k}(t)q_k(t) \\ &= \sum_{k=0}^{n-1} A_{n-k}(t)q_k(t) + A_0 q_n(t). \end{aligned}$$

Mais, la proposition 1.3.1 affirme que

$$q_n(t) = \frac{1}{n}\sum_{k=0}^{n-1} A_{n-k}(t)q_k(t), \tag{3}$$

de sorte qu'on obtient la "propriété d'Appell"

$$q_{n+1}'(t) = nq_n(t) + A_0 q_n(t) = (n+A_0)q_n(t).$$

de laquelle découle, par induction, le développement binomial suivant

$$q_n(t) = \sum_{k=0}^{n}\binom{n-1+A_o}{k} q_{n-k}(a)(t-a)^k. \tag{4}$$

L'ancrage se déduit de l'équation (2). En effet, pour $n=1$, celle-ci s'écrit $q_1'(t) = A_0 q_0(t) = A_0$ et entraîne le développement $q_1(t) = \binom{A_0}{1} q_0(a)(t-a) + q_1(a)$. Quant au pas d'induction, on l'établit en exprimant $q_{n+1}'(t)$, à l'aide de (4), comme suit

$$\begin{aligned} q_{n+1}'(t) &= (n+A_0)q_n(t) \\ &= (n+A_0)\sum_{k=0}^{n}\binom{n-1+A_0}{k} q_{n-k}(a)(t-a)^k. \end{aligned}$$

Et ainsi on obtient bien

$$\begin{aligned} q_{n+1}(t) &= \sum_{k=0}^{n} \frac{n+A_0}{k+1}\binom{n-1+A_0}{k} q_{n-k}(a)(t-a)^{k+1} + q_{n+1}(a) \\ &= \sum_{k=0}^{n} \binom{n+A_0}{k+1} q_{n-k}(a)(t-a)^{k+1} + q_{n+1}(a) \\ &= \sum_{k=0}^{n+1} \binom{n+A_0}{k} q_{n+1-k}(a)(t-a)^{k}. \end{aligned}$$

Nous devons démontrer que, pour tout $n \geq 1$, le polynôme

$$q_n(t) = \sum_{k=0}^{n} \binom{n-1+A_0}{k} q_{n-k}(a)(t-a)^k \tag{5}$$

appartient à $\mathbf{Z}_p[t]$. L'hypothèse $(i)'$ postule que la série formelle

$$\sum_{n\geq 1} \frac{A_n(a)}{n} x^n$$

est de type $p-T$ ou, de façon équivalente (théorème 1.3.1), que les coefficients $q_n(a)$ sont dans $\mathbf{Z}_p$.

Comme $A_0 \in \mathbf{Z}_p$, il en va de même des coefficients binomiaux $\binom{n-1+A_0}{k}$. Ainsi, tous les termes du membre de droite de (4) sont entiers p-adiques; ce qui montre que $q_n(t) \in \mathbf{Z}_p[t]$ pour tout $n \geq 0$ ou, de façon équivalente (théorème 1.3.1), que la série formelle

$$\sum_{n\geq 1} \frac{A_n(t)}{n} x^n$$

est de type $p-T$. A ce titre, ses coefficients satisfont à la relation de congruence

$$A_{np}(t) \equiv A_n(t^p) \ mod\ np\,\mathbf{Z}_p[t].$$

■

Remarque.- Soit $(q_n(t))_{n\geq 1}$ la suite de polynômes associée à une famille d'Appell $(A_n(t))_{n\geq 0} \in \mathbf{Z}_p[t]$ par l'identité de Spitzer

$$\exp\left(\sum_{n\geq 1} \frac{A_n(t)}{n} x^n\right) = 1 + \sum_{n\geq 1} q_n(t) x^n.$$

Au cours de la démonstration du théorème 2.1.1, nous avons établi les propriétés suivantes pour la suite $(q_n(t))_{n\geq 0}$.

a) Le polynôme $q_{n+1}(t)$ est une pseudo-puissance $n + A_0$;

b) Si $A_0 = 1$, alors la suite $(q_n(t))_{n\geq 0}$ est une famile d'Appell.

2.2 Les polynômes $R_n(t) = (1+t)^n$

En guise de premier exemple de familles d'Appell, considérons les polynômes

$$R_n(t) := (1+t)^n, \quad (n \geq 0).$$

Comme

$$R_n'(t) = n(1+t)^{n-1} = nR_{n-1}(t), \quad (n \geq 1) ;$$

$$R_0(t) = 1 ;$$

$$R_n(0) = 1, \quad (n \geq 1);$$

le théorème 2.1.1 s'applique et établit les congruences de Honda transcrites dans la proposition suivante[2].

Proposition 2.2.1 *Pour tout $n \geq 0$, on a la congruence*

$$(1+t)^{np} \equiv (1+t^p)^n \ mod\ np\mathbf{Z}_p[t].$$

Remarques.- 1) Le développement binomial de $R_n(t)$ implique que les coefficients binomiaux satisfont à la relation

$$\binom{np}{kp} \equiv \binom{n}{k} \ mod\ np\,\mathbf{Z}_p.$$

En effet, on a

$$\begin{aligned} R_{np}(t) - R_n(t^p) &= \sum_{k=0}^{np} \binom{np}{k} t^k - \sum_{k=0}^{n} \binom{n}{k} t^{pk} \\ &= \sum_{k=0}^{n} \left\{ \binom{np}{kp} - \binom{n}{k} \right\} t^{pk} + \sum_{\substack{k=0 \\ p \text{ ne divise pas } k}}^{np} \binom{np}{k} t^k \\ &\equiv 0 \ mod\ np\mathbf{Z}_p[t]. \end{aligned}$$

Ces congruences sont bien connues et ne représentent qu'une version plus faible d'un résultat de G. S. Kazandzidis [22], [23], [24], qui sera utilisé au chapitre 4.
2) Notons que la proposition 2.2.1 se démontre aussi à partir du théorème de Barsky. En effet, la série formelle

$$f(x) = \sum_{n \geq 1} \frac{R_n(t)}{n} x^n$$

[2] Equivalente au lemme 1.4 de [7].

se laissant écrire sous la forme

$$\begin{aligned} f(x) &= \sum_{n\geq 1} \frac{(1+t)^n}{n} x^n \\ &= \sum_{n\geq 1} \{(1+t)x\}^n \frac{1}{n} \\ &= -\log(1-tx), \end{aligned}$$

le développement de son exponentielle

$$\exp(f(x)) = \frac{1}{1-tx} = 1 + \sum_{n\geq 1} q_n(t) x^n,$$

fait apparaître les polynômes $q_n(t) = t^n \in \mathbf{Z}_p[t]$. Ainsi, la série formelle $f(x)$ est de type $p - T$, et de ce fait, ses coefficients vérifient les congruences de Honda. Au passage, on trouve le groupe formel

$$F(x,y) = f^{-1}(f(x) + f(y)) = x + y - txy,$$

isomorphe sur $\mathbf{Z}[t]$ au groupe multiplicatif

$$G_m(x,y) = x + y + xy,$$

via l'isomorphisme

$$h(x) = \exp(f(x)) - 1 = \frac{1}{1-tx} - 1 = \frac{tx}{1-tx} = tx + t^2x^2 + \cdots.$$

■

Pour le cas particulier où $n = p^r$ avec $r \geq 0$, la congruence de la proposition 2.2.1 s'écrit

$$(1+y)^{p^{r+1}} \equiv (1+y^p)^{p^r} \mod p^{r+1}\, \mathbf{Z}_p[y]. \tag{1}$$

Maintenant, si y est choisi égal à

$$y = -2tx + x^2,$$

alors il existe un polynôme $s(x,t) \in \mathbf{Z}_p[x,t]$ pour lequel

$$y^p = -2t^p x^p + x^{2p} + ps(x,t).$$

Dès lors, en appliquant le *théorème des accroissements finis* à la congruence (1), on obtient

$$\begin{aligned} \left(1 - 2tx + x^2\right)^{p^{r+1}} &\equiv \left(1 - 2t^p x^p + x^{2p} + ps(x,t)\right)^{p^r} \mod p^{r+1}\, \mathbf{Z}_p[x,t] \\ &\equiv \left(1 - 2t^p x^p + x^{2p}\right)^{p^r} \mod p^{r+1} \mathbf{Z}_p[x,t]. \end{aligned}$$

Si $q_r(t,x)$ et $q_{r+1}(t,x)$ dénotent les polynômes définis par

$$\begin{aligned}(1-2tx+x^2)^{p^{r+1}} &= 1+q_{r+1}(t,x),\\ (1-2t^px^p+x^{2p})^{p^r} &= 1+q_r(t^p,x^p),\end{aligned}$$

alors, la dernière congruence exprime le fait que

$$q_{r+1}(t,x) \equiv q_r(t^p,x^p) \ mod\ p^{r+1}\mathbf{Z}_p[x,t].$$

Soit maintenant $\mu \in \mathbf{Z}_p$; on a alors

$$\begin{aligned}(1-2tx+x^2)^{-\mu p^{r+1}} &= \left\{(1-2tx+x^2)^{p^{r+1}}\right\}^{-\mu}\\ &= \{1+q_{r+1}(t,x)\}^{-\mu}\\ &= \sum_{k\geq 0}\binom{-\mu}{k}q_{r+1}(t,x)^k\\ &= \sum_{k\geq 0}\binom{-\mu}{k}\left(q_r(t^p,x^p)+p^{r+1}u(x,t)\right)^k.\end{aligned}$$

où $u(x,t)$ est un polynôme à coefficients dans $\mathbf{Z}_p$. On en déduit la congruence

$$(1-2tx+x^2)^{-\mu p^{r+1}} \equiv \sum_{k\geq 0}\binom{-\mu}{k}q_r(t^p,x^p)^k \ mod\ p^{r+1}\mathbf{Z}_p[t][[x]].$$

dont le second membre peut s'écrire

$$\begin{aligned}\sum_{k\geq 0}\binom{-\mu}{k}q_r(t^p,x^p)^k &= \{1+q_r(t^p,x^p)\}^{-\mu}\\ &= \left\{(1-2t^px^p+x^{2p})^{p^r}\right\}^{-\mu}\\ &= (1-2t^px^p+x^{2p})^{-\mu p^r}.\end{aligned}$$

Tout ceci nous permet d'énoncer le résultat technique suivant.

Lemme 2.2.1 *Pour tout $\mu \in \mathbf{Z}_p$ et tout entier $r \geq 0$, la congruence suivante est vérifiée*

$$\left(1-2tx+x^2\right)^{-\mu p^{r+1}} \equiv \left(1-2t^px^p+x^{2p}\right)^{-\mu p^r} \ mod\ p^{r+1}\mathbf{Z}_p[t][[x]].$$

Définition 2.2.1 *Les* polynômes de Gegenbauer $C_n^\nu(t)$ *sont définis*[3] *formellement comme coefficients de la fonction génératrice*

$$g(x) = \left(1-2tx+x^2\right)^{-\nu} = \sum_{n\geq 0}C_n^\nu(t)x^n.$$

[3] voir [1], [28].

Voici la liste des six premiers.

$$\begin{aligned}
C_0^\nu(t) &= 1;\\
C_1^\nu(t) &= 2\nu t;\\
C_2^\nu(t) &= -\nu + 2\nu(1+\nu)t^2;\\
C_3^\nu(t) &= -2\nu(1+\nu)t + \tfrac{4\nu(1+\nu)(2+\nu)}{3}t^3;\\
C_4^\nu(t) &= \tfrac{\nu(1+\nu)}{2} - 2(1+\nu)(2+\nu)t^2 + \tfrac{2\nu(1+\nu)(2+\nu)(3+\nu)}{3}t^4;\\
C_5^\nu(t) &= \nu(1+\nu)(2+\nu)t - \tfrac{4\nu(1+\nu)(2+\nu)(3+\nu)}{3}t^3 + \tfrac{4\nu(1+\nu)(2+\nu)(3+\nu)(4+\nu)}{15}t^5.
\end{aligned}$$

Proposition 2.2.2 *Les polynômes de Cegenbauer $C_n^\nu(t)$ vérifient les congruences suivantes*

- $C_{np}^{\nu p}(t) \equiv C_n^\nu(t^p) \ mod\ \nu p\mathbf{Z}_p[t],\ \ (n \geq 0, \nu \in \mathbf{Z}_p)$;
- $C_n^{\nu p}(t) \equiv 0 \ mod\ \nu p\mathbf{Z}_p[t]$ *si* p *ne divise pas* $n \geq 1$.

Preuve.- Par définition

$$g(x) = \left(1 - 2tx + x^2\right)^{-\nu} = \sum_{n\geq 0} C_n^\nu(t)x^n;$$

soit alors l'unique unité p-adique $\mu \in \mathbf{Z}_p^\times$ telle que $\nu = \mu p^r \neq 0$, $(r \geq 0)$. Appliqué à $g(x)^p - \sigma.g(x^p)$, le lemme 2.2.1 fournit la congruence

$$\begin{aligned}
\sum_{n\geq 0} C_n^{\nu p}(t)x^n \ - \ & \sum_{n\geq 0} C_n^\nu(t^p)x^{np}\\
&= \left(1 - 2tx + x^2\right)^{-\mu p^{r+1}} - \left(1 - 2t^p x^p + x^{2p}\right)^{-\mu p^r}\\
&\equiv 0 \ mod\ p^{r+1}\mathbf{Z}_p[t][[x]],
\end{aligned}$$

dans laquelle, l'identification des coefficients des puissances de x traduit les deux points de la proposition. ∎

Remarque.- Dans [7], J-L Brylinski établit des congruences analogues à celles énoncées dans la proposition 2.2.2, mais seulement modulo p. Plus précisément, il démontre que si ν est un demi-entier et si p est premier impair, alors

- $C_{np}^{\nu p}(t) \equiv C_n^\nu(t)^p \ mod\ p,\ \ (n \geq 0)$;
- $C_n^{\nu p}(t) \equiv 0 \ mod\ p$ si p ne divise pas $n \geq 1$.

Notre résultat représente donc une amélioration sensible.

2.3 Nombres et polynômes de Bernoulli

Une abondante littérature[4] est consacrée à l'étude des nombres et polynômes de Bernoulli.[5] Le but de cette section est, d'une part, d'établir les congruences de Honda pour les polynômes de Bernoulli et d'autre part d'apporter des preuves p-adiques aux célèbres résultats de von Staudt-Clausen et Kummer ainsi que d'énoncer de nouvelles congruences sur les nombres de Bernoulli.

Définition 2.3.1 *Le développement en série*

$$\frac{xe^{xt}}{e^x-1}=\sum_{n\geq 0}B_n(t)\frac{x^n}{n!}$$

définit les polynômes de Bernoulli $B_n(t)$ *qui ont pour coefficients constants, les* nombres de Bernoulli $b_n := B_n(0)$.

Citons les premiers de ces polynômes

$$\begin{aligned}
B_0(t) &= 1;\\
B_1(t) &= t-\tfrac{1}{2};\\
B_2(t) &= t^2-t+\tfrac{1}{6};\\
B_3(t) &= t^3-\tfrac{3}{2}t^2+\tfrac{1}{2}t;\\
B_4(t) &= t^4-2t^3+t^2-\tfrac{1}{30};\\
B_5(t) &= t^5-\tfrac{5}{2}t^4+\tfrac{5}{3}t^3-\tfrac{1}{6}t.
\end{aligned}$$

Ainsi $b_0=1$, $b_1=\frac{1}{2}$, $b_2=\frac{1}{6}$, $b_3=0$, $b_4=-\frac{1}{30}$, $b_5=0$, etc...

La proposition suivante dresse une liste des propriétés dont nous ferons usage dans la suite.

Proposition 2.3.1 *Les nombres et polynômes de Bernoulli ont les propriétés suivantes*

1) $b_{2n+1}=0, \qquad (n\geq 1);$

2) $B_n'(t)=nB_{n-1}(t), \qquad (n\geq 1);$

3) $B_n(t+1)-B_n(t)=nt^{n-1}, \quad (n\geq 1);$

4) $B_n(t)=\sum_{k=0}^{n}\binom{n}{k}b_kt^{n-k}, \qquad (n\geq 0);$

lr

[4] Cf. [27], [17].

[5] Il s'agit ici des nombres de Jacques Bernoulli (1654-1705) et des polynômes de Daniel Bernoulli (1700-1782). Le terme de "polynômes de Bernoulli" fut introduit par J.-L. Raabe en 1851.

5) $S_k(N) := \sum_{0\le t<N} t^k = \frac{B_{k+1}(N)-b_{k+1}}{k+1}$, $(N \ge 1)$;

6) $B_n(1-t) = (-1)^n B_n(t)$, $(n \ge 0)$;

7) $(-1)^n B_n(-t) = B_n(t) + nt^{n-1}$. $(n \ge 0)$;

8) $B_n(mt) = m^{n-1} \sum_{k=0}^{m-1} B_n\left(t + \frac{k}{m}\right)$, $(n \ge 0, m \ge 1)$.

Preuve.- En dérivant, par rapport à t, la fonction génératrice

$$b(x,t) = \frac{xe^{xt}}{e^x - 1} = \sum_{n\ge 0} B_n(t)\frac{x^n}{n!},$$

on obtient

$$\frac{\partial b(x,t)}{\partial t} = \frac{x^2 e^{xt}}{e^x - 1} = x \cdot b(x,t);$$

une identité qui s'écrit, in extenso

$$\sum_{n\ge 0} B_n'(t)\frac{x^n}{n!} = \sum_{n\ge 1} nB_{n-1}(t)\frac{x^n}{n!}$$

et qui entraîne que $B_0'(t) = 0$ ainsi que la propriété d'Appell 2) $B_n'(t) = nB_{n-1}(t)$. A l'aide de cette seule propriété, on établit, par induction sur $n \ge 0$ (tout comme dans l'équation (3) de la section 2.1), le développement binomial

$$4)\ B_n(t) = \sum_{k=0}^{n} \binom{n}{k} b_k t^{n-k}.$$

Afin de démontrer la propriété 3), comparons les deux séries formelles $b(x,t)$ et $b(x,t+1)$. D'une part, on a

$$b(x,t+1) - b(x,t) = \sum_{n\ge 0} \{\, B_n(t+1) - B_n(t) \,\} \frac{x^n}{n!},$$

d'autre part

$$b(x,t+1) - b(x,t) = \frac{xe^{tx}\cdot e^x}{e^x - 1} - \frac{xe^{tx}}{e^x - 1} = xe^{tx} = \sum_{n\ge 1} n \cdot t^{n-1}\frac{x^n}{n!},$$

ce qui fait que $B_n(t+1) - B_n(t) = nt^{n-1}$, $(n \ge 0)$. La fonction génératrice $b(x,t)$ a également la propriété suivante

$$b(-x,-t) = \frac{-xe^{tx}}{e^{-x} - 1} = \frac{-xe^{x(t+1)}}{1 - e^x} = b(x,t+1). \qquad (1)$$

Le développement en séries des deux membres de (1) s'écrit

$$\sum_{n\geq 0} B_n(-t)\frac{(-x)^n}{n} = \sum_{n\geq 0} B_n(t+1)\frac{x^n}{n},$$

et fournit l'identité $B_n(t+1) = (-1)^n B_n(-t)$. Grâce à la substitution $t \mapsto -t$, on en déduit la relation

$$6)\ B_n(1-t) = (-1)^n B_n(t).$$

En substituant la propriété 3) dans l'identité $B_n(t+1) = (-1)^n B_n(-t)$, on tire

$$(-1)^n B_n(-t) = B_n(t+1) = B_n(t) + nt^{n-1};$$

c'est-à-dire la propriété 7), dont l'évaluation en $t = 0$ établit 1).
Grâce à la propriété 3), on a, pour $k \geq 0$

$$\ell^k = \frac{B_{k+1}(\ell+1) - B_{k+1}(\ell)}{k+1},$$

expression qui conduit à la relation avec les sommes de puissances

$$S_k(N) = \sum_{\ell=0}^{N-1} \ell^k = \frac{1}{k+1}\sum_{\ell=0}^{N-1}\left\{B_{k+1}(\ell+1) - B_{k+1}(\ell)\right\}.$$

Dans la dernière sommation, seuls subsistent le premier et le dernier terme. Autrement dit

$$5)\ \ S_k(N) = \frac{1}{k+1}\left\{B_{k+1}(N) - b_{k+1}\right\}.$$

Reste à démontrer l'identité dite "de Raabe" 8). Il s'agit de prouver que

$$B_n(mt) = \frac{1}{m}\sum_{k=0}^{m-1} m^n B_n\left(t + \frac{k}{m}\right).$$

A cet effet, multiplions numérateur et dénominateur de la fonction génératrice $b(x,t)$ par $e^{mx} - 1$ et développons

$$\begin{aligned} b(x,t) &= \frac{xe^{xt}}{e^{mx}-1}\cdot\frac{e^{mx}-1}{e^x-1} \\ &= \frac{1}{m}\cdot\frac{mx\cdot e^{xt}}{e^{mx}-1}\cdot\sum_{k=0}^{m-1} e^{kx} \\ &= \frac{1}{m}\sum_{k=0}^{m-1}\frac{mxe^{mx\frac{x+k}{m}}}{e^{mx}-1} \\ &= \frac{1}{m}\sum_{k=0}^{m-1} b\left(mx, \frac{x+k}{m}\right). \end{aligned}$$

En identifiant les coefficients des puissances de x correspondantes dans le développement de cette dernière identité, on obtient 8). ∎

Les nombres de Bernoulli sont rationnels; le théorème suivant, qui regroupe des résultats de von-Staudt, Clausen et Kummer, fournit des renseignements aussi bien sur leur numérateur que sur leur dénominateur. La preuve que nous reproduisons ici, est celle que A. Robert a présenté comme exemple d'application du *théorème des accroissements finis p-adiques* lors de son cours du 3eme cycle à Lausanne [33].

Théorème 2.3.1 *Les nombres de Bernoulli ont les propriétés suivantes*

1) *Si $p-1$ ne divise pas $k \geq 1$, alors il existe $r_k \in \mathbf{Z}_p$, tel que*

$$b_k = k \cdot r_k \, ;$$

2) *Si p est impair et si $p-1$ divise $k \geq 1$, alors il existe $r_k \in \mathbf{Z}_p$, tel que*

$$b_k = \frac{p-1}{p} + k \cdot r_k \, .$$

Preuve.- Considérons $S_k(p)$ la somme des puissances k-ièmes ($k \geq 1$), des entiers strictement inférieurs à p

$$S_k(p) = \sum_{i=1}^{p-1} i^k.$$

Pour tout $i \leq p-1$, il existe un unique entier p-adique ζ_i tel que

$$\begin{array}{l} \zeta_i^{p-1} = 1 \quad \text{et} \\ \zeta_i \equiv i \ mod\, p\mathbf{Z}_p. \end{array}$$

Alors

$$S_k(p) \equiv \sum_{i=1}^{p-1} \zeta_i^k = \sum_{\zeta \in \mu_{p-1}} \zeta^k \ mod\, p\mathbf{Z}_p.$$

On raffine cette congruence à l'aide du *théorème des accroissements finis* appliqué à la fonction $f(x) = x^k$ (pour laquelle $f'(x) = kx^{k-1}$) au voisinage de $x = i$.
Comme $\zeta_i \equiv i \ mod\, p\mathbf{Z}_p$, c'est-à-dire $|\zeta_i - i| \leq |p| \leq r_c$, on obtient la majoration

$$\begin{array}{rcl} \left|\zeta_i^k - i^k\right| & = & |f(\zeta_i) - f(i)| \\ & \leq & \|f'\| \cdot |\zeta_i - i| \\ & \leq & |kp|. \end{array}$$

L'inégalité ultramétrique entraîne alors la suivante

$$\left| S_k(p) - \sum_{\zeta \in \mu_{p-1}} \zeta^k \right| \leq |kp|,$$

que l'on transcrit sous la forme

$$S_k(p) = \sum_{\zeta \in \mu_{p-1}} \zeta^k + kp \cdot u_k, \quad \text{avec } u_k \in \mathbf{Z}_p. \tag{1}$$

Par ailleurs, rappelons la propriété 5) (proposition 2.3.1)

$$S_k(N) = \frac{B_{k+1}(N) - b_{k+1}}{k+1}.$$

qui s'exprime, à l'aide du développement binomial (propriété 4) de la proposition 2.3.1 de $B_{k+1}(t)$, comme suit

$$\begin{aligned} S_k(N) &= \frac{1}{k+1} \sum_{i=1}^{k+1} \binom{k+1}{i} b_{k+1-i} N^i \\ &= \sum_{i=1}^{k+1} \frac{1}{i} \binom{k}{i-1} N^i b_{k+1-i} \\ &= N b_k + \sum_{i=2}^{k+1} \frac{1}{i} \binom{k}{i-1} N^i b_{k+1-i}. \end{aligned}$$

Le choix $N = p$ fournit l'égalité

$$S_k(p) = p \cdot b_k + pk \sum_{i=2}^{k+1} \frac{1}{i(i-1)} \binom{k-1}{i-2} p^{i-2} \cdot p b_{k+1-i},$$

ou encore

$$S_k(p) = p \cdot b_k + pk \sum_{i=2}^{k+1} \frac{(k-1)!}{(k-i+1)!} \cdot \frac{p^{i-2}}{i!} \cdot p b_{k+1-i}. \tag{2}$$

Dans le membre de droite de (2), le terme $\frac{(k-1)!}{(k-i+1)!}$ est entier et le terme $\frac{p^{i-2}}{i!} \in \mathbf{Z}_p$ pour $p \neq 2$. En effet

$$\begin{aligned} ord_p\left(\frac{p^{i-2}}{i!}\right) &= ord_p\left(p^{i-2}\right) - ord_p(i!) \\ &= i - 2 - \frac{i - S_p(i)}{p-1} \\ &> \frac{i}{2} - 2 \\ &> -1 \end{aligned}$$

A l'aide de l'équation (2), on démontre alors (par induction sur k), que pb_k est entier p-adique, quel que soit $k \geq 0$ et de plus, qu'il existe $v_k \in \mathbf{Z}_p$ tel que

$$S_k(p) = pb_k + pk \cdot v_k \text{ avec } v_k \in \mathbf{Z}_p. \tag{3}$$

En comparant les deux expressions (1) et (3) trouvées pour la somme $S_k(p)$

$$S_k(p) = \begin{cases} pb_k + pkv_k \\ \sum_{\zeta \in \mu_{p-1}} \zeta^k + pku_k, \end{cases}$$

on obtient

$$pb_k = \sum_{\zeta \in \mu_{p-1}} \zeta^k + pk \cdot r_k \quad \text{avec} \quad r_k \in \mathbf{Z}_p. \tag{4}$$

Lorsque k n'est pas multiple de $p-1$, la somme apparaissant dans le membre de droite de (4) s'annule, de sorte que

$$b_k = kr_k \quad \text{avec } r_k \in \mathbf{Z}_p,$$

tandis que si $p-1$ divise k, alors

$$pb_k = p - 1 + pk \cdot r_k,$$

c'est-à-dire

$$b_k = \frac{p-1}{p} + kr_k \quad \text{avec} \quad r_k \in \mathbf{Z}_p \ (p \neq 2).$$

■

Remarque.- Le théorème précédent montre que $pb_k \in \mathbf{Z}_p$ pour tout p premier impair, ce qui est encore vrai pour $p = 2$. En effet, via l'identité (2)

$$S_k(2) = 2b_k + k \sum_{i=2}^{k+1} \frac{(k-1)!}{(k-i+1)!} \cdot \frac{2^{i-1}}{i!} 2 \cdot b_{k+1-i}, \tag{3}$$

on montre, par induction, que $2b_k \in \mathbf{Z}_2$ pour tout k, et ceci, grâce au fait que $ord_2\left(\frac{2^{i-1}}{i!}\right) = S_2(i) - 1 \geq 0$. Mieux, le point 2) du théorème est vérifié pour $k \geq 4$ pair.

Proposition 2.3.2 *Si $p = 2$ et $k \geq 4$ est un nombre pair, alors le nombre de Bernoulli b_k admet le développement*

$$b_k = \frac{p-1}{p} + k \cdot r_k = \frac{1}{2} + kr_k, \ \textit{avec } r_k \in \mathbf{Z}_2.$$

Preuve.- Rappelons que $b_0 = 1$ et $b_2 = \frac{1}{6}$. Ainsi

$$b_2 = \frac{1}{6} = \frac{1}{2} - \frac{1}{3}$$

fait bien exception. La proposition se démontre par induction sur k. Tout d'abord, pour $k = 4$, le nombre de Bernoulli $b_4 = -\frac{1}{30}$ admet le développement

$$\begin{aligned} b_4 &= -\frac{1}{30} = \frac{1}{2} - \frac{8}{15} \\ &= \frac{1}{2} + 4r_4 \\ &\quad \text{avec } r_4 = -\frac{2}{15} \in \mathbf{Z}_2; \end{aligned}$$

ce qui établit l'ancrage. De même, remarquons que

$$\begin{aligned} b_6 &= \frac{2}{42} = \frac{1}{2} - \frac{10}{21} \\ &= \frac{1}{2} + 6 \cdot \left(-\frac{5}{63}\right) \\ &= \frac{1}{2} + 6r_6 \\ &\qquad \text{avec } r_6 = -\frac{5}{63} \in \mathbf{Z}_2. \end{aligned}$$

Supposons maintenant que $k > 6$ et écrivons l'identité (3) sous la forme

$$\begin{aligned} 1 &= 2b_k + k(k-1)!\frac{2^{k+1}}{k+1}b_0 + k(k-1)!\frac{2^k}{k!}b_1 + \\ &\quad + k2^{k-2}b_2 + k\sum_{i=2}^{k-3}\frac{(k-1)!}{(k-i+1)!}\frac{2^{i-1}}{i!}\cdot 2b_{k+1-i}. \end{aligned}$$

En admettant l'hypothèse d'induction et en utilisant le fait que $2^\ell/\ell! \in 2\,\mathbf{Z}_2$ si $\ell \geq 1$, on obtient

$$1 = 2b_k + 2ks_k + k\sum_{\substack{2\leq i\leq k-3 \\ i \text{ impair}}}(k-1)\cdots(k-i+2)\frac{2^{i-1}}{i!}\left\{1 + 2(k+1-i)r_{k+1-i}\right\}.$$

avec s_k, r_{k+1-i} tous dans $\mathbf{Z}_2$. Il s'ensuit que

$$1 = 2b_k + 2ks_k + 2ku_k \text{ avec } u_k \in \mathbf{Z}_2;$$

d'où la proposition. ∎

Corollaire 2.3.1 (von Staudt) *Pour $k \geq 1$, le nombre de Bernoulli b_k peut s'écrire sous la forme*

$$b_k = -\sum_{p-1|k}\frac{1}{p} + m_k \text{ où } m_k \in \mathbf{Z}.$$

Preuve [33].- Le nombre rationnel

$$b_k + \sum_{p-1|k}\frac{1}{p}$$

est entier p-adique pour tout nombre p premier. Par conséquent, son dénominateur est 1. ∎

Autre corollaire du théorème 2.3.1, le lemme suivant nous permettra de présenter une nouvelle démonstration des congruences dites "de Kummer" [6].

Lemme 2.3.1 *Si $p-1$ ne divise pas n, alors le nombre rationnel*

$$\frac{B_n(a)}{n}$$

est entier p-adique, quel que soit $a \in \mathbf{Z}_p$.

Preuve.- On montre, par induction, que l'énoncé du lemme est vérifié par tout entier naturel $a = k$ et on conclut en utilisant la densité des entiers naturels dans $\mathbf{Z}_p$.
Si $k = 0$, alors le point 2 du théorème 2.3.1 montre que

$$\frac{1}{n}B_n(0) = \frac{b_n}{n} \in \mathbf{Z}_p.$$

Puis, la propriété 3) de la proposition 2.3.1, qui s'écrit

$$\frac{B_n(k+1)}{n} = \frac{B_n(k)}{n} + k^{n-1},$$

établit le pas d'induction. ∎

Théorème 2.3.2 (Congruences de Kummer) *Si $p-1$ ne divise pas $n \geq 2$, alors*

$$\frac{b_{n+p-1}}{n+p-1} \equiv \frac{b_n}{n} \ mod\, p\,\mathbf{Z}_p.$$

Preuve.- Il faut tout d'abord remarquer que les termes de la congruence sont tous deux nuls si $n \geq 2$ est impair. La congruence

$$\ell^{n-1} \equiv \ell^{n-1+(p-1)} \ mod\, p,$$

valable pour ℓ entier quelconque, entraîne la suivante

$$S_{n-1}(N) \equiv S_{n-1+p-1}(N) \ mod\, p,$$

qui, traduite à l'aide de la propriété 5) de la proposition 2.3.1, montre qu'il existe une constante $0 \leq c \leq p-1$, telle que la congruence

$$R(N) := \frac{B_{n+p-1}(N)}{n+p-1} - \frac{B_n(N)}{n} \equiv \frac{b_{n+p-1}}{n+p-1} - \frac{b_n}{n} \equiv c \ mod\, p,$$

est vérifiée pour tout entier N. Donc, quel que soit l'entier p-adique $a \in \mathbf{Z}_p$, on a

$$R(a) \equiv c \ mod\, p\,\mathbf{Z}_p.$$

[6] Cf. section V.8, (théorème 5) de [5].

L'identité de Raabe [propriété S), proposition 2.3.1], évaluée en $t = 1$, fournit les égalités

$$\frac{B_n(m)}{n} = m^{n-1} \sum_{k=0}^{m-1} \frac{B_n(1+\frac{k}{m})}{n}, \tag{1}$$

$$\frac{B_{n+p-1}(m)}{n+p-1} = m^{n-1+(p-1)} \sum_{k=0}^{m-1} \frac{B_{n+p-1}(1+\frac{k}{m})}{n+p-1}. \tag{2}$$

En effectuant la soustraction (2) − (1), on obtient

$$R(m) = m^{n-1} \sum_{k=0}^{m-1} \left\{ m^{p-1} \frac{B_{n+p-1}(1+\frac{k}{m})}{n+p-1} - \frac{B_n(1+\frac{k}{m})}{n} \right\}. \tag{3}$$

Si m est premier à p, alors $a = 1 + \frac{k}{m} \in \mathbf{Z}_p$ pour tout $k = 0, \ldots, m-1$ et $m^{p-1} \equiv 1 \ mod\ p$. Le lemme 2.3.1 donne alors lieu à la congruence

$$R(m) \equiv m^{n-1} \sum_{k=0}^{m-1} R\left(1+\frac{k}{m}\right) \ mod\ p\mathbf{Z}_p,$$

qui s'exprime

$$c \equiv m^{n-1} \sum_{k=0}^{m-1} c \ mod\ p\mathbf{Z}_p$$

ou encore

$$c(m^n - 1) \equiv 0 \ mod\ p\mathbf{Z}_p.$$

Choisissons m tel que $\tilde{m} := m \ mod\ p$ soit générateur du groupe $(\mathbf{Z}/p\mathbf{Z})^\times$. Comme $p-1$ ne divise pas n, la simplification est licite et amène bien la congruence de Kummer

$$c \equiv \frac{b_{n+p-1}}{n+p-1} - \frac{b_n}{n} \equiv 0 \ mod\ p\mathbf{Z}_p.$$

■

Remarque.- D'après le théorème 2.3.1, le nombre de Bernoulli b_n, pour $p-1$ ne divisant pas n, s'écrit $b_n = nr_n$. Les congruences de Kummer établissent donc la $(p-1)$-périodicité modulo p dans la suite $(r_n)_{n\geq 1}$ (pour les n non multiples de $p-1$).

Théorème 2.3.3 *Les nombres de Bernoulli vérifient les congruences suivantes*

1) $b_{np+k} \equiv b_{n+k} \ mod\ n\mathbf{Z}_p$, $(p \neq 2,\ n \geq 1,\ k \geq 0)$;

2) $b_{np^2-k} \equiv b_{np-k} \ mod\ n\mathbf{Z}_p$, $(p \neq 2,\ n \geq 1,\ 0 \leq k \leq n(p-1))$.

La démonstration de ce théorème s'appuie sur les deux lemmes suivants qui exploitent la relation entre les nombres de Bernoulli et les sommes de puissances d'entiers.

Lemme 2.3.2 *Pour $n \geq 0$ et $k \geq 0$, on a la congruence*

$$S_{np+k}(p) \equiv S_{n+k}(p) \ mod\ np\,\mathbf{Z}_p.$$

Preuve.- Soit un entier $\ell \in \{1, \ldots, p-1\}$; on a

$$\ell^{np+k} = \ell^k \cdot \ell^{np} = \ell^k \cdot \{\ell^p\}^n = \ell^k\{\ell + up\}^n \text{ avec } u \in \mathbf{Z}_p.$$

Appliqué à la fonction x^n au voisinage de $x = \ell$, *le théorème des accroissements finis* fournit la congruence

$$\ell^{np+k} = \ell^k\{\ell + up\}^n \equiv \ell^k \cdot \ell^n = \ell^{n+k} \ mod\ np\,\mathbf{Z}_p.$$

On somme sur ℓ pour obtenir

$$\sum_{\ell=1}^{p-1} \ell^{np+k} \equiv \sum_{\ell=1}^{p-1} \ell^{n+k} \ mod\ np\,\mathbf{Z}_p.$$

Lemme 2.3.3 *Si $n \geq 1$ et $k \geq 1$, alors*

$$S_{n+k}(p) \equiv p \cdot b_{n+k} + \sum_{j=2}^{k+1} k(k-1)\cdots(k-j+2) \cdot \frac{p^j}{j!} \cdot b_{n+k+1-j} \ \ modulo \begin{cases} np\,\mathbf{Z}_p & si\ p \neq 2 \\ n\,\mathbf{Z}_p & si\ p = 2. \end{cases}$$

Preuve.- En utilisant la proposition 2.3.1 [propriétés 5) et 6)], on obtient l'expression suivante pour $S_{n+k}(p)$.

$$\begin{aligned} S_{n+k}(p) &= \frac{B_{n+k+1}(p) - b_{n+k+1}}{n+k+1} \\ &= \frac{1}{n+k+1} \sum_{j=1}^{n+k+1} \binom{n+k+1}{j} b_{n+k+1-j} \cdot p^j \\ &= p \cdot b_{n+k} + (n+k)\frac{p^2}{2!} \cdot b_{n+k-1} + \\ &\quad \sum_{j=3}^{n+k+1} \binom{n+k+1}{j} \frac{1}{n+k+1} p^{j-2} \cdot p \cdot pb_{n+k+1-j} \\ &= p \cdot b_{n+k} + (n+k)\frac{p}{2!} \cdot pb_{n+k-1} + \\ &\quad + \sum_{j=3}^{n+k+1} (n+k)\cdots(n+k-j+2) \cdot \frac{p^{j-2}}{j!} \cdot p \cdot pb_{n+k+1-j}. \end{aligned}$$

Rappelons que $p \cdot b_n \in \mathbf{Z}_p$ quel que soit n (théorème 2.3.1). Si $p \neq 2$, alors $p^{j-2}/j! \in \mathbf{Z}_p$ pour tout $j \geq 2$ et ainsi

$$\begin{aligned} S_{n+k}(p) &\equiv p \cdot b_{n+k} + k\frac{p^2}{2!} b_{n+k-1} + \sum_{j=3}^{k+1} k \cdots (k-j+2) \cdot \frac{p^j}{j!} b_{n+k+1-j} \ mod\ np\,\mathbf{Z}_p \\ &\equiv p \cdot b_{n+k} + \sum_{j=2}^{k+1} k \cdots (k-j+2) \cdot \frac{p^j}{j!} \cdot b_{n+k+1-j} \ mod\ np\,\mathbf{Z}_p. \end{aligned}$$

Si $p = 2$, alors $p^{j-1}/j! \in \mathbf{Z}_p$ pour tout $j \geq 2$, et la congruence obtenue n'est vraie que *modulo* $n\,\mathbf{Z}_2$. ∎

Preuve du théorème 2.3.3.- Démontrons, par induction sur $k \geq 0$, la congruence

$$b_{np+k} \equiv b_{n+k} \ mod\, n\,\mathbf{Z}_p, \ \ (p \neq 2).$$

Grâce au théorème 2.3.1, on peut écrire

$$\begin{aligned} (1)\ b_n &= \delta(n) \cdot \frac{p-1}{p} + nr_n \\ (2)\ b_{np} &= \delta(np) \cdot \frac{p-1}{p} + npr_{np} \end{aligned}$$

avec r_n et r_{np}, deux entiers p-adiques et où $\delta(i)$ est définie par

$$\delta(i) = \begin{cases} 0 & \text{si } p-1 \text{ ne divise pas } i; \\ 1 & \text{si } p-1 \text{ divise } i. \end{cases}$$

De la soustraction (1)−(2) (et du fait que $\delta(np) = \delta(n)$), suit la congruence

$$b_{np} \equiv b_n \ mod\, n\,\mathbf{Z}_p,$$

qui établit l'ancrage d'induction. Par le lemme 2.3.3 , on a

$$S_{np+k}(p) \equiv p \cdot b_{np+k} + \sum_{j=2}^{k+1} k \cdots (k-j+2)\frac{p^j}{j!} b_{np+k+1-j} \ mod\, np^2\,\mathbf{Z}_p, \qquad (3)$$

$$S_{n+k}(p) \equiv p \cdot b_{n+k} + \sum_{j=2}^{k+1} k \cdots (k-j+2)\frac{p^j}{j!} b_{n+k+1-j} \ mod\, np\,\mathbf{Z}_p. \qquad (4)$$

En effectuant la soustraction (3)−(4) et grâce au lemme 2.3.2, on obtient

$$\begin{aligned} 0 &\equiv S_{np+k}(p) - S_{n+k}(p) \\ &\equiv p(b_{np+k} - b_{n+k}) + \sum_{j=2}^{k+1} k \cdots (k-j+2)\frac{p^j}{j!}(b_{np+k+1-j} - b_{n+k+1-j}) \ mod\, np\,\mathbf{Z}_p. \end{aligned}$$

Mais si l'on admet l'hypothèse d'induction

$$b_{np+k+1-j} - b_{n+k+1-j} \equiv 0 \ mod\, n\,\mathbf{Z}_p, \ (j \geq 2),$$

alors

$$\frac{p^j}{j!}(b_{np+k+1-j} - b_{n+k+1-j}) \equiv 0 \ mod\, np\,\mathbf{Z}_p \ (\text{ et même } \ mod\, np^2\,\mathbf{Z}_p).$$

On en conclut que

$$p(b_{np+k} - b_{n+k}) \equiv 0 \ mod\ np\,\mathbf{Z}_p,$$

d'où la congruence à démontrer. Le point 2) s'établit en utilisant successivement le point 1), comme suit.

$$\begin{aligned}
b_{np^2-k} &= b_{(np-k)+np(p-1)} && \text{avec } np-k \geq 0\\
&\equiv b_{(np-k)+n(p-1)} \ mod\ n\,\mathbf{Z}_p && \text{par le point 1)}\\
&= b_{np+(n(p-1)-k)} && \text{avec } n(p-1)-k \geq 0\\
&\equiv b_{n+n(p-1)-k} \ mod\ n\,\mathbf{Z}_p && \text{par le point 1)}\\
&\equiv b_{np-k} \ mod\ n\,\mathbf{Z}_p.
\end{aligned}$$

■

Corollaire 2.3.2 *Pour tous entiers $m \geq 0$, k et ℓ, la suite*

$$(B_{mp^\nu+k}(\ell))_{\nu \geq \nu_0}$$

converge dans $\frac{1}{p}\mathbf{Z}_p$, $(p \neq 2)$.

Preuve.- Le théorème 2.3.3 stipule que

$$\begin{aligned}
&1)\ b_{mp^\nu+k} \equiv b_{mp^{\nu-1}+k} \ mod\ mp^{\nu-1}\,\mathbf{Z}_p && (p \neq 2,\ m \geq 1,\ k \geq 0,\ \nu \geq 1);\\
&2)\ b_{mp^\nu-k} \equiv b_{mp^{\nu-1}-k} \ mod\ mp^{\nu-2}\,\mathbf{Z}_p && (p \neq 2,\ m \geq 1,\ 0 \leq k \leq mp^{\nu-2}(p-1)).
\end{aligned}$$

Cette autre formulation montre que, quels que soient $m \geq 0$ et $k \in \mathbf{Z}$, la suite

$$(B_{mp^\nu+k}(0))_{\nu \geq \nu_0} = (b_{mp^\nu+k})_{\nu \geq \nu_0}$$

converge (avec, ici, ν_0 défini de sorte que $mp^{\nu_0} + k \geq 0$). Ceci établit l'ancrage d'une induction dont le pas se démontre grâce à la propriété 3) de la proposition 2.3.1 qui s'écrit

$$B_{mp^\nu+k}(\ell+1) = B_{mp^\nu+k}(\ell) + (mp^\nu + k)\ell^{mp^\nu+k-1}.$$

Finalement, la propriété 6) de la même proposition, à savoir

$$B_{mp^\nu+k}(-\ell)(-1)^{m+k} = B_{mp^\nu+k}(\ell) + (mp^\nu + k)\ell^{mp^\nu+k-1},$$

achève la démonstration. ■

Après ces quelques résultats sur les nombres de Bernoulli, il est temps de revenir à l'étude des polynômes du même nom. Notons que ces derniers ne satisfont qu'à une relation de congruence de Honda affaiblie. Plus précisément, on a

Théorème 2.3.4 *Les polynômes de Bernoulli $(B_n(t))_{n\geq 0}$ sont des polynômes d'Appell à coefficients dans $\frac{1}{p}\mathbf{Z}_p$; ils vérifient les congruences*

$$\begin{array}{lrcl} \mathbf{1)} & B_{np}(t) & \equiv & B_n(t^p) \ \ mod\ n\mathbf{Z}_p[t]; \quad (p\neq 2,\ n\geq 0); \\ \mathbf{2)} & B_{2n}(t) & \equiv & B_n(t^2) \ \ mod\ \frac{n}{2}\mathbf{Z}_2[t], \qquad\qquad (n\geq 0). \end{array}$$

Preuve.- Le théorème de von Staudt (Corollaire 2.3.1) ainsi que la propriété 4) de la proposition 2.3.1 montrent que le polynôme $B_n(t)$ a ses coefficients dans $\frac{1}{p}\mathbf{Z}_p[t]$. Appliquons le théorème 2.1.1 à la suite $(\beta_n(t))_{n\geq 0}$ définie par

$$\beta_n(t) = 2pB_n(t).$$

Par construction, celle-ci constitue une famille d'Appell dans $\mathbf{Z}_p[t]$.

1) Si $p\neq 2$, alors le théorème 2.3.3 implique la congruence

$$\beta_{np}(0) - \beta_n(0) = 2p\,(b_{np} - b_n) \equiv 0 \ \ mod\ np\,\mathbf{Z}_p,$$

équivalente, par le théorème 2.1.1, à la congruence polynomiale

$$\beta_{np}(t) - \beta_n(t^p) = 2p\,(B_{np}(t) - B_n(t^p)) \equiv 0 \ \ mod\ np\,\mathbf{Z}_p[t],$$

qui établit le point 1) du théorème.

2) Si $p=2$, alors

$$\beta_{2n}(0)-\beta_n(0) = 4\,(b_{2n} - b_n) = \left\{ \begin{array}{ll} 4b_2 - 4b_1 = \frac{8}{3} \equiv 0\ mod\ 2n\,\mathbf{Z}_2 & \text{si } n=1 \\ 4b_4 - 4b_2 = -\frac{4}{5} \equiv 0\ mod\ 2n\,\mathbf{Z}_2 & \text{si } n=2 \\ 4b_6 - 4b_3 = 4b_6 \equiv 0\ mod\ 2n\,\mathbf{Z}_2 & \text{si } n=3 \\ 4\,(2nr_{2n} - nr_n) \equiv 0\ mod\ 2n\,\mathbf{Z}_2 & \text{si } n\geq 4, \\ & \text{(proposition 2.3.2)} \end{array} \right.$$

Dans tous les cas

$$\beta_{2n}(0) - \beta_n(0) \equiv 0 \ \ mod\ 2n\,\mathbf{Z}_2,$$

congruence équivalente (théorème 2.1.1) à la congruence polynomiale

$$4B_{2n}(t) \equiv 4B_n(t^2) \ \ mod\ 2n\,\mathbf{Z}_2[t].$$

■

Corollaire 2.3.3 *Pour $p \neq 2$, la série formelle*

$$b(x) = \sum_{n\geq 1} p \cdot B_{n(p-1)}(t)\frac{x^n}{n}$$

donne naissance à un groupe formel à coefficients dans $\mathbf{Z}_p[[t]]$, défini par

$$F_b(x,y) = b^{-1}(b(x) + b(y))$$

et isomorphe au groupe multiplicatif $G_m(x,y)$.

Preuve.- D'après le LEF, il suffit de vérifier que

$$\frac{d}{dx}b(x)\Big|_{x=0} \in \mathbf{Z}_p[[t]]^{\times}.$$

On calcule

$$\begin{aligned}\frac{d}{dx}b(x)\Big|_{x=0} &= pB_{p-1}(t)\\ &= pb_{p-1} + ts(t)\\ &\quad \text{avec } s(t) \in \mathbf{Z}_p[t].\end{aligned}$$

D'après le théorème 2.3.1, on a

$$pb_{p-1} = p - 1 + p(p-1)r_{p-1}, \text{ avec } r_{p-1} \in \mathbf{Z}_p.$$

Par conséquent $pb_{p-1} \in \mathbf{Z}_p^{\times}$, si bien que $pB_{p-1}(t) \in \mathbf{Z}_p[[t]]^{\times}$. ∎

Corollaire 2.3.4 *Pour $p \neq 2$ et $\nu \geq 2$, les rayons critiques du polynôme de Bernoulli $B_{p^\nu}(t)$ sont*

$$0,\ 1 \text{ et } r_k = p^{-\frac{1}{(p-1)p^k}} = r_c^{p^{-k}},\ k = 0,\ldots,\nu-2,$$

tandis que pour $p = 2$, le polynôme $B_{2^\nu}(t)$, $(\nu \geq 1)$, possède l'unique rayon critique $2^{\frac{1}{2^\nu}}$.

Preuve.- Supposons tout d'abord que $p \neq 2$ et considérons, cette fois, les polynômes

$$\beta_n(t) := B_{np}(t).$$

On applique alors le principe de la proposition 1.7.2 à la sous-suite $(\beta_{p^\nu}(t))_{\nu\geq 0}$, pour laquelle

2. $\beta_{p^\nu}(t) - \beta_{p^{\nu-1}}(t^p) = B_{p^{\nu+1}}(t) - B_{p^\nu}(t^p) \equiv 0 \ mod\ p^\nu\, \mathbf{Z}_p[t]$. Autrement dit, la congruence de Honda est vérifiée.

3. Le coefficient dominant de $\beta_{p^\nu}(t)$ est égal à 1 (donc d'ordre p-adique nul). En effet, ceci découle de la propriété d'Appell $B_n'(t) = nB_{n-1}(t)$ et du fait que $B_0(t) = 1$.

4. $\beta_{p^\nu}(0) = b_{p^{\nu+1}} = 0$, puisque p est impair.

5. Grâce au théorème 2.3.3, on a

$$\beta'_{p^\nu}(0) = B'_{p^{\nu+1}}(0) = p^{\nu+1} b_{p^{\nu+1}-1} \equiv (p-1)p^\nu \mod p^{\nu+1}\mathbf{Z}_p,$$

donc $\beta'_{p^\nu}(0) \in p^\nu \mathbf{Z}_p^\times$.

1. Le fait que $\deg(\beta_{p^\nu}(t)) = \deg(B_{p^{\nu+1}}(t)) = p^{\nu+1}$ modifie d'un rien les conclusions de la proposition 1.7.2. En fait, celle-ci montre que le polynôme $\beta_{p^{\nu-1}}(t) = B_{p^\nu}(t)$ possède, outre 0 et $-\infty$, les $\nu - 1$ pentes critiques

$$\Delta_k = -\frac{1}{(p-1)p^k}, \quad k = 0, \ldots, \nu - 2.$$

Remarquons que tout ceci provient du fait que le polynôme

$$B_p(t) = pb_{p-1}t + \cdots + t^p$$

possède les pentes critiques 0 et $-\infty$.

Supposons maintenant que $p = 2$ et intéressons-nous aux pentes critiques de $B_{2^\nu}(t)$ pour $\nu \geq 1$. Le polynôme $B_2(t) = t^2 - t + \frac{1}{6}$, dont le polygone de Newton est représenté ci-dessous, possède l'unique pente critique $\frac{1}{2}$.

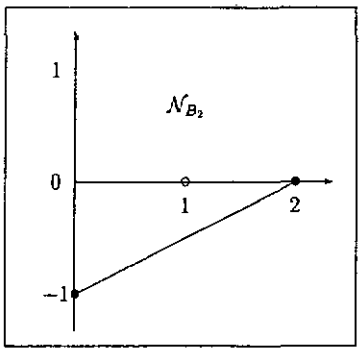

fig. 2.3.1

■

Le coefficient constant de $B_{2^\nu}(t)$ est le nombre de Bernoulli b_{2^ν} qui, par le théorème de von Staudt, a un ordre 2-adique égal à -1, . Comme

$$B_{2^{\nu+1}}(t) \equiv B_{2^\nu}(t^2) \ mod\, 2^{\nu-1}\, \mathbf{Z}_2[t],$$

on déduit la construction du polygone de Newton de $B_{2^{\nu+1}}(t)$ à partir de celui de $B_{2^\nu}(t)$ et on hérite ainsi de la seule pente critique $\frac{1}{2^{\nu+1}}$.

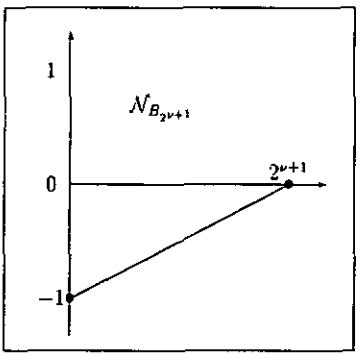

fig. 2.3.2

Terminons cette section consacrée aux nombres et polynômes de Bernoulli, par l'étude de la fonction limite définie à la section 1.5.

Proposition 2.3.3 *Si b_m est la fonction définie sur la lemniscate p-adique*

$$L_{r_e} = \{a \in \mathbf{C}_p \,:\, |a^p - a| \leq r_e\}$$

par la limite

$$b_m(a) = \lim_{\nu \to \infty} B_{mp^\nu}(a),$$

alors

$$b_m(a) = \begin{cases} \frac{p-1}{p} & \text{si } p = 2 \text{ ou si } p \text{ impair est tel que } p-1 \text{ divise } m \text{ pair} \\ 0 & \text{si } p \text{ et } m \text{ sont impairs ou si } p-1 \text{ ne divise pas } m \text{ pair} \end{cases}$$

Preuve.- Rappelons que

$$L_{r_e} = \coprod_{i \in \mu_{p-1} \cup \{0\}} B_{\leq r_e}(i) = \coprod_{i \in \{0,\ldots,p-1\}} B_{\leq r_e}(i).$$

Puisque b_m est constante sur les boules $B_{\leq r_c}(i)$ (proposition 1.5.1), il suffit de déterminer $b_m(i)$ pour $i = 0, \ldots, p-1$. Mieux, comme (proposition 2.3.1)

$$B_{mp^\nu}(a+1) = B_{mp^\nu}(a) + mp^\nu a^{mp^\nu - 1},$$

b_m est constante et égale à $b_m(0) = \lim_{\nu \to -\infty} B_{mp^\nu}(0)$. Ainsi

$$\lim_{\nu \to -\infty} B_{mp^\nu}(0) = \begin{cases} 0 & \text{si } m \text{ impair et } p \text{ impair} \\ \lim_{\nu \to -\infty} mp^\nu r_{mp^\nu} = 0 & \text{si } p \text{ impair et } p-1 \text{ ne divise pas } m \text{ pair} \\ \lim_{\nu \to -\infty} \left\{ \frac{p-1}{p} + mp^\nu r_{mp^\nu} \right\} & \text{si } p = 2 \\ & \text{ou si } p \text{ est tel que } p-1 \text{ divise } m \text{ pair} \end{cases}$$

d'où la proposition. ∎

2.4 Polynômes d'Euler

Définition 2.4.1 *Les polynômes $E_n(t)$, définis par le développement en série*

$$\frac{2e^{xt}}{e^x + 1} = \sum_{n \geq 0} E_n(t) \frac{x^n}{n!},$$

sont appelés polynômes d'Euler. *Les valeurs qu'ils prennent en $t = \frac{1}{2}$ définissent les nombres d'Euler e_n*

$$e_n := 2^n E_n\left(\tfrac{1}{2}\right),$$

qui apparaissent dans le développement

$$\frac{1}{\cosh x} = \sum_{n \geq 0} e_n \frac{x^n}{n!}.$$

Ainsi, par exemple

$$\begin{aligned} E_0(t) &= 1; \\ E_1(t) &= t - \tfrac{1}{2}; \\ E_2(t) &= t^2 - t; \\ E_3(t) &= t^3 - \tfrac{3}{2}t^2 + \tfrac{1}{4}; \\ E_4(t) &= t^4 - 2t^3 + t; \\ E_5(t) &= t^5 - \tfrac{5}{2}t^4 + \tfrac{5}{2}t^2 - \tfrac{1}{2} \\ &\quad \text{etc...} \end{aligned}$$

et donc

$$e_0 = 1,\ e_1 = 0,\ e_2 = -1,\ e_3 = 0,\ e_4 = 5,\ e_5 = 0,\ \text{etc...}$$

La proposition suivante fait l'inventaire des quelques propriétés bien connues dont nous ferons usage dans la suite.

Proposition 2.4.1 *Les nombres et polynômes d'Euler ont les propriétés suivantes*

1) $E_n'(t) = nE_{n-1}(t)$, $(n \geq 1)$;

2) $E_n(t) = \sum_{k=0}^{n} \binom{n}{k} E_k(0) t^{n-k}$, $(n \geq 0)$;

3) $E_n(t+1) + E_n(t) = 2t^n$, $(n \geq 0)$;

4) $S_k^-(N) := \sum_{0 \leq \ell < N} (-1)^{\ell+1} \ell^k = \frac{1}{2}\left(-E_k(0) + (-1)^N E_k(N)\right)$, $(N \geq 1, k \geq 1)$;

5) $E_n(1-t) = (-1)^n E_n(t)$, $(n \geq 0)$;

6) $(-1)^{n+1} E_n(-t) = E_n(t) - 2t^n$, $(n \geq 0)$.

Preuve.- En dérivant la fonction génératrice

$$e(x,t) = \frac{2e^{xt}}{e^x + 1} = \sum_{n \geq 0} E_n(t) \frac{x^n}{n!},$$

par rapport à t, on obtient

$$\frac{\partial}{\partial t} e(x,t) = x \frac{2e^{xt}}{e^x + 1} = x e(x,t),$$

c'est-à-dire

$$\sum_{n \geq 0} E_n'(t) \frac{x^n}{n!} = \sum_{n \geq 0} n E_{n-1}(t) \frac{x^n}{n!}.$$

On en déduit que $E_0'(t) = 0$ ainsi que la propriété d'Appell $E_n'(t) = nE_{n-1}(t)$. De cette dernière découle (par induction) le développement binomial

$$2) \quad E_n(t) = \sum_{k=0}^{n} \binom{n}{k} E_k(0) t^{n-k}.$$

La propriété 3) se démontre en considérant la somme des deux séries formelles $e(x,t)$ et $e(x,t+1)$ qui vaut, d'une part

$$e(x,t+1) + e(x,t) = \sum_{n \geq 0} \{E_n(t+1) + E_n(t)\} \frac{x^n}{n!},$$

et d'autre part

$$e(x,t+1) + e(x,t) = \frac{2e^{xt}e^x}{e^x + 1} + \frac{2e^{xt}}{e^x + 1} = 2e^{xt} = 2 \sum_{n \geq 0} t^n \frac{x^n}{n!}.$$

Ainsi, on obtient l'identité

$$E_n(t+1) + E_n(t) = 2t^n.$$

La propriété 4) s'en déduit alors, comme suit

$$\begin{aligned} S_k^-(N) &= \sum_{0<\ell<N} (-1)^{\ell+1}\ell^k \\ &= \frac{1}{2}\sum_{1\le\ell\le N-1} (-1)^{\ell+1}\left\{E_k(\ell+1)+E_k(\ell)\right\} \\ &= \frac{1}{2}\left\{E_k(1)+E_k(2)-E_k(2)+\cdots+(-1)^N E_k(N)\right\} \\ &= \frac{E_k(1)+(-1)^N E_k(N)}{2} \\ &= \frac{-E_k(0)+(-1)^N E_k(N)}{2}. \end{aligned}$$

Le développement en séries de l'expression

$$e(-x,-t)=\frac{2e^{xt}}{e^{-x}+1}=\frac{2e^{x(t+1)}}{e^x+1}=e(x,t+1),$$

s'écrit

$$\sum_{n\ge 0} E_n(-t)(-1)^n\frac{x^n}{n!}=\sum_{n\ge 0} E_n(t+1)\frac{x^n}{n!}.$$

Cela implique l'égalité

$$E_n(t+1)=(-1)^n E_n(-t),$$

dans laquelle la substitution $t\mapsto -t$ entraîne la propriété 5)

$$(-1)^n E_n(t)=E_n(1-t).$$

Finalement, en introduisant 3) dans l'identité

$$E_n(t+1)=(-1)^n E_n(-t),$$

on établit la propriété 6), à savoir

$$(-1)^n E_n(-t)=E_n(t+1)=2t^n-E_n(t).$$

■

Corollaire 2.4.1

1) $E_{2n+1}\left(\frac{1}{2}\right)=0$ *pour tout* $n\ge 0$ *et donc, les nombres d'Euler* e_n *d'indice impair sont nuls;*

2) $E_{2n}(0)=0$ *pour tout* $n\ge 1$.

Preuve.- L'évaluation en $t=\frac{1}{2}$ de l'expression de la propriété 5) (proposition 2.4.1) fournit l'égalité

$$(-1)^n E_n\left(\frac{1}{2}\right)=E_n\left(\frac{1}{2}\right),$$

qui montre bien que $E_n\left(\frac{1}{2}\right)=0$ si n est impair. Le point 2) se démontre en posant $t=0$ dans la propriété 6). ■

Proposition 2.4.2 *Pour $p \neq 2$, les polynômes d'Euler sont à coefficients dans $\mathbf{Z}_p$. De plus, en $a = 0$ et en $a = \frac{1}{2}$ la congruence*

$$E_{np}(a) \equiv E_n(a) \ mod\ np\,\mathbf{Z}_p$$

est vérifiée quel que soit $n \geq 0$.

Preuve.- Par définition, on a

$$\frac{\partial^n}{\partial x^n} e(x,t)\bigg|_{x=0} = E_n(t) = 2\sum_{k=0}^{n} \binom{n}{k} \cdot \frac{\partial^k}{\partial x^k} e^{xt} \cdot \frac{\partial^{n-k}}{\partial x^{n-k}} (e^x - 1)^{-1}\bigg|_{x=0},$$

formule qui montre que $E_n(t) \in \mathbf{Z}[1/2][t] \subset \mathbf{Z}_p[t]$, $(p \neq 2)$. Reprenons un argument analogue à celui exposé dans la preuve du lemme 2.3.2. Ainsi, soit un entier $\ell \geq 0$: comme $\ell^p \equiv \ell \ mod\ p$, *le théorème des accroissements finis* permet d'écrire

$$\ell^{np} = (\ell + up)^n \equiv \ell^n \ mod\ np\,\mathbf{Z}_p, \quad (\text{où } u \in \mathbf{Z}_p).$$

Il suit que pour $n \geq 1$ et $N \geq 2$, on a la congruence

$$S_{np}^-(N) = \sum_{1 \leq \ell < N} (-1)^{\ell+1} \ell^{np} \equiv \sum_{1 \leq \ell < N} (-1)^{\ell+1} \ell^n \equiv S_n^-(N) \ mod\ np\,\mathbf{Z}_p.$$

En vertu de la propriété 4), celle-ci est équivalente à la congruence

$$-E_{np}(0) + (-1)^N E_{np}(N) \equiv -E_n(0) + (-1)^N E_n(N) \ mod\ np\,\mathbf{Z}_p. \ (p \neq 2)$$

que l'on écrit sous la forme

$$(-1)^N \{E_{np}(N) - E_n(N)\} \equiv E_{np}(0) - E_n(0) \ mod\ np\,\mathbf{Z}_p. \tag{1}$$

Prenons N entier positif et congru à $\frac{1}{2}$ modulo $p\,\mathbf{Z}_p$. Ecrivons

$$N = \frac{p+1}{2} + c \cdot p \text{ avec } c \text{ entier},$$

et choisissons c de sorte que N soit pair. Comme les polynômes d'Euler sont à coefficients entiers p-adiques et satisfont à la propriété d'Appell, après application du *théorème des accroissements finis*, le membre de gauche de (1) devient

$$\begin{aligned}(-1)^N \{E_{np}(N) - E_n(N)\} &= E_{np}\left(\frac{1}{2} + N - \frac{1}{2}\right) - E_n\left(\frac{1}{2} + N - \frac{1}{2}\right) \\ &\equiv E_{np}\left(\frac{1}{2}\right) - E_n\left(\frac{1}{2}\right) \ mod\ np\,\mathbf{Z}_p.\end{aligned}$$

Ainsi, quel que soit $n \geq 0$, la congruence suivante est vérifiée

$$E_{np}\left(\frac{1}{2}\right) - E_n\left(\frac{1}{2}\right) \equiv E_{np}(0) - E_n(0) \ mod\ np\,\mathbf{Z}_p. \tag{2}$$

- si $n = 0$, alors les deux membres de (2) sont nuls;
- si $n > 0$ est pair, alors le membre de droite est nul (corollaire 2.4.1);
- si $n > 0$ est impair, alors le membre de gauche est nul (corollaire 2.4.1).

Autrement dit, les congruences suivantes sont vérifiées pour tout $n \geq 0$

$$E_{np}\left(\frac{1}{2}\right) - E_n\left(\frac{1}{2}\right) \equiv 0 \equiv E_{np}(0) - E_n(0) \ mod\ np\,\mathbf{Z}_p.$$

■

Corollaire 2.4.2 *Pour p impair, les polynômes d'Euler vérifient les congruences de Honda*

$$E_{np}(t) \equiv E_n(t^p) \ mod\ np\,\mathbf{Z}_p[t], \quad (n \geq 0).$$

Preuve.- La suite $(E_n(t))_{n\geq 1}$ est une famille d'Appell dans $\mathbf{Z}_p[t]$ $(p \neq 2)$. En $a = 0$ et $a = \frac{1}{2}$, la congruence

$$E_{np}(a) - E_n(a) \ mod\ np\,\mathbf{Z}_p$$

est vérifiée, quel que soit n. Le théorème 2.1.1 s'applique et entraîne la congruence à démontrer. ■

Corollaire 2.4.3 *La série formelle*

$$e(x) = \sum_{n\geq 1} E_n(t)\frac{x^n}{n}$$

donne naissance à un groupe formel

$$F_e(x, y) = e^{-1}(e(x) + e(y))$$

sur l'anneau des polynômes de Laurent en $t - 1/2$, $\mathbf{Z}_p\left[t, (t-\frac{1}{2})^{-1}\right]$, $(p \neq 2)$, isomorphe au groupe multiplicatif.

Preuve.- La série formelle $e(x) = \sum_{n\geq 1} E_n(t)\frac{x^n}{n}$ est de type $p - T$ sur $A = \mathbf{Z}_p\left[t, (t-\frac{1}{2})^{-1}\right]$. Puis, comme $E_1(t) = t - \frac{1}{2}$, alors $E_1^{-1} \in A$ et le point (i) du LEF permet de conclure. ■

Comme nous l'avons déjà vu dans le cas général (proposition 1.5.1) ainsi que pour les polynômes de Bernoulli, la congruence de Honda assure l'existence d'une fonction limite définie sur un domaine contenant la lemniscate L_{r_e}. Le lemme suivant, résultat élémentaire bien connu, nous permettra de déterminer la fonction limite propre aux polynômes d'Euler.

Lemme 2.4.1 *Si $x \in \mathbf{Z}_p^\times$, alors la suite $\left(x^{p^n}\right)_{n\geq 0}$ converge vers le nombre p-adique $\zeta \in \mathbf{Z}_p$ défini par*

$$\begin{aligned} \zeta &\equiv x \ mod\, p\mathbf{Z}_p; \\ \zeta &\in \mu_{p-1}. \end{aligned}$$

Preuve.- Comme $x^p \equiv x \ mod\, p\mathbf{Z}_p$, alors

$$x^{p^n} = (x+up)^{p^{n-1}} \equiv x^{p^{n-1}} \ mod\, p^n\mathbf{Z}_p, \ \ (u \in \mathbf{Z}_p).$$

et ainsi

$$\left|x^{p^n} - x^{p^{n-1}}\right| \leq |p^n|.$$

Donc, $\left(x^{p^n}\right)$ est une suite de Cauchy dans $\mathbf{Z}_p^\times$ complet. Si l'on pose $\zeta = lim_{n-\infty} x^{p^n}$, alors évidemment $\zeta^p = \zeta$ c'est-à-dire $\zeta \in \mu_{p-1}$. La congruence

$$\zeta \equiv x \ mod\, p\mathbf{Z}_p$$

résulte du passage à la limite dans la relation

$$x^{p^n} \equiv x \ mod\, p\mathbf{Z}_p.$$

■

Proposition 2.4.3 *Soit m un entier pair non nul et ϵ_m la fonction définie sur la lemniscate p-adique ($p \neq 2$), $L_{r_e} = \{x \in \mathbf{C}_p \ : \ |x^p - x| \leq r_e\}$ par limite*

$$\epsilon_m(a) := \lim_{\nu-\infty} E_{mp^\nu}(a);$$

alors

- $\epsilon_m(a) = 0$, *si* $a \in B_{\leq r_e}(0) \cup B_{\leq r_e}(1)$;
- $\epsilon_m(a) = 2\sum_{j=1}^{k-1}(-1)^{k-j-1}\zeta_j^m$, *si* $a \in B_{\leq r_e}(k)$

  avec $2 \leq k \leq p-1$ *et où* $\zeta_j \in \mu_{p-1}$ *et* $\zeta_j \equiv j \ mod\, p\mathbf{Z}_p$.

Remarques.- **1)** Dans le cas particulier où $p-1$ divise m, l'image de ϵ_m se réduit aux deux éléments $\{0,2\}$. Plus précisément

$$\epsilon_m(a) = \begin{cases} 0 & \text{si } a \in B_{\leq r_e}(k) \text{ avec } k = 0 \text{ ou } k \text{ impair;} \\ 2 & \text{si } a \in B_{\leq r_e}(k) \text{ avec } k \text{ pair non nul.} \end{cases}$$

2) Nous ne donnons pas d'énoncé pour le cas m impair, parce que le résultat correspondant, bien qu'essentiellement identique à celui du cas m pair, nécessite des notations que nous jugeons trop lourdes et dont nous décidons de faire l'économie.

Preuve de la proposition 2.4.3.- Comme m est pair et p impair, le corollaire 2.4.1 et la proposition 2.4.1 montrent que

$$E_{mp^\nu}(0) = E_{mp^\nu}(1) = 0 \text{ pour tout } \nu \geq 1,$$

si bien que

$$\epsilon_m(0) = \epsilon(1) = 0.$$

La propriété 3) de la proposition 2.4.1, qui s'écrit

$$E_{mp^\nu}(a+1) + E_{mp^\nu}(a) = 2a^{mp^\nu}$$

se traduit à la limite $\nu \to \infty$, par

$$\epsilon_m(a+1) = -\epsilon_m(a) + 2 \cdot \begin{cases} \zeta_a^m & \text{avec } \zeta_a \in \mu_{p-1} \text{ et } \zeta_a \equiv a \ mod\, p\mathbf{Z}_p, \text{ si } a \not\equiv 0 \ mod\, p\mathbf{Z}_p; \\ 0 & \text{si } a \equiv 0 \ mod\, p\mathbf{Z}_p; \end{cases}$$

d'où la proposition. ∎

Il existe une relation entre les nombres de Bernoulli et les coefficients constants des polynômes d'Euler. Celle-ci nous permettra d'établir l'existence d'autres fonctions limites issues de sous-suites de ces polynômes.

Lemme 2.4.2 *Pour $n \geq 1$, on a la relation*

$$E_n(0) = -\frac{2(2^{n+1}-1)}{n+1} b_{n+1}.$$

Preuve.- En utilisant les définitions des fonctions génératrices concernées, on a

$$\begin{aligned}
-\sum_{n\geq 1} \frac{2(2^{n+1}-1)}{n+1} b_{n+1} \frac{x^n}{n!} &= -2\sum_{n\geq 1} 2^{n+1} \frac{b_{n+1}}{n+1} \frac{x^n}{n!} + 2\sum_{n\geq 1} b_{n+1} \frac{x^n}{(n+1)!} \\
&= -\frac{2}{x} \sum_{n\geq 1} b_{n+1} \frac{(2x)^{n+1}}{(n+1)!} + \frac{2}{x} \sum_{n\geq 1} b_{n+1} \frac{x^{n+1}}{(n+1)!} \\
&= -\frac{2}{x} \left\{ \frac{2x}{e^{2x}-1} - 1 + x \right\} + \frac{2}{x} \left\{ \frac{x}{e^x - 1} - 1 + \frac{x}{2} \right\} \\
&= -\frac{4}{e^{2x}-1} + \frac{2}{e^x - 1} - 1 \\
&= \frac{2}{e^x + 1} - 1 \\
&= \sum_{n\geq 1} E_n(0) \frac{x^n}{n!}.
\end{aligned}$$

∎

Proposition 2.4.4 *Pour tous entiers $m \geq 0$, ℓ et k, la suite*

$$(E_{mp^\nu+k}(\ell))_{\nu \geq \nu_0}$$

converge dans $\mathbf{Z}_p$. *($p \neq 2$).*

Preuve.- Le lemme précédent associé au théorème 2.3.3 montre que la suite

$$(E_{mp^\nu+k}(0))_{\nu \geq \nu_0}$$

converge. Le reste de la proposition se démontre par induction en utilisant les propriétés

$$E_{mp^\nu+k}(\ell+1) = 2\ell^{mp^\nu+k} - E_{mp^\nu+k}(\ell) \quad \text{et} \tag{3}$$

$$(-1)^{m+k+1} E_{mp^\nu+k}(-\ell) = E_{mp^\nu+k}(\ell) - 2\ell^{mp^\nu+k} \tag{6}$$

de la proposition 2.4.1.

Nous terminons ce chapitre en nous permettant d'énoncer une conjecture concernant les polynômes d'Euler. Soit $(q_n(t))_{n\geq 0}$ la suite des polynômes définie par l'identité de Spitzer

$$\exp\left(\sum_{n\geq 1} E_n(t)\frac{x^n}{n}\right) = 1 + \sum_{n\geq 1} q_n(t)x^n.$$

Les premiers termes de cette suite sont

$$\begin{aligned}
q_1(t) &= E_1(t) = t - \tfrac{1}{2};\\
q_2(t) &= t^2 - t - \tfrac{1}{8};\\
q_3(t) &= t^3 - \tfrac{3}{2}t^2 + \tfrac{3}{2}t + \tfrac{1}{16};\\
q_4(t) &= t^4 - 2t^3 + \tfrac{3}{4}t^2 + \tfrac{1}{4}t - \tfrac{5}{128};\\
q_5(t) &= t^5 - \tfrac{5}{2}t^4 + \tfrac{5}{4}t^3 + \tfrac{5}{8}t^2 - \tfrac{25}{128}t - \tfrac{23}{256}.
\end{aligned}$$

On constate alors que

$$\begin{aligned}
q_3(t) &\equiv q_1(t^3) \ mod\ 3\,\mathbf{Z}_3[t],\\
q_5(t) &\equiv q_1(t^5) \ mod\ 5\,\mathbf{Z}_5[t].
\end{aligned}$$

Plus loin

$$\begin{aligned}
q_{10}(t) &\equiv q_2(t^5) \ mod\ 5\,\mathbf{Z}_5[t],\\
q_9(t) &\equiv q_3(t^3) \ mod\ 9\,\mathbf{Z}_3[t].
\end{aligned}$$

Ces quelques essais numériques, ajoutés à bien d'autres, justifient l'affirmation suivante.

Conjecture 2.4.1 *Les polynômes $q_n(t)$ vérifient les congruences de Honda*

$$q_{np}(t) \equiv q_n(t^p) \ mod\ np\,\mathbf{Z}_p[t],\ (p \neq 2).$$

2.5 Polynômes d'Hermite

Définition 2.5.1 *Les polynômes $H_n(t)$, définis par le développement en série*

$$e^{2xt-x^2} = \sum_{n\geq 0} H_n(t)\frac{x^n}{n!},$$

sont appelés polynômes d'Hermite.

En voici la liste des six premiers

$$\begin{aligned} H_0(t) &= 1; \\ H_1(t) &= 2t; \\ H_2(t) &= 4t^2 - 2; \\ H_3(t) &= 8t^3 - 12t; \\ H_4(t) &= 16t^4 - 48t^2 + 12; \\ H_5(t) &= 32t^5 - 160t^3 + 120t. \end{aligned}$$

Ils possèdent, entre autres, les propriétés suivantes.

Proposition 2.5.1

1) *La suite $(H_n(t))_{n\geq 0}$ satisfait la formule de récurrence*

$$H_{n+1}(t) = 2tH_n(t) - 2nH_{n-1}(t);$$

2) *La dérivée $H_n'(t)$ s'écrit*

$$H_n'(t) = 2nH_{n-1}(t), \quad (n \geq 1);$$

3) *Le polynôme $H_n(t)$ admet le développement explicite*

$$H_n(t) = \sum_{m=0}^{[\frac{n}{2}]} (-1)^m \frac{n!}{m!(n-2m)!}(2t)^{n-2m}.$$

Preuve.- Notons $h(x,t)$, la fonction génératrice

$$h(x,t) = e^{2xt-x^2};$$

on a alors

$$\frac{\partial}{\partial x}h(x,t) = (2t-2x)h(x,t),$$

et donc

$$\frac{\partial^{n+1}}{\partial x^{n+1}}h(x,t) = (2t-2x)\frac{\partial^n}{\partial x^n}h(x,t) - 2n\frac{\partial^{n-1}}{\partial x^{n-1}}h(x,t).$$

L'évaluation en $x = 0$ de cette dernière égalité fournit exactement la formule de récurrence 1).
En dérivant la fonction génératrice $h(x,t)$ par rapport à t, on obtient

$$\sum_{n\geq 0} H_n'(t)\frac{x^n}{n!} = 2\sum_{n\geq 0} H_n(t)\frac{x^{n+1}}{n!},$$

identité de laquelle ressort la "propriété d'Appell"

$$H_n'(t) = 2nH_{n-1}(t), \ \ (n \geq 1).$$

La formule explicite 3) s'établit par induction et à l'aide de la formule de récurrence 1). ∎

Proposition 2.5.2 *Les polynômes d'Hermite vérifient les congruences*

$$H_{np}(t) \equiv H_n(t^p) \ mod\, n\, \mathbf{Z}_p[t], \ \ (p \neq 2, n \geq 0).$$

Preuve.- Remarquons tout d'abord que, par définition, $H_n(t)$ est à coefficients dans Z. La propriété

$$H_n'(t) = 2nH_{n-1}(t) \ \ (n \geq 1),$$

et le fait que

$$H_n(0) = \begin{cases} 0 & \text{si } n = 2m+1 \\ (-1)^m \frac{(2m)!}{m!} & \text{si } n = 2m, \end{cases}$$

montrent que la famille $\left(\bar{H}_n(t)\right)_{n\geq 0}$ définie par

$$\bar{H}_n(t) := p \cdot H_n\left(\frac{t}{2}\right), \ \ (n \geq 0),$$

est une famille d'Appell dans $\mathbf{Z}_p[t]$. De plus, comme $H_n(0) \equiv 0 \ mod\, n$, on a

$$\bar{H}_{np}(0) \equiv \bar{H}_n(0) \ mod\, np\, \mathbf{Z}_p.$$

Le théorème 2.1.1 montre alors que

$$\bar{H}_{np}(t) - \bar{H}_n(t^p) = pH_{np}\left(\frac{t}{2}\right) - pH_n\left(\frac{t^p}{2}\right) \ mod\, np\, \mathbf{Z}_p[t].$$

La substitution $t \mapsto 2t$ fournit la congruence

$$H_{np}(t) \equiv H_n(2^{p-1}t^p) \ mod\, n\, \mathbf{Z}_p[t].$$

Grâce au *théorème des accroissements finis*, pour $p \neq 2$, celle-ci peut s'écrire

$$H_{np}(t) \equiv H_n(t^p) \ mod\, n\, \mathbf{Z}_p[t].$$

∎

Remarque.- Cette suite n'intervient, dans notre propos[7], qu'en tant qu'exemple d'application du théorème 2.1.1. En effet, le résultat suivant est plus fort et s'établit plus simplement.

Proposition 2.5.3 *On a la congruence*

$$H_n(t) \equiv (2t)^n \ mod\ n\,\mathbf{Z}[t].$$

Preuve[8].- Remarquons tout d'abord que $H_1(t) = 2t$ confirme la proposition. Considérons la formule explicite

$$H_n(t) = \sum_{m=0}^{[\frac{n}{2}]} (-1)^m \frac{n!}{m!(n-2m)!}(2t)^{n-2m}.$$

Si $m \geq 1$, alors

$$\begin{aligned} \frac{n!}{m!(n-2m)!} &= \frac{n!}{(2m)!(n-2m)!} \cdot \frac{(2m)!}{m!} = \binom{n}{2m}\frac{(2m)!}{m!} = \\ &= \frac{n}{2m}\binom{n-1}{2m-1}\frac{(2m)!}{m!} = n\binom{n-1}{2m-1}\frac{(2m-1)!}{m!} \\ &\equiv 0 \ mod\ n. \end{aligned}$$

■

Corollaire 2.5.1

1) *Si* $[\alpha_\nu] \in \mathbf{Z}_p(1)$ *et* $m \geq 1$, *alors*

$$\lim_{\nu\to\infty} H_{mp^\nu}(\alpha_\nu) = \begin{cases} 0 & si\ p = 2; \\ \zeta_2^m & si\ p\ est\ impair; \end{cases}$$

2) *Si* $m \geq 1$ *et* $a \in L_{r_\epsilon}$, *alors*

$$\lim_{\nu\to\infty} H_{mp^\nu}(a) = \begin{cases} 0 & si\ a \in B_{\leq r_\epsilon}(0)\ ou\ si\ p = 2; \\ \zeta_2^m\zeta_i^m & si\ a \in B_{\leq r_\epsilon}(i)\ avec\ i \in \{1,\ldots,p-1\}, \\ & p\ impair\ et\ \zeta_\epsilon \in \mu_{p-1}. \end{cases}$$

Plus généralement, quels que soient les entiers $m \geq 0$, $r \geq 0$ *et* $a \in L_{r_\epsilon}$, *la suite*

$$(H_{mp^\nu+r}(a))_{\nu\geq 0}$$

converge dans $\mathbf{C}_p$. *De plus, si l'on note* $h_{m,r}(a)$ *sa limite, alors*

$$\begin{aligned} h_{m,1}(a) &= 2ah_{m,0}(a); \\ h_{m,r}(a) &= 2ah_{m,r-1}(a) - 2(r-1)h_{m,r-2}(a). \end{aligned}$$

[7]Pour d'autres résultats concernant les polynômes d'Hermite (congruences, polygones de Newton, etc ...) voir [37].

[8]Pour une autre démonstration, voir [11]

Preuve.- Si $[\alpha_\nu] \in \mathbf{Z}_p(1)$, alors $\alpha_\nu^{p^\nu} = 1$, alors grâce au lemme 2.4.1, on a

$$\lim_{\nu \to \infty} H_{mp^\nu}(\alpha_\nu) = \lim_{\nu \to \infty} 2^{mp^\nu} = \begin{cases} 0 & \text{si } p = 2; \\ \zeta_2^m & \text{si } p \text{ est impair.} \end{cases}$$

De même, si $a \in L_{r_e}$, alors la limite

$$\lim_{\nu \to \infty} H_{mp^\nu}(a) = \lim_{\nu \to \infty} 2^{mp^\nu} a^{mp^\nu}$$

existe et vaut

- 0 si $a \in B_{\leq r_e}(0)$ ou si $p = 2$ et
- $\zeta_2^m \zeta_i^m$ si $a \in B_{\leq r_e}(i)$ avec $i \in \{1, \ldots, p-1\}$ si p est impair.

Finalement, la formule de récurrence

$$H_{mp^\nu + r}(a) = 2aH_{mp^\nu + r-1}(a) - 2(mp^\nu + r - 1)H_{mp^\nu + r-2}(a)$$

donne, à la limite $\nu \to \infty$

$$h_{m,r}(a) = 2ah_{m,r-1}(a) - 2(r-1)h_{m,r-2}(a).$$

■

J'aimais et j'aime encore les mathématiques pour elles-mêmes comme n'admettant pas l'hypocrisie et le vague, mes deux bêtes d'aversion.

Stendhal

Chapitre 3

POLYNOMES DE TCHEBYCHEV

3.1 Définitions et propriétés

Définition 3.1.1 *Les* polynômes de Tchebychev *de première espèce $T_n(t)$, et de seconde espèce $U_n(t)$, sont définis par les développements en série*

$$\frac{1-tx}{1-2tx+x^2} = \sum_{n\geq 0} T_n(t)x^n;$$
$$\frac{1}{1-2tx+x^2} = \sum_{n\geq 0} U_n(t)x^n.$$

Par exemple

$$\begin{array}{lllllll} T_0(t) &=& 1; & & U_0(t) &=& 1; \\ T_1(t) &=& t; & & U_1(t) &=& 2t; \\ T_2(t) &=& 2t^2-1; & & U_2(t) &=& 4t^2-1; \\ T_3(t) &=& 4t^3-3t; & & U_3(t) &=& 8t^3-4t; \\ T_4(t) &=& 8t^4-8t^2+1; & & U_4(t) &=& 16t^4-12t^2+1; \\ T_5(t) &=& 16t^5-20t^3+5t; & & U_5(t) &=& 32t^5-32t^3+6t. \end{array}$$

L'objet de ce chapitre consiste en l'étude des polynômes de Tchebychev de première espèce. La proposition suivante dresse une liste de quelques-unes de leurs remarquables propriétés.

Proposition 3.1.1 *Les polynômes $T_n(t)$ ont les propriétés suivantes*

1) $T_{n+1}(t) = 2tT_n(t) - T_{n-1}(t), \ (n \geq 1);$

2) $T_n(\cos\theta) = \cos n\theta, \ (n \geq 0);$

3) $T_n \circ T_m = T_{nm} = T_m \circ T_n, \ (n, m \geq 0);$

4) $T_n'(t) = nU_{n-1}(t), \ (n \geq 1).$

Preuve.- Nous allons montrer que

$$g(x,t) := \sum_{n\geq 1} \{T_{n+1}(t) - 2tT_n(t) + T_{n-1}(t)\}\, x^n = 0.$$

A cet effet, appelons $f(x,t)$ la fonction génératrice

$$f(x,t) = T_0(t) + \sum_{n\geq 1} 2T_n(t)x^n.$$

On a alors

$$\begin{aligned} g(x,t) &= \frac{1}{2x}\{f(x,t) - T_0(t) - 2T_1(t)x\} - \{tf(x,t) - tT_0(t)\} + \frac{x}{2}\{f(x,t) + T_0(t)\} \\ &= f(x,t)\left(\frac{1}{2x} - t + \frac{x}{2}\right) - \frac{1}{2x} + \frac{x}{2} \\ &= f(x,t)\frac{1-2tx+x^2}{2x} - \frac{1}{2x} + \frac{x}{2} \\ &= 0, \end{aligned}$$

ce qui établit la relation de récurrence 1).
Des formules d'addition

$$\cos(n+1)\theta = \cos n\theta\cos\theta - \sin n\theta\sin\theta,$$
$$\cos(n-1)\theta = \cos n\theta\cos\theta + \sin n\theta\sin\theta,$$

on tire la relation

$$\cos(n+1)\theta = 2\cos\theta\cos n\theta - \cos(n-1)\theta.$$

On en déduit, par induction, la propriété 2), à savoir

$$T_n(\cos n\theta) = \cos n\theta, \quad (n \geq 0).$$

Et la propriété 3) est un corollaire immédiat de cette dernière. Finalement, l'identité

$$(1-x^2)\sum_{n\geq 0} U_n(t)x^n = T_0(t) + \sum_{n\geq 1} 2T_n(t)x^n$$

entraîne la relation

$$U_n(t) = 2T_n(t) - U_{n-2}(t), \ (n \geq 1),$$

qui permet d'établir, par induction et grâce à la propriété 2), le fait que, pour $n \geq 0$

$$U_n(\cos\theta) = \frac{\sin(n+1)\theta}{\sin\theta}. \tag{1}$$

Dès lors, en dérivant, par rapport à θ, l'identité

$$T_n(\cos\theta) = \cos n\theta,$$

on obtient

$$-\sin\theta \cdot T_n'(\cos\theta) = -n\sin n\theta$$

ou encore [grâce à (2)]

$$T_n'(\cos\theta) = nU_{n-1}(\cos\theta),$$

c'est-à-dire la propriété 4). ∎

Remarque.- Conformément à ce que nous annoncions en section 1.4. cette proposition montre que le polynôme $T_n(t) \in \mathbf{Z}[t]$ est une pseudo-puissance n.

3.2 La congruence de Honda

Théorème 3.2.1 [1] *Les polynômes de Tchebychev de première espèce vérifient la congruence*

$$2T_{np}(t) \equiv 2T_n(t^p) \ mod\ np\,\mathbf{Z}_p[t], \quad (n \geq 0).$$

Preuve.- Il s'agit d'appliquer le théorème de Barsky (th. 1.3.1) à la série formelle

$$f(x) = \sum_{n\geq 1} 2T_n(t)\frac{x^n}{n} \in \mathbf{Q}[t][[x]],$$

en montrant que $\exp(f(x)) \in \mathbf{Z}_p[t][[x]]$. Mais, puisque (cf. [28])

$$T_0(t) + \sum_{n\geq 1} 2T_n(t)x^n = \frac{1-x^2}{1-2tx+x^2},$$

on a

$$\begin{aligned} f(x) &= \int_0^x \left(\frac{1-\xi^2}{1-2t\xi+\xi^2} - T_0(t)\right)\frac{d\xi}{\xi} \\ &= \int_0^x \left(\frac{1-\xi^2-1+2t\xi-\xi^2}{1-2t\xi+\xi^2}\right)\frac{d\xi}{\xi} \\ &= -\int_0^x \frac{2\xi-2t}{1-2t\xi+\xi^2}d\xi \\ &= -\log(1-2t\xi+\xi^2)\Big|_0^x \\ &= -\log\left(1-2tx+x^2\right); \end{aligned}$$

si bien qu'apparaît la remarquable relation

$$\exp(f(x)) = \frac{1}{1-2tx+x^2},$$

c'est-à-dire l'identité de Spitzer (découverte par C. Vonlanthen)

$$\exp\left(\sum_{n\geq 1} 2T_n(t)\frac{x^n}{n}\right) = \sum_{n\geq 0} U_n(t)x^n.$$

[1] Ce théorème améliore très nettement la congruence

$$T_{kp}(t) \equiv T_k(t)^p \ mod\ p,$$

de R. Askey, présentée dans [7], (proposition 3.4).

En application du point (ii) du théorème 1.3.1, la congruence de Honda

$$2T_{np}(t) \equiv 2T_n(t^p) \ mod\ np\,\mathbf{Z}_p[t]$$

a donc lieu pour tout $n \geq 0$. ∎

Autre démonstration.- Le fait que

$$T_n(\cos\theta) = \cos n\theta$$

se traduit par l'identité formelle

$$T_n\left(\frac{x+x^{-1}}{2}\right) = \frac{x^n + x^{-n}}{2}.$$

On pose $n = p$ impair et on effectue le changement de variables $t = \frac{x+x^{-1}}{2}$, pour retrouver la congruence

$$T_p(t) = \frac{x^p + x^{-p}}{2} \equiv \left(\frac{x+x^{-1}}{2}\right)^p = t^p \ mod\ p\,\mathbf{Z}_p[t];$$

en d'autres termes

$$T_p(t) \equiv T_1(t^p) \ mod\ p\,\mathbf{Z}_p[t].$$

Maintenant, si $n = mp^\nu$, avec $\nu \geq 0$ et $(m,p) = 1$, alors, grâce au *théorème des accroissements finis* et aux propriétés 3) et 4) de la proposition 3.1.1, on obtient

$$\begin{aligned} T_{np}(t) &= T_{mp^{\nu+1}}(t) \\ &= T_{mp^\nu}(T_p(t)) \\ &= T_{mp^\nu}(t^p + pr(t)) \quad \text{avec } r(t) \in \mathbf{Z}_p[t] \\ &\equiv T_{mp^\nu}(t^p) \ mod\ p^{\nu+1}\,\mathbf{Z}_p[t] \\ &\equiv T_n(t^p) \ mod\ np\,\mathbf{Z}_p[t]. \end{aligned}$$

∎

Pour le cas $p = 2$, la congruence du théorème 3.2.1 peut être précisée comme suit.

Proposition 3.2.1 *Pour tout $n \geq 0$, la congruence suivante est vérifiée*

$$T_{2n}(t) \equiv (-1)^n \ mod\ 2n\,\mathbf{Z}_2[t].$$

Preuve.- En utilisant les propriétés 3) et 4) de la proposition 3.1.1, ainsi que le *théorème des accroissements finis*, on peut écrire

$$T_{2n}(t) = T_n \circ T_2(t) = T_n\left(2t^2 - 1\right) \equiv T_n(-1) \ mod\ 2n\,\mathbf{Z}_2[t].$$

Comme

$$T_n(\cos\theta) = \cos n\theta,$$

alors

$$T_n(-1) = \begin{cases} -1 & \text{si } n \text{ est impair} \\ 1 & \text{si } n \text{ est pair,} \end{cases}$$

et ainsi

$$T_{2n}(t) \equiv (-1)^n \ mod\ 2n\,\mathbf{Z}_2[t].$$

■

Corollaire 3.2.1 *Si $p \neq 2$, la série formelle*

$$\tau(x) = \sum_{n\geq 1} T_n(t)\frac{x^n}{n}$$

donne naissance au groupe formel

$$F_\tau(x,y) = \tau^{-1}(\tau(x) + \tau(y)),$$

défini sur $\mathbf{Z}_p[t,t^{-1}]$ et isomorphe au groupe formel multiplicatif.

Preuve.- Le théorème 3.2.1 prouve que, pour $p \neq 2$, la série formelle $\tau(x)$ est de type $p-T$ et possède une inverse dans l'anneau $A = \mathbf{Z}_p[t,t^{-1}]$. On conclut en appliquant le point (i) du LEF.

■

Remarques.- **1)** L'isomorphisme de groupes formels

$$h(x) : F_\tau(x,y) \to G_m(x,y)$$

donné par

$$\begin{aligned} h(x) &= \exp(\tau(x)) - 1 \\ &= \frac{1}{\sqrt{1-2tx+x^2}} - 1 \\ &= \sum_{n\geq 1} P_n(t)x^n, \end{aligned}$$

fait intervenir une suite $(P_n(t))_{n\geq 1}$: la famille des polynômes de Legendre. Comme nous le verrons au chapitre 4, ces derniers satisfont, eux aussi, aux congruences de Honda. Ainsi, à l'image de ce que nous conjecturions au sujet des polynômes d'Euler (cf. Conjecture 2.4.1), nous avons en main deux suites de polynômes $(T_n(t))_{n\geq 1}$ et $(P_n(t))_{n\geq 1}$, liées par l'identité de Spitzer

$$\exp\left(\sum_{n\geq 1} T_n(t)\frac{x^n}{n}\right) = \sum_{n\geq 0} P_n(t)x^n,$$

et vérifiant, toutes deux, les congruences de Honda.

2) Notons que ces dernières n'ont pas lieu pour la famille $(U_n(t))_{n\geq 0}$. Pour preuve, les différences suivantes

$$\begin{aligned} U_3(t) - U_1(t^3) &= 6t^3 - 4t \equiv -4t \ mod\ 3; \\ U_5(t) - U_1(t^5) &= 30t^5 - 32t^3 + 6t \equiv -2t^3 + t \ mod\ 5. \end{aligned}$$

3.3 Une fonction limite

Le but de cette section est de déterminer la fonction limite relative aux polynômes de Tchebychev et définie par la proposition 1.5.1. Nous distinguons le cas $p = 2$ du cas p impair.

Proposition 3.3.1 *Pour tout $a \in B_{\leq 1}(0) \subset \mathbf{C}_2$ et quel que soit $m \geq 0$*

$$\lim_{\nu \to \infty} T_{m2^\nu}(a) = 1.$$

Preuve.- En vertu de la proposition 3.2.1, il existe $r_\nu(t) \in \mathbf{Z}_2[t]$, tel que

$$T_{m2^\nu}(a) = 1 + \mathrm{m}2^\nu r_\nu(a). \quad (\nu > 1).$$

Puis, comme $|a| \leq 1$, alors $|r_\nu(a)| \leq 1$ et donc

$$\lim_{\nu \to \infty} T_{m2^\nu}(a) = 1.$$

■

Avant d'exhiber la fonction limite relative au cas p impair, énonçons un résultat concernant les points fixes de $T_p(t)$.

Lemme 3.3.1 *Si p est impair et si $\xi_0, \xi_1, \ldots, \xi_{p-1}$ désignent les p points fixes du polynôme $T_p(t)$, convenablement numérotés, c'est-à-dire les p solutions de l'équation $T_p(t) = t$, alors*

$$\xi_\ell \in \mathbf{Z}_p \quad et \quad \xi_\ell \equiv \ell \ mod\ p\mathbf{Z}_p, \quad pour \quad \ell = 0, \ldots, p-1.$$

Preuve.- La propriété 3) de la proposition 3.1.1 montre que

$$T_k(0) = 0 \text{ pour tout } k \text{ impair};$$

en particulier

$$T_p(0) = 0,$$

et on peut prendre $\xi_0 = 0$. Considérons, maintenant, le polynôme

$$h(t) := T_p(t) - t.$$

Par la proposition 3.1.1, sa dérivée est

$$h'(t) = pU_{p-1}(t) - 1.$$

Soit $\ell \in \{1, \ldots, p-1\}$. Grâce à la congruence de Houda, on a

$$h(\ell) = T_p(\ell) - \ell \equiv \ell^p - \ell \equiv 0 \ mod\, p\,\mathbf{Z}_p; \tag{1}$$

Par ailleurs, puisque $U_{p-1}(t) \in \mathbf{Z}_p[t]$

$$|h'(\ell)| = |pU_{p-1}(\ell) - 1| = 1:$$

et donc

$$h'(\ell) \not\equiv 0 \ mod\, p\,\mathbf{Z}_p. \tag{2}$$

Les expressions (1) et (2) constituent les hypothèse dudit *Lemme de Hensel* ([2], [3], [36]). Ce dernier montre qu'il existe un unique entier p-adique ζ_ℓ, congru à ℓ modulo $p\,\mathbf{Z}_p$ et racine de $h(t) = 0$, autrement dit, point fixe de $T_p(t)$. ∎

Il est maintenant loisible de déterminer la fonction limite à laquelle nous faisions allusion plus haut.

Proposition 3.3.2 *Soit p impair, $m \geq 1$ et t_m la fonction définie sur la lemniscate L_{r_e} par la limite*

$$t_m(a) = \lim_{\nu \to \infty} T_{mp^\nu}(a);$$

soit encore

$$\{\xi_0 = 0, \xi_1, \ldots, \xi_{p-1}\}$$

l'ensemble des points fixes de $T_p(t)$. Alors

$$t_m(a) = \begin{cases} T_m(0) & si\ a \in B_{\leq r_e}(0); \\ T_m(\xi_\ell) & si\ a \in B_{\leq r_e}(\ell),\ (\ell = 1, \ldots, p-1). \end{cases}$$

Preuve.- Remarquons tout d'abord que, puisque p est impair

$$T_{mp^\nu}(0) = T_m\left(T_{p^\nu}(0)\right) = T_m(0),$$

donc

$$t_m(0) = T_m(0).$$

Maintenant, si $a \in B_{\leq r_a}(\ell)$ avec $\ell = 1, \ldots, p-1$, on calcule

$$\begin{aligned} t_m(a) &= \lim_{\nu \to -\infty} T_{mp^\nu}(a) \\ &= \lim_{\nu \to -\infty} T_m\left(T_{p^\nu}(a)\right) \\ &= T_m\left(\lim_{\nu \to -\infty} T_{p^\nu}(a)\right) \\ &= T_m\left(t_1(a)\right). \end{aligned}$$

Ainsi

$$t_m = T_m \circ t_1.$$

Mais

$$t_1(a) = \lim_{\nu \to -\infty} T_{p^{\nu+1}}(a) = T_p\left(\lim_{\nu \to -\infty} T_{p^\nu}(a)\right) = T_p\left(t_1(a)\right): \tag{1}$$

et comme

$$T_{p^\nu}(x) \equiv T_1\left(x^{p^\nu}\right) = x^{p^\nu} \ mod\ p\,\mathbf{Z}_p[x],$$

cela signifie que

$$\lim_{\nu \to -\infty} T_{p^\nu}(a) = \lim_{\nu \to -\infty} T_{p^\nu}(\ell) \equiv \ell \ mod\ p\mathbf{Z}_p. \tag{2}$$

Il suit, de (1) et (2), que $t_1(a)$ est le point fixe de $T_p(t)$ congru à ℓ modulo $p\mathbf{Z}_p$. ■

3.4 Polygones de Newton

Nous nous proposons de calculer tous les rayons critiques, dans $\mathbf{C}_p$, du polynôme $T_n(t)$, à l'aide des résultats de congruences établis auparavant. Le lemme suivant nous permettra de traiter, d'abord, le cas "spécial" $p = 2$.

Lemme 3.4.1 *Soit, pour $m \geq 1$, le développement explicite du polynôme $T_m(t)$*

$$T_m(t) = \sum_{k=0}^{m} a_k t^k;$$

alors (avec la convention $ord_2(0) = +\infty$)

$$ord_2(a_k) \geq k - 1.$$

Preuve.- Les polynômes $T_1(t) = t$ et $T_2(t) = 2t^2 - 1$ confirment l'affirmation. Pour $m \geq 1$, la formule de récurrence

$$T_{m+1}(t) = 2tT_m(t) - T_{m-1}(t)$$

s'écrit, à l'aide des développements des polynômes y apparaissant, comme suit

$$\sum_{k=0}^{m+1} a_k t^k = 2t \sum_{i=0}^{m} b_i t^i - \sum_{\ell=0}^{m-1} c_\ell t^\ell.$$

Admettant l'hypothèse d'induction, on obtient alors

- $a_{m+1} = 2b_m$, donc $ord_2(a_{m+1}) = ord_2(b_m) + 1 \geq m$;
- $a_m = 2b_{m-1}$, donc $ord_2(a_m) = ord_2(b_{m-1}) + 1 \geq m - 1$;
- pour $1 \leq k \leq m-2$, $a_k = 2b_{k-1} - c_k$ et donc 2^{k-1} divise a_k, ce qui signifie que $ord_2(a_k) \geq k - 1$.
- Finalement, comme $T_n(t) \in \mathbf{Z}[t]$ pour tout n, $a_0 = -c_0 \in \mathbf{Z}$, donc $ord_2(a_0) \geq 0$.

■

Proposition 3.4.1 *Si $m \neq 1$ est impair, alors 0 et 2 sont les rayons critiques de $T_m(t)$ dans $\mathbf{C}_2$.*

Preuve.- Comme m est impair, alors $T_m(0) = 0$. D'autre part, si

$$T_m(t) = a_1 t + \cdots + a_m t^m,$$

alors

$$a_1 = T'_m(0) = mU_{m-1}(0) = \pm m \text{ et } a_m = 2^{m-1}.$$

On tire de ceci et du lemme 3.4.1, la construction du polygone de Newton de $T_m(t)$.

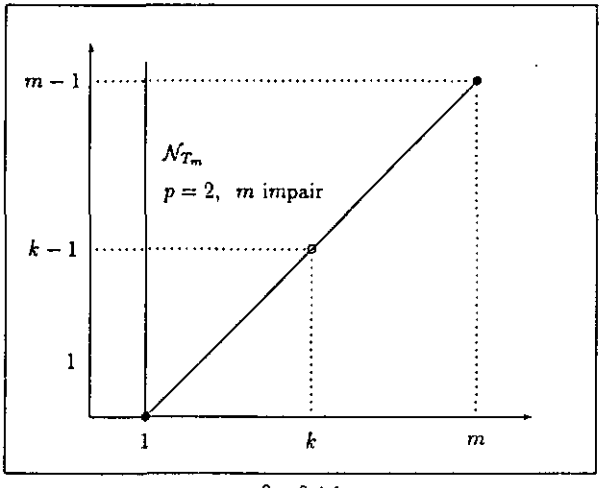

fig. 3.4.1

Ainsi que le montre la figure ci-dessus, celui-ci est constitué d'un segment vertical (de pente $-\infty$) et d'un segment oblique de pente critique égale à 1. ■

Proposition 3.4.2 *Pour $\nu \geq 1$, le polynôme $T_{2^\nu}(t)$ possède, dans C_2, l'unique pente critique*

$$\Delta_\nu = \frac{2^\nu - 1}{2^\nu}.$$

Preuve.- Cette proposition se démontre par induction.
Tout d'abord, si $\nu = 1$, le polygone de Newton de $T_2(t) = 2t^2 - 1$, est bien réduit à un segment de pente $\frac{1}{2} = \Delta_1$.

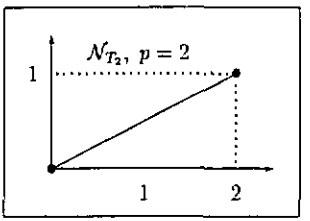

fig. 3.4.2

Maintenant, si $a \in C_2$ est un zéro de $T_{2^{\nu+1}}(t)$, alors

$$T_{2^{\nu+1}}(a) = 0 = T_{2^\nu}(T_2(a)).$$

Ainsi, $b := T_2(a)$ est zéro de $T_{2^\nu}(t)$. Par hypothèse d'induction, ceci signifie que

$$|b| = 2^{1-\frac{1}{2^\nu}} = |2|^{\frac{1}{2^\nu}-1}.$$

Puis, *a annule le polynôme*

$$q(t) := T_2(t) - b = 2t^2 - 1 - b,$$

dont le polygone de Newton est réduit à un segment oblique d'extrémités
$s_0 = (0, ord_2(b)) = (0, \frac{1}{2^\nu} - 1)$, $s_2 = (2, 1)$,

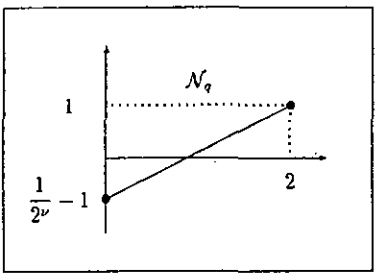

fig. 3.4.3

donc de pente

$$\frac{1}{2}\left(1 + 1 - \frac{1}{2^\nu}\right) = 1 - \frac{1}{2^{\nu+1}} = \frac{2^{\nu+1} - 1}{2^{\nu+1}} = \Delta_{\nu+1}$$

■

Corollaire 3.4.1 *Les zéros du polynôme $T_{2^\nu}(t)$, $(\nu \geq 0)$, sont simples.*

Preuve.- En préambule, notons que si $a \in \mathbf{C}_2 - \{1\}$, alors les deux solutions, dans $\mathbf{C}_2$, de l'équation

$$T_2(t) = a$$

sont distinctes. En effet

$$T_2(t) - a = 2t^2 - 1 - a.$$

Démontrons maintenant, par induction sur $\nu \geq 0$, que les zéros de $T_{2^\nu}(t)$ sont simples. Ceci est évident pour $T_1(t) = t$ et, comme on vient de le voir, pour $T_2(t)$. Soit a l'un des zéros (simples par hypothèse d'induction) de $T_{2^\nu}(t)$. Comme $T_{2^\nu}(1) = 1$, a n'est pas égal à 1 et alors, l'équation $T_2(t) = a$, admet deux solutions b_1 et b_2, distinctes, pour lesquelles

$$T_{2^{\nu+1}}(b_i) = T_{2^\nu}(T_2(b_i)) = T_{2^\nu}(a) = 0.$$

Ainsi, le polynôme $T_{2^{\nu+1}}(t)$ possède dans $\mathbf{C}_2$, les $2^{\nu+1}$ zéros distincts

$$b = T_2^{-1}(a), \text{ avec } a \text{ zéro de } T_{2^\nu}(t).$$

■

Proposition 3.4.3 *Pour $m \neq 1$ impair et $\nu \geq 1$, les deux pentes critiques, dans $\mathbf{C}_2$, du polynôme $T_{m2^\nu}(t)$ sont*

$$\Delta_1 = 1 - \frac{1}{2^\nu} \quad et \quad \Delta_2 = 1.$$

Preuve.- Si a est un zéro de $T_{2^\nu}(t)$, alors, comme m est impair

$$T_{m2^\nu}(a) = T_m(T_{2^\nu}(a)) = T_m(0) = 0.$$

Ainsi $T_{m2^\nu}(t)$ possède la pente critique $\Delta_1 = \frac{2^\nu - 1}{2^\nu}$ (proposition 3.4.2).
D'autre part, si b est tel que $a = T_m(b)$ est un zéro de $T_{2^\nu}(t)$, alors

$$T_{m2^\nu}(b) = T_{2^\nu}(a) = 0.$$

Déterminons $|b|$. Sachant que m est impair et que $|a| = 2^{\frac{2^\nu - 1}{2^\nu}}$, on construit le polygone de Newton du polynôme

$$T_m(t) - a.$$

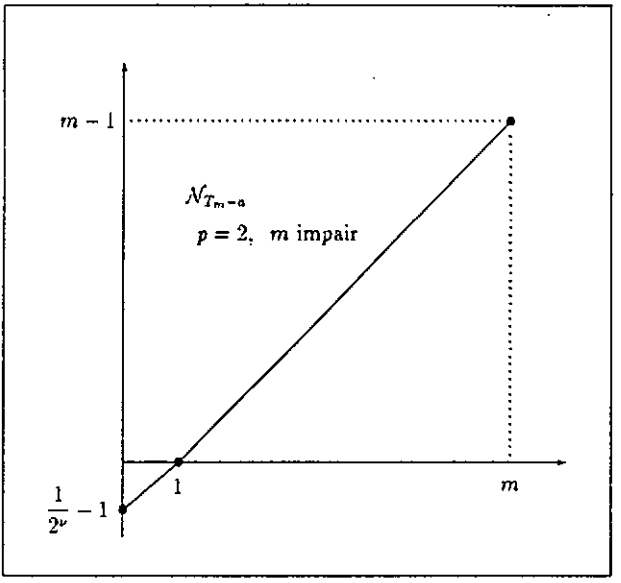

fig. 3.4.4

Comme le montre la figure ci-dessus, ce polygone est constitué de deux segments obliques, l'un de pente $\Delta_1 = 2^{1-\frac{1}{2^\nu}}$, l'autre de pente $\Delta_2 = 1$. ∎

Proposition 3.4.4 *Si p est impair et n pair, alors tous les zéros de $T_n(t)$ se situent sur la sphère-unité $B_{=1}(0)$ de $\mathbf{C}_p$.*

Preuve.- Comme n est pair, le polynôme $T_n(t)$ s'écrit

$$T_n(t) = \pm 1 + \cdots + 2^{n-1}t^n,$$

et, par conséquent, son polygone de Newton est réduit au segment horizontal d'extrémités $(0,0)$ et $(n,0)$. ∎

Proposition 3.4.5 *Si $p \neq 2$ et $\nu \geq 1$, le polynôme de Tchebychev $T_{p^\nu}(t)$ (pour lequel $T_{p^\nu}(0) = 0$) possède dans $\mathbf{C}_p$*

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

zéros, de valeur absolue égale à

$$|p|^{\frac{1}{\varphi(p^k)}} = r_c^{p^{1-k}}, \quad k = 1, \ldots, \nu.$$

Preuve.- Ce résultat est un corollaire de la proposition 1.7.2. En effet, puisque pour tout $\nu \geq 0$

- la congruence de Honda est satisfaite, c'est-à-dire $T_{p^{\nu+1}}(t) \equiv T_{p^\nu}(t^p) \ mod\ p^{\nu+1}\mathbf{Z}_p[t]$;
- le coefficient dominant de $T_p^\nu(t)$, égal à $2^{p^\nu-1}$, est une unité p-adique;
- $T_{p^\nu}(0) = 0$;
- $T'_{p^\nu}(0) = p^\nu U_{p^\nu-1}(0) = \pm p^\nu$;

la suite des polygones de Newton $\mathcal{N}_{T_{p^\nu}}$, $\nu \geq 1$, se laisse construire récursivement.

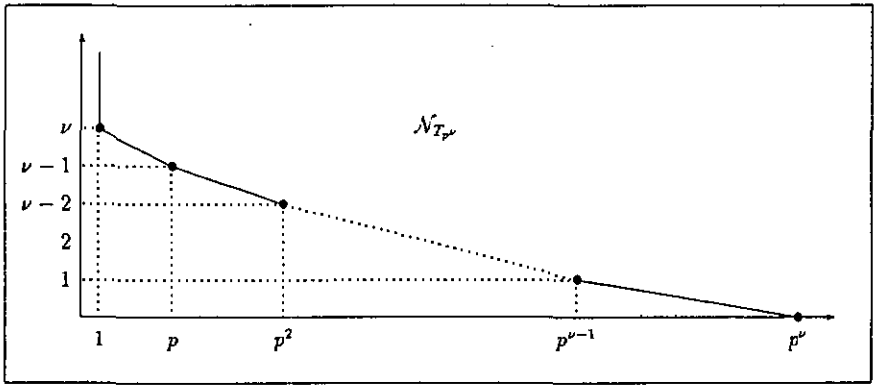

fig. 3.4.5

Ainsi, conformément à la figure ci-dessus, le polygone de Newton de $T_{p^\nu}(t)$ est constitué des segments reliant les points

$$\left(p^k, \nu - k\right), \quad k = 0, \ldots, \nu,$$

ainsi que du segment vertical, provenant du fait que $T_{p^\nu}(0) = 0$. Ceci traduit, précisément, l'énoncé de la proposition. ∎

Corollaire 3.4.2 *Si $p \neq 2$, les zéros de $T_{p^\nu}(t)$ sont simples.*

Preuve.- Si $T_{p^\nu}(a) = 0$, alors, comme nous venons de le voir, $|a| < 1$. Par suite

$$T'_{p^\nu}(a) = p^\nu U_{p^\nu-1}(a)$$

ne saurait être nul. En effet, le polynôme

$$U_{p^\nu-1}(t) = \pm 1 + \cdots + 2^{p^\nu} t^{p^\nu-1}$$

dont le polygone est réduit à un segment horizontal, possède tous ses zéros sur la sphère unité de $\mathbf{C}_p$. ∎

Proposition 3.4.6 *Si $m \neq 1$ est impair et premier à $p \neq 2$, alors le polynôme $T_{mp^\nu}(t)$ possède, outre les zéros de $T_{p^\nu}(t)$, $(m-1)p^\nu$ zéros situés sur la sphère unité de C_p.*

Preuve.- Si a est un zéro de $T_{p^\nu}(t)$, alors, comme m est impair

$$T_{mp^\nu}(a) = T_m\left(T_{p^\nu}(a)\right) = T_m(0) = 0.$$

D'autre part, le polygone de Newton de $T_{mp^\nu}(t)$ s'obtient en adjoignant, à celui de $T_{p^\nu}(t)$, le segment horizontal d'extrémités $(p^\nu, 0)$ et $(mp^\nu, 0)$, qui fait état de $mp^\nu - p^\nu$ zéros de valeur absolue égale à 1. ∎

3.5 Relation avec la fonction $\arcsin x$

Dans toute cette section, p désigne un nombre premier impair.

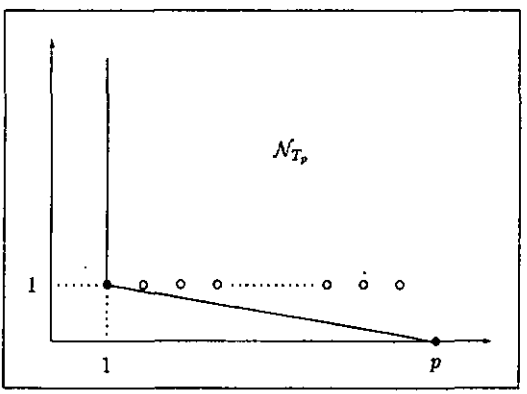

fig. 3.5.1

A l'aide du polygone de Newton du polynôme $T_p(t)$ construit en section 3.4, (cf. figure 3.5.1), on obtient la majoration suivante, pour $T_p(x)$.

$$|T_p(x)| \leq M_r(T_p) = \begin{cases} |p|r & \text{si } 0 \leq r = |x| \leq r_e; \\ r^p & \text{si } r_e \leq |x| = r. \end{cases} \qquad (1)$$

De la propriété de composition

$$T_{mn} = T_m \circ T_n,$$

il suit, immédiatement, que

$$\lim_{\nu \to \infty} T_{p^\nu}(a) = 0$$

quel que soit $a \in B_{<1}(0) \subset \mathrm{C}_p$.
Mais, en regard de la majoration (1), il est préférable de considérer la suite

$$\left(\frac{T_{p^\nu}(a)}{p^\nu}\right),$$

plutôt que $(T_{p^\nu}(a))$ qui tend vers 0 trivialement; d'où l'énoncé suivant.

Théorème 3.5.1 *Quel que soit $a \in B_{<1}(0) \subset \mathrm{C}_p$, la suite $(\tau_\nu)_{\nu\geq 0}$, définie par*

$$\tau_\nu := (-1)^{\frac{p-1}{2}\nu}\,\frac{T_{p^\nu}(a)}{p^\nu},$$

converge dans C_p.

Preuve.- Si $|a| < 1$, l'inégalité (1) fournit l'existence d'un entier $k \geq 0$, pour lequel

$$\left|T_{p^k}(a)\right| \leq r_e.$$

Comme

$$\frac{T_{p^\nu}(a)}{p^\nu} = \frac{1}{p^k}\cdot\frac{T_{p^{\nu-k}}\left(T_{p^k}(a)\right)}{p^{\nu-k}},$$

il suffira de démontrer la convergence de la suite pour les éléments a de la boule $B_{\leq r_e}(0)$.
La différence, $|\tau_{\nu+1} - \tau_\nu|$ peut s'écrire

$$\begin{aligned}
|\tau_{\nu+1} - \tau_\nu| &= \left|(-1)^{\frac{p-1}{2}(\nu+1)}\,\frac{T_{p^{\nu+1}}(a)}{p^{\nu+1}} - (-1)^{\frac{p-1}{2}\nu}\frac{T_{p^\nu}(a)}{p^\nu}\right| \\
&= \left|\frac{1}{p^{\nu+1}}\left\{T_{p^{\nu+1}}(a) - (-1)^{\frac{p-1}{2}}pT_{p^\nu}(a)\right\}\right| \\
&= \frac{1}{\left|p^{\nu+1}\right|}\left|T_p\left(T_{p^\nu}(a)\right) - (-1)^{\frac{p-1}{2}}pT_{p^\nu}(a)\right|.
\end{aligned}$$

Posons $y = T_{p^\nu}(a)$ et estimons

$$\left|T_p(y) - (-1)^{\frac{p-1}{2}}py\right|.$$

Le polynôme

$$q(t) := T_p(t) - (-1)^{\frac{p-1}{2}}pt$$

est divisible par t^3. En effet, $T_p(t)$ a la parité de son indice et de plus

$$T_p'(0) = pU_{p-1}(0) = (-1)^{\frac{p-1}{2}}p.$$

Ainsi, $q(t)$ s' écrit

$$q(t) = a_3t^3 + \cdots + a_pt^p,$$

et alors

$$|q(y)| = \left| T_p(y) - (-1)^{\frac{p-1}{2}} py \right| \leq |y|^3 \cdot \max_{3 \leq i \leq p} |a_i| \, |y|^{i-3} \leq |y|^3.$$

De plus, comme $|a| \leq r_e$, on peut affirmer que

$$|y| = |T_{p^\nu}(a)| = |T_p(T_{p^{\nu-1}}(a))| \leq |p| \cdot |T_{p^{\nu-1}}(a)| \leq \ldots \leq |p|^\nu |a|.$$

Ainsi, on obtient

$$|r_{\nu+1} - r_\nu| \leq \frac{1}{|p^{\nu+1}|} |T_{p^\nu}(a)|^3 \leq \frac{|p|^{3\nu}|a|^3}{|p|^{\nu+1}} \leq |p|^{2\nu-1} \longrightarrow 0 \text{ lorsque } \nu \to \infty.$$

■

Il nous est, dès lors, permis de définir la fonction

$$\begin{array}{rccl} T : & B_{<1}(0) & \longrightarrow & \mathbf{C}_p \\ & a & \longmapsto & T(a) := \lim_{\nu \to \infty} (-1)^{\frac{p-1}{2}\nu} \frac{T_{p^\nu}(a)}{p^\nu}. \end{array}$$

Afin de déterminer sa nature, revenons au lien existant entre polynômes de Tchebychev et fonctions trigonométriques.

Proposition 3.5.1 *Pour tout $n \geq 0$, on a les relations formelles*

1) $T_{2n}(\sin\theta) = (-1)^n \cos 2n\theta$;

2) $T_{2n+1}(\sin\theta) = (-1)^n \sin(2n+1)\theta$.

Preuve.- Dans le but d'éviter l'évocation du nombre π (quel sens dans $\mathbf{C}_p$?), nous effectuons une démonstration entièrement formelle basée sur la formule de récurrence définissant les polynômes de Tchebychev.
Tout d'abord, si $n = 0$, alors $T_0(\sin\theta) = 1$ et $T_1(\sin\theta)$ confirment bien nos affirmations.
Procédons au pas d'induction en employant les formules d'addition des fonctions *sinus* et *cosinus*.
D'une part, pour $n \geq 1$, on a

$$\begin{aligned} T_{2n+1}(\sin\theta) &= 2\sin\theta \cdot T_{2n}(\sin\theta) - T_{2n-1}(\sin\theta) \\ &= (-1)^n 2\sin\theta \cdot \cos 2n\theta - (-1)^{n-1} \sin(2n-1)\theta \\ &= (-1)^n \left(2\sin\theta\cos 2n\theta + \sin 2n\theta \cos\theta - \sin\theta\cos 2n\theta \right) \\ &= (-1)^n \left(\sin\theta\cos 2n\theta + \sin 2n\theta\cos\theta \right) \\ &= (-1)^n \sin(2n+1)\theta; \end{aligned}$$

et d'autre part

$$\begin{aligned} T_{2n}(\sin\theta) &= 2\sin\theta \cdot T_{2n-1}(\sin\theta) - T_{2n-2}(\sin\theta) \\ &= (-1)^{n-1} 2\sin\theta\sin(2n-1)\theta - (-1)^{n-1}\cos(2n-2)\theta \\ &= (-1)^n \left\{ \cos(2n-2)\theta - 2\sin\theta\sin(2n-1)\theta \right\} \\ &= (-1)^n \left\} \cos(2n-1)\theta\cos\theta + \sin\theta\sin(2n-1)\theta - 2\sin\theta\sin(2n-1)\theta \right\} \\ &= (-1)^n \left\{ \cos(2n-1)\theta\cos\theta - \sin\theta\sin(2n-1)\theta \right\} \\ &= (-1)^n \cos 2n\theta. \end{aligned}$$

Corollaire 3.5.1 *Pour tout $\nu \geq 0$, l'identité formelle suivante est satisfaite*

$$T_{p^\nu}(\sin\theta) = (-1)^{\frac{p^\nu-1}{2}} \sin p^\nu\theta = (-1)^{\frac{p-1}{2}\nu} \sin p^\nu\theta.$$

Preuve.- La première égalité traduit la proposition précédente. Pour démontrer la seconde, il suffit de vérifier que

$$(-1)^{\frac{p^\nu-1}{2}} = (-1)^{\frac{p-1}{2}\nu}. \tag{1}$$

De deux choses l'une: ou bien $p \equiv 1 \ mod\ 4$, auquel cas

$$\frac{p^\nu - 1}{2} \equiv \frac{p-1}{2}\nu \equiv 0 \ mod\ 2$$

et alors les deux membres de (1) sont égaux à 1,
ou bien $p \equiv 3 \ mod\ 4$, auquel cas

$$p^\nu \equiv \begin{cases} 1 \ mod\ 4 \text{ si } \nu \text{ est pair} \\ 3 \ mod\ 4 \text{ si } \nu \text{ est impair} \end{cases}$$

et alors (1) s'écrit

$$(-1)^{\frac{p^\nu-1}{2}} = (-1)^\nu = (-1)^{\frac{p-1}{2}\nu}.$$

■

Proposition 3.5.2 *(sinus et arcsinus p-adiques) Les séries*

$$\begin{aligned} \sin x &= \sum_{n\geq 0}(-1)^n \frac{x^{2n+1}}{(2n+1)!} \quad \textit{et} \\ \arcsin x &= \sum_{n\geq 0}\binom{-\frac{1}{2}}{n}(-1)^n \frac{x^{2n+1}}{2n+1} \end{aligned}$$

définissent des fonctions

$$\begin{aligned} \sin &: B_{<r_e}(0) \longrightarrow B_{<r_e}(0) \ \textit{et} \\ \arcsin &: B_{<1}(0) \longrightarrow \mathbf{C}_p \end{aligned}$$

analytiques et surjectives. De plus

(i) $\sin(\arcsin x) = x = \arcsin(\sin x)$ *pour tout* $x \in B_{<r_e}(0)$;

(ii) $|\sin x| = |x|$.

Preuve.- Outre une démonstration de cette proposition, on trouvera dans [36], bien d'autres résultats concernant les fonctions trigonométriques p-adiques.

Théorème 3.5.2 *Si $x \in B_{<1}(0) \subset \mathbf{C}_p$, alors*

$$T(x) := \lim_{\nu \to \infty} (-1)^{\frac{p-1}{2}\nu} \frac{T_{p^\nu}(x)}{p^\nu} = \arcsin x.$$

Preuve.- Il suffit de vérifier que, pour tout $x \in B_{<r_c}(0)$

$$T(\sin x) = x = \sin(T(x)).$$

Mais si $x \in B_{<r_c}(0)$, alors $\sin x$ est bien défini (proposition 3.5.2) et, grâce au *corollaire* 3.5.1

$$\begin{aligned} T(\sin x) &= \lim_{\nu \to \infty} (-1)^{\frac{p-1}{2}\nu} \frac{T_{p^\nu}(x)}{p^\nu} \\ &= \lim_{\nu \to \infty} \frac{\sin p^\nu x}{p^\nu} \\ &= x \lim_{\alpha \to 0} \frac{\sin \alpha}{\alpha} \\ &= x. \end{aligned}$$

Si $|x| < r_c$, la fonction *sinus* étant surjective (proposition 3.5.2), il existe $y \in B_{<r_c}(0)$ tel que $x = \sin y$. En vertu de ce qui vient d'être établi, on a

$$\sin(T(x)) = \sin(T(\sin y)) = \sin y = x.$$

■

Cette description de la fonction arcsin nous donne la possibilité d'en déterminer facilement les zéros.

Proposition 3.5.3 *On a*

$$Z\acute{e}ros(\arcsin x) = \bigcup_{\nu \geq 0} Z\acute{e}ros\,(T_{p^\nu}(x)) = \left\{ \frac{\zeta - \zeta^{-1}}{2i} \,:\, \zeta \in \mu_{p^\infty} \right\}.$$

Preuve.- Intéressons-nous tout d'abord à la première égalité. Il est clair que si $T_{p^k}(a) = 0$ pour un certain entier k, alors $T_{p^\nu}(a) = 0$ pour tout $\nu \geq k$ et donc

$$T(a) = \arcsin a = 0.$$

Réciproquement, soit $a \in B_{<1}(0)$ tel que

$$T(a) = \arcsin a = 0.$$

Comme

$$|T_p(a)| \leq \max\left(|p| \cdot |a|,\ |a|^p\right),$$

il existe un entier k pour lequel

$$\left|T_{p^k}(a)\right| < r_e.$$

Mais alors, comme $|T(x)| = |x|$ pour tout $|x| < r_e$, on aura

$$\begin{aligned} 0 = |T(a)| &= \lim_{\nu\to\infty}\left|\frac{T_{p^{\nu-k}}\left(T_{p^k}(a)\right)}{p^{\nu-k}\cdot p^k}\right| \\ &= \frac{1}{|p^k|}\lim_{\alpha\to\infty}\left|\frac{T_{p^\alpha}\left(T_{p^k}(a)\right)}{p^\alpha}\right| \\ &= \frac{1}{|p^k|}\left|T\left(T_{p^k}(a)\right)\right| \\ &= \frac{1}{|p^k|}\left|T_{p^k}(a)\right|. \end{aligned}$$

Ainsi $T_{p^k}(a) = 0$ et la première égalité est établie. La seconde découle du lemme suivant. ∎

Lemme 3.5.1 *Soit l'application*

$$J : \mathbf{C}_p - \{0\} \longrightarrow \mathbf{C}_p,\ x \longmapsto \frac{x - x^{-1}}{2i}.$$

Quel que soit $\nu \geq 0$

$$J(\mu_{p^\nu}) = Z\acute{e}ros(T_{p^\nu}).$$

Preuve.- Le fait que (corollaire 3.5.1)

$$T_{p^\nu}(\sin\theta) = (-1)^{\frac{p-1}{2}\nu}\sin p^\nu\theta,$$

se traduit par l'identité formelle

$$T_{p^\nu}\left(\frac{x - x^{-1}}{2i}\right) = (-1)^{\frac{p-1}{2}\nu}\,\frac{x^{p^\nu} - x^{-p^\nu}}{2i}.$$

Si $\zeta \in \mu_{p^\nu}$, c'est-à-dire si $\zeta^{p^\nu} = 1$, alors

$$T_{p^\nu}\left(\frac{\zeta - \zeta^{-1}}{2i}\right) = 0,$$

ce qui signifie que

$$J(\mu_{p^\nu}) \subset Z\acute{e}ros(T_{p^\nu}). \tag{1}$$

Pour montrer que (1) est une égalité, il suffit d'établir l'injectivité de l'application $J : \mu_{p^\nu} \longrightarrow \mathbf{C}_p$. Remarquons tout d'abord que si $\zeta \in \mu_{p^\infty}$, alors

$$|J(\zeta)| = \left|\frac{\zeta - \zeta^{-1}}{2i}\right| = |\zeta|\cdot\left|\zeta - \zeta^{-1}\right| = \left|1 - \zeta^2\right| = |p|^{\frac{1}{p^{k-1}(p-1)}},$$

où k est l'entier défini par le fait que

$$\zeta^{p^k} = 1 \text{ et } \zeta^{p^{k-1}} \neq 1.$$

(cf. chapitre 1 section 7). Soient, maintenant, deux éléments ζ et ξ de μ_{p^ν} tels que

$$J(\zeta) = \frac{\zeta - \zeta^{-1}}{2i} = \frac{\xi - \xi^{-1}}{2i} = J(\xi). \tag{2}$$

En particulier, il y a égalité des valeurs absolues, ce qui signifie que $\zeta = \xi = 1$ ou alors, qu'il existe $1 \leq k \leq \nu$, tel que

$$\xi^{p^k} = \zeta^{p^k} = 1$$

avec $\xi^{p^{k-1}}$ et $\zeta^{p^{k-1}}$ tous deux différents de 1. La relation (2) entraîne

$$\zeta - \xi = (-1) \cdot \frac{\zeta - \xi}{\zeta\xi}. \tag{3}$$

En élevant (3) à la puissance p^k, on obtient

$$(\zeta - \xi)^{p^k} = -(\zeta - \xi)^{p^k},$$

ce qui montre que

$$(\zeta - \xi)^{p^k} = 0 \text{ et } \zeta - \xi = 0.$$

■

Remarque.- Nous trouvons dans l'énoncé de ce lemme, la confirmation des résultats de la section 4, concernant les polygones de Newton, ainsi qu'une autre méthode de détermination des zéros des polynômes de Tchebychev.

On perd la plus grande partie de sa jeunesse à coups de maladresses.

L.-F. Céline

Chapitre 4

POLYNOMES DE COSTER ET DE LEGENDRE

4.1 Polynômes de Coster

Définition 4.1.1 *Soit $d \geq 2$; nous appelerons* polynômes de Coster, *les polynômes à d variables $\pi_n(a_1, \ldots, a_d)$ définis par le développement en série*

$$\frac{1}{\sqrt[d]{1 + a_1 x + \cdots + a_d x^d}} = \sum_{n \geq 0} \pi_n(a_1, \ldots, a_d) x^n.$$

Exemple.- Les premiers polynômes, correspondant au cas $d = 2$, sont

$$\begin{aligned}
\pi_0(a_1, a_2) &= 1; \\
\pi_1(a_1, a_2) &= -\tfrac{1}{2} a_1; \\
\pi_2(a_1, a_2) &= \tfrac{3}{8} a_1^2 - \tfrac{1}{2} a_2; \\
\pi_3(a_1, a_2) &= -\tfrac{5}{16} a_1^3 + \tfrac{3}{4} a_1 a_2; \\
\pi_4(a_1, a_2) &= \tfrac{35}{128} a_1^4 - \tfrac{15}{16} a_1^2 a_2 + \tfrac{3}{8} a_2^2; \\
\pi_5(a_1, a_2) &= -\tfrac{63}{256} a_1^5 + \tfrac{35}{32} a_1^3 a_2 - \tfrac{15}{16} a_1 a_2^2 \\
&\cdots
\end{aligned}$$

La définition 4.1.1 trouve son origine dans l'article [15], que M. Coster consacre à l'étude de la série formelle définie par le développement de Taylor

$$\left(1 + \sum_{i=1}^{e} \alpha_i x^i\right)^{-\frac{1}{e}} = \sum_{n=0}^{\infty} u_n x^n,$$

où $\alpha_1, \ldots, \alpha_\ell$ sont dans $\mathbf{Z}$. En effectuant l'adaptation qui consiste à considérer les α_i. non pas comme des nombres mais comme des indéterminées, nous héritons du résultat suivant.

Théorème 4.1.1 *Pour* $p \equiv 1$ *mod* d, *les polynômes de Coster vérifient les congruences*

$$\pi_{np}(a_1, \ldots, a_d) \equiv \pi_n(a_1^p, \ldots, a_d^p) \ mod\ np\, \mathbf{Z}_p[a_1, \ldots, a_d],\ (n \geq 0).$$

Preuve.- Il suffit de modifier, dans la démonstration de ([15], Théorème A, p. 51.)[1], la congruence (10) comme suit

$$\left(b_1' p^j \ldots b_d' p^j\right)^{-\frac{1}{d}} \prod_i a_i^{b_i' p^j} \equiv \left(b_1' p^{j-1} \ldots b_d' p^{j-1}\right)^{-\frac{1}{d}} \prod_i a_i^{b_i' p^{j-1}} \ mod\ p^r\, \mathbf{Z}_p;$$

avec les nouvelles notations $d = e$, $a_i = \alpha_i$, $\pi_n = u_n$. ∎

Pour ce qui concerne le cas $d = 2$ (duquel relève la section 4.2), nous apportons, au théorème 4.1.1, une preuve indépendante.

Lemme 4.1.1 *Les séries formelles*

$$f_0(x) := \sum_{n \geq 1} \pi_{n-1}(a_1, a_2) \frac{x^n}{n} \quad et$$
$$f_1(x) := \sum_{n \geq 1} \pi_n(a_1, a_2) \frac{x^n}{n},$$

définies à l'aide des polynômes intervenant dans le développement

$$\frac{1}{R(x)} := \frac{1}{\sqrt{1 + a_1 x + a_2 x^2}} = \sum_{n \geq 0} \pi_n(a_1, a_2) x^n,$$

satisfont aux identités formelles

$$f_0(x) = \frac{1}{\sqrt{a_2}} \log\left(\frac{a_1 + 2a_2 x + 2\sqrt{a_2}\, R(x)}{a_1 + 2\sqrt{a_2}}\right),$$
$$f_1(x) = -\log\left(\frac{2 + a_1 x + 2R(x)}{4}\right).$$

[1] Ce théorème établit les congruences

$$u_{mp^r} \equiv u_{mp^{r-1}},\ mod\ p^r,\ (m, r \geq 1).$$

Preuve.- Ces identités s'établissent directement par dérivation. Ainsi

$$f_0'(x) - \frac{1}{R} = \frac{1}{\sqrt{a_2}} \frac{2a_2 + \sqrt{a_2}(a_1 + 2a_2x)R^{-1}}{a_1 + 2a_2x + 2\sqrt{a_2}R} - \frac{\sqrt{a_2}}{\sqrt{a_2}R} = 0.$$

et on vérifie que

$$\log\left(\frac{a_1 + 2a_2x + 2\sqrt{a_2}\,R(x)}{a_1 + 2\sqrt{a_2}}\right)\Big|_{x=0} = 0 = f_0(0).$$

De même

$$\begin{aligned} f_1'(x) - \frac{R^{-1} - \pi_0}{x} &= f_1'(x) - \frac{1 - R}{Rx} \\ &= -\left(\frac{a_1 + a_1R^{-1} + 2a_2xR^{-1}}{2 + a_1x + 2R} + \frac{1 - R}{Rx}\right) \\ &= -\frac{2 + 2a_1x + 2a_2x^2 - 2R^2}{Rx(2 + a_1x + 2R)} \\ &= 0; \end{aligned}$$

de plus

$$\log\left(\frac{2 + a_1x + 2R}{4}\right)\Big|_{x=0} = 0 = f_1(0).$$

■

Théorème 4.1.2 *Si p est premier impair, alors les polynômes de Coster satisfont à la relation de congruence*

$$\pi_{np}(a_1, a_2) \equiv \pi_n(a_1^p, a_2^p) \ mod\ np\,\mathbf{Z}_p[a_1, a_2].\ (n \geq 0).$$

De plus, la série formelle

$$f_1(x) = \pi_1 x + \pi_2 \frac{x^2}{2} + \cdots$$

donne naissance au groupe formel

$$F_1(x, y) = f_1^{-1}\left(f_1(x) + f_2(y)\right) \in \mathbf{Z}_p[a_1, a_1^{-1}, a_2],$$

isomorphe au groupe formel multiplicatif, via l'isomorphisme

$$h(x) = \frac{4}{2 + a_1x + 2R} - 1.$$

Preuve.- Si l'on considère

$$A = \mathbf{Z}_p[a_1, a_2],\ I = pA.\ \sigma : a_i \mapsto a_i^p, \tag{1}$$

alors la série formelle $f_1(x)$, qui s'écrit

$$f_1(x) = -\log(1 + r(x)),\ \text{avec } r(x) \in A[[x]],$$

est de type $p - T$, relativement aux "ingrédients", que (1) désigne. Ceci établit les congruences

$$\pi_{np}(a_1, a_2) \equiv \pi_n(a_1^p, a_2^p)\ mod\ npA,\ (n \geq 1).$$

De plus, dans $\mathbf{Z}_p[a_1, a_1^{-1}, a_2]$, le coefficient $f_1'(0) = \pi_1(a_1, a_2) = -\frac{a_1}{2}$ est inversible. Ainsi

$$f_1^{-1}(f_1(x) + f_2(y))$$

est une loi de groupe formel sur $\mathbf{Z}_p[a_1, \ldots, a_d]$. ∎

Lemme 4.1.2 *Si $p \equiv 1$ mod d, alors pour tout $n \geq 1$ et $i \in \{1, \ldots, d\}$*

$$\frac{\partial}{\partial a_i}\pi_n(a_1, \ldots, a_d) \in n\mathbf{Z}_p[a_1, \ldots, a_d].$$

Preuve.- Comme $p \equiv 1\ mod\ d$, les polynômes $\pi_n(a_1, \ldots, a_d)$ ont leurs coefficients dans $\mathbf{Z}_p$. Ainsi, si $\nu = ord_p(n) = 0$, alors

$$\frac{\partial}{\partial a_i}\pi_n(a_1, \ldots, a_d) \in \mathbf{Z}_p[a_1, \ldots, a_d] = n\,\mathbf{Z}_p[a_1, \ldots, a_d].$$

Supposons maintenant que $\nu = ord_p(n) > 0$. En dérivant la congruence

$$\pi_{np}(a_1, \ldots, a_d) \equiv \pi_n(a_1^p, \ldots, a_d^p)\ mod\ np\,\mathbf{Z}_p[a_1, \ldots, a_d].$$

du lemme 4.1.1, par rapport à a_i, on obtient

$$\frac{\partial}{\partial a_i}\pi_{np}(a_1, \ldots, a_d) \equiv pa_i^{p-1}\frac{\partial}{\partial a_i}\pi_n(a_1^p, \ldots, a_d^p)\ mod\ np\,\mathbf{Z}_p[a_1, \ldots, a_d].$$

Par hypothèse d'induction, le second membre de cette dernière expression est nul modulo $np\,\mathbf{Z}_p[a_1, \ldots, a_d]$, ce qui prouve bien que

$$\frac{\partial}{\partial a_i}\pi_{np}(a_1, \ldots, a_d) \in np\,\mathbf{Z}_p[a_1, \ldots, a_d].$$

∎

Corollaire 4.1.1 *Si $p \equiv 1$ mod d, alors la congruence*

$$\pi_{np}(a_1(t),\dots,a_d(t)) \equiv \pi_n(a_1(t^p),\dots,a_d(t^p)) \ mod\ np\mathbf{Z}_p[t]$$

est vérifiée pour tout $n \geq 0$ et quels que soient les polynômes

$$a_1(t),\dots,a_d(t) \in \mathbf{Z}_p[t].$$

Preuve.- le théorème 4.1.1 stipule que

$$\pi_{np}(a_1(t),\dots,a_d(t)) \equiv \pi_n(a_1(t)^p,\dots,a_d(t)^p) \ mod\ np\,\mathbf{Z}_p[t]. \tag{2}$$

Choisissons d polynômes $\alpha_1(t),\dots,\alpha_d(t) \in \mathbf{Z}_p[t]$, tels que

$$a_i(t)^p = a_i(t^p) + p\alpha_i(t).$$

Grâce au lemme 4.1.2 et aux applications successives du *théorème des accroissements finis* (pour chaque variable), la congruence (2) peut s'écrire

$$\begin{aligned}\pi_{np}(a_1(t),\dots,a_d(t)) &\equiv \pi_n(a_1(t^p)+p\alpha_1(t),\dots,a_d(t^p)+p\alpha_d(t)) \ mod\ np\,\mathbf{Z}_p[t]\\ &\equiv \pi_n(a_1(t^p),\dots,a_d(t^p)) \ mod\ np\,\mathbf{Z}_p[t].\end{aligned}$$

■

Théorème 4.1.3 *Pour $p \equiv 1$ mod d, les polynômes de Coster vérifient les congruences dites de Schur*[2]*; c'est-à-dire que si*

$$n = n_0 + n_1 p + \cdots + n_k p^k$$

est le développement de l'entier n dans la base p, alors

$$\begin{aligned}\pi_n(a_1,\dots,a_d) &\equiv \pi_{n_0}(a_1,\dots,a_d)\cdot\pi_{n_1}(a_1,\dots,a_d)^p\cdots\pi_{n_k}(a_1,\dots,a_d)^{p^k}\\ &\equiv \pi_{n_0}(a_1,\dots,a_d)\cdot\pi_{n_1}(a_1^p,\dots,a_d^p)\cdots\pi_{n_k}\left(a_1^{p^k},\dots,a_d^{p^k}\right)\\ &\quad mod\ p\,\mathbf{Z}_p[a_1,\dots,a_d].\end{aligned}$$

Preuve[3].- Posons $A = \mathbf{Z}_p[a_1,\dots,a_d]$ et $p(x) = 1 + a_1x + \cdots + a_dx^d$. Puisque d divise $p-1$, le nombre $-\frac{1}{d}$ se laisse développer, comme suit, dans la base p

$$-\frac{1}{d} = \frac{1}{d}(-1) = \frac{p-1}{d} + \frac{p-1}{d}p + \cdots + \frac{p-1}{d}p^\nu + \cdots$$

On a alors

$$\begin{aligned}\frac{(1+a_1x+\cdots+a_dx^d)^{-\frac{1}{d}}}{\left(1+a_1x+\cdots+a_dx^d\right)^{\frac{p-1}{d}+\cdots+\frac{p-1}{d}p^\nu}} &= \left\{\left(1+a_1x+\cdots+a_dx^d\right)^{-\frac{1}{d}}\right\}^{p^{\nu+1}}\\ &\equiv 1 \ mod\ \left(pA[x], x^{p^{\nu+1}}\right),\end{aligned}$$

[2]On dit aussi que la suite $\pi_n(a_1,\dots,a_d)$ satisfait à la propriété de Lucas, cf. [29].
[3]Voir aussi [26], p.75.

autrement dit

$$p(x)^{-\frac{1}{d}} \equiv \left\{p(x)^{\frac{p-1}{d}}\right\}^{1+p+\cdots+p^{\nu}} \mod \left(pA, x^{p^{\nu+1}}\right).$$

Puis, comme d divise $p-1$, alors $p(x)^{-\frac{1}{d}}$ est un polynôme de degré $p-1$ en x, et

$$p(x)^{-\frac{1}{d}} \equiv \pi_0(a_1,\ldots,a_d) + \cdots + \pi_{p-1}(a_1,\ldots,a_d)x^{p-1} \mod p\,A[x].$$

En effet

$$\begin{aligned} p(x)^{\frac{p-1}{d}} &= p(x)^{\frac{1}{d}}\left(p(x)^{-\frac{1}{d}}\right)^{p} \\ &\equiv \left(1+\pi_1(a_1,\ldots,a_d)x+\cdots+\pi_{p-1}(a_1,\ldots,a_d)x^{p-1}+*x^{p}\right)(1+*x^{p}) \mod p\,A[[x]] \\ &\equiv 1+\pi_1(a_1,\ldots,a_d)x+\cdots+\pi_{p-1}(a_1,\ldots,a_d)x^{p-1} \mod (p\,A[x],x^{p}) \end{aligned}$$

et le membre de gauche de cette dernière congruence est un polynôme de degré $p-1$ en x. On parvient ainsi à la congruence

$$\sum_{n\geq 0}\pi_n(a_1,\ldots,a_d)x^n \equiv \left(\sum_{n<p}\pi_n(a_1,\ldots,a_d)x^n\right)^{1+p+\cdots+p^{\nu}} \mod \left(p\,A[x],x^{p^{\nu+1}}\right).$$

L'identification des coefficients de x^n, pour

$$n = n_0 + n_1 p + \cdots + n_k p^k < p^{\nu+1},$$

donne lieu à la congruence de Schur

$$\pi_n(a_1,\ldots,a_d) \equiv \pi_{n_0}(a_1,\ldots,a_d)\cdot\pi_{n_1}(a_1,\ldots,a_d)^{p}\cdots\pi_{n_k}(a_1,\ldots,a_d)^{p^k} \mod p\,A.$$

■

4.2 Polynômes de Legendre

Définition 4.2.1 *Les polynômes $P_n(t)$, définis par le développement en série*

$$\frac{1}{\sqrt{1-2tx+x^2}} = \sum_{n\geq 0} P_n(t)x^n,$$

sont appelés polynômes de Legendre.

Ainsi, avec les notations de la section précédente, pour tout $n \geq 0$, on a l'égalité

$$P_n(t) = \pi_n(-2t,1).$$

Réciproquement, en partant des polynômes de Legendre, on fabrique les polynômes de Coster, comme suit.

Proposition 4.2.1 *Pour tout $n \geq 0$, on a la relation*

$$\pi_n(a_1, a_2) = (-1)^n \sqrt{a_2}^n P_n\left(\frac{a_1}{2\sqrt{a_2}}\right).$$

Preuve.- Les fonctions

$$Q(a_1, a_2, x) = \frac{1}{\sqrt{1 + a_1 x + a_2 x^2}} = \sum_{n \geq 0} \pi_n(a_1, a_2) x^n,$$

$$q(t, x) = \frac{1}{\sqrt{1 - 2tx + x^2}} = \sum_{n \geq 0} P_n(t) x^n,$$

sont liées entre elles, par la formule

$$q\left(-\frac{a_1}{2\sqrt{a_2}}, \frac{x}{\sqrt{a_2}}\right) = \left(1 + a_1 \frac{x}{a_2} + \frac{x^2}{a_2}\right)^{-\frac{1}{2}} = Q\left(a_1, a_2, \frac{x}{a_2}\right).$$

dont le développement en séries s'écrit

$$\sum_{n \geq 0} P_n\left(-\frac{a_1}{2\sqrt{a_2}}\right) a_2^{-\frac{n}{2}} x^n = \sum_{n \geq 0} \pi_n(a_1, a_2) a_2^{-n} x^n.$$

Par identification, on trouve

$$\pi_n(a_1, a_2) = P_n\left(-\frac{a_1}{2\sqrt{a_2}}\right) a_2^{\frac{n}{2}} = (-\sqrt{a_2})^n P_n\left(\frac{a_1}{2\sqrt{a_2}}\right).$$

■

Voici la liste des premiers polynômes de Legendre

$$\begin{aligned}
P_0(t) &= 1; \\
P_1(t) &= t; \\
P_2(t) &= \tfrac{3}{2}t^2 - \tfrac{1}{2}; \\
P_3(t) &= \tfrac{5}{2}t^3 - \tfrac{3}{2}t; \\
P_4(t) &= \tfrac{35}{8}t^4 - \tfrac{15}{4}t^2 + \tfrac{3}{8}; \\
P_5(t) &= \tfrac{63}{8}t^5 - \tfrac{35}{4}t^3 + \tfrac{15}{8}t; \\
&\cdots
\end{aligned}$$

Corollaire 4.2.1 *([34], [38], [29]) Les polynômes de Legendre vérifient les congruences de Schur dans $\mathbf{Z}_p[t]$, pour $p \neq 2$. Autrement dit, si un entier*

$$n = n_0 + n_1 p + \cdots + n_k p^k,$$

est développé dans la base p, alors

$$\begin{aligned} P_n(t) &\equiv P_{n_0}(t) \cdot P_{n_1}(t)^p \cdots P_{n_k}(t)^{p^k} \\ &\equiv P_{n_0}(t) \cdot P_{n_1}(t^p) \cdots P_{n_k}(t^{p^k}) \ mod\, p\, \mathbf{Z}_p[t]. \end{aligned}$$

Preuve.- D'après le théorème 4.1.3, les polynômes de Coster $\pi_n(a_1, a_2)$ vérifient les congruences de Schur dans $\mathbf{Z}_p[a_1, a_2]$, $(p \neq 2)$. Ainsi

$$\pi_n(a_1, a_2) \equiv \pi_{n_0}(a_1, a_2) \cdot \pi_{n_1}(a_1, a_2)^p \cdots \pi_{n_k}(a_1, a_2)^{p^k} \ mod\, p\, \mathbf{Z}_p[a_1, a_2],$$

et l'évaluation de cette dernière relation en

$$a_1 = -2t \ \text{ et } \ a_2 = 1,$$

établit le corollaire. ∎

La suite du présent chapitre est consacrée aux deux résultats qui ont été le point de départ de cette thèse: les congruences établies par T. Honda dans [21],(ici théorèmes 4.2.1 et 4.2.3). Nous en apportons différentes améliorations et démonstrations.

Théorème 4.2.1 *Si p est impair et $n \geq 0$, alors on a la congruence*

$$P_{np}(t) \equiv P_n(t^p) \ mod\, np\, \mathbf{Z}_p[t].$$

Preuve.- En vertu du corollaire 4.1.1, la congruence

$$\pi_{np}(a_1(t), a_2(t)) \equiv \pi_n(a_1(t^p), a_2(t^p)) \ mod\, np\, \mathbf{Z}_p[t],$$

est vérifiée, quels que soient les polynômes $a_1(t), a_2(t) \in \mathbf{Z}_p[t]$, ($p$ impair). En particulier pour

$$a_1(t) = -2t \ \text{ et } \ a_2(t) = 1,$$

on peut écrire

$$P_{np}(t) = \pi_{np}(-2t, 1) \equiv \pi_n(-2t^p, 1) = P_n(t^p) \ mod\, np\, \mathbf{Z}_p[t].$$

∎

Corollaire 4.2.2 *Le polynôme $P_n(t)$ est une pseudo-puissance n dans $\mathbf{Z}_p[t]$, $(p \neq 2)$.*

Preuve.- C'est une conséquence directe de la proposition 1.4.1. ∎

Remarque.- Dans le contexte du corollaire 4.2.2, il convient de citer la relation bien connue [28] et plus précise suivante

$$P_n'(t) = n \cdot \frac{P_{n-1}(t) - tP_n(t)}{1-t^2}.$$

Le théorème 4.2.1 ne vaut que pour p impair. A l'aide du changement[4] d'indéterminée $t \mapsto 1+2t$, il est possible d'énoncer et de démontrer "à la main", un résultat englobant, également, le cas exceptionnel $p = 2$.

Lemme 4.2.1 *Les polynômes $P_n(1+2t)$ sont à coefficients dans $\mathbf{Z}$ et admettent le développement explicite*

$$P_n(1+2t) = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} t^k, \ (n \geq 0).$$

Preuve.- On trouvera une preuve de ce lemme, bien connu [28], dans [34], par exemple. ∎

Théorème 4.2.2 *Pour tout p premier et pour tout $n \geq 0$, les polynômes de Legendre satisfont à la relation de congruence*

$$P_{np}(1+2t) \equiv P_n(1+2t^p) \ mod\ np\,\mathbf{Z}_p[t].$$

Preuve.- Grâce aux congruences

$$\binom{np}{kp} \equiv \binom{n}{k} \ mod\ np\,\mathbf{Z}_p,$$

(remarque 1, section 2.2) et au lemme précédent, on obtient

$$\begin{aligned} P_{np}(1+2t) - P_n(1+2t^p) &= \sum_{k=0}^{np} \binom{np}{k}\binom{np+k}{k} t^k - \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} t^{pk} \\ &= \sum_{k=1}^{n} \left\{ \binom{np}{kp}\binom{np+kp}{kp} - \binom{n}{k}\binom{n+k}{k} \right\} t^{pk} + \\ &\quad + \sum_{\substack{k=1 \\ p \text{ ne divise pas } k}}^{np} \frac{np}{k}\binom{np-1}{k-1}\binom{np+k}{k} t^k \\ &\equiv 0 \ mod\ np\,\mathbf{Z}_p[t]. \end{aligned}$$

[4] L'astuce de ce changement de variables et la compréhension de son enjeu sont dues à A. Robert, cf. [34].

En effet, il existe deux entiers p-adiques $\alpha_{n,k}$ et $\beta_{n,k}$ tels que

$$\binom{np}{kp} = \binom{n}{k} + np\alpha_{n,k},$$

$$\binom{np+kp}{kp} = \binom{n+k}{k} + (n+k)p\beta_{n,k}$$

de sorte que si $1 \leq k \leq n$, alors

$$\begin{aligned}\binom{np}{kp}\binom{np+kp}{kp} - \binom{n}{k}\binom{n+k}{k} &= \binom{n}{k}(n+k)p\beta_{n,k} + \binom{n+k}{k}np\alpha_{n,k} + \\ &\quad np\alpha_{n,k}(n+k)p\beta_{n,k} \\ &\equiv \binom{n}{k}np\beta_{n,k} + \frac{n}{k}\binom{n-1}{k-1}kp\beta_{n,k} \\ &\equiv 0 \ mod\ np\,\mathbf{Z}_p.\end{aligned}$$

Remarque.- Si, pour p impair, on effectue, dans la relation

$$P_{np}(1+2t) \equiv P_n(1+2t^p) \ mod\ np\,\mathbf{Z}_p[t],$$

la substitution

$$t = \frac{x-1}{2} \in \mathbf{Z}_p[x],$$

on obtient la congruence

$$P_{np}(x) \equiv P_n(x^p) \ mod\ np\,\mathbf{Z}_p[x].$$

En effet, il existe $r(x) \in \mathbf{Z}_p[x]$, tel que

$$1 + 2t^p = 1 + 2 \cdot 2^{-p}(x-1)^p = x^p + pr(x).$$

Comme le polynôme $P_n(x)$ est une pseudo-puissance n dans $\mathbf{Z}_p[x]$ pour $p \neq 2$ (c'est-à-dire que $P_n'(x) \in n\mathbf{Z}_p[x]$), le *théorème des accroissements finis* fournit la congruence

$$P_n\left(1 + 2 \cdot 2^{-p}(x-1)^p\right) = P_n\left(x^p + pr(x)\right) \equiv P_n(x^p) \ mod\ np\,\mathbf{Z}_p[x].$$

Ceci, pour montrer comment le théorème 4.2.1 découle du théorème 4.2.2. ∎

Corollaire 4.2.3 *La série formelle*

$$f_1(x) = \sum_{n \geq 1} P_n(1+2t)\frac{x^n}{n}$$

donne naissance à la loi de groupe formel

$$F_1(x,y) = f_1^{-1}(f_1(x) + f_1(y)),$$

définie sur l'anneau $\mathbf{Z}[t, \frac{1}{1+2t}]$*et isomorphe au groupe formel multiplicatif, via l'isomorphisme*

$$h(x) = \frac{2}{1 - x - 2tx + \sqrt{x^2 - 2(1+2t)x + 1}} - 1.$$

Preuve.- La série formelle

$$f_1(x) \in \mathbf{Q}[t][[x]]$$

est de type p$-T$, sur $A_p = \mathbf{Z}_p[t, \frac{1}{1+2t}]$. Ainsi, quel que soit p, $F_1(x,y)$ a ses coefficients dans A_p. Le reste de l'énoncé se déduit du théorème 4.1.2. ∎

Théorème 4.2.3 *Si p est impair, alors pour tout $n \geq 1$, on a la congruence*

$$P_{np-1}(t) \equiv P_{n-1}(t^p) \ mod \ np\,\mathbf{Z}_p[t].$$

Preuve.- Si l'on considère la série formelle

$$f_0(x) = \sum_{n \geq 1} P_{n-1}(t)\frac{x^n}{n},$$

alors le lemme 4.1.1 fournit la formule explicite

$$f_0(x) = \log\left(\frac{x - t + \sqrt{1 - 2tx + x^2}}{1 - t}\right).$$

Il s'ensuit que

$$\exp(f_0(x)) = \frac{x - t + \sqrt{1 - 2tx + x^2}}{1 - t}$$

a ses coefficients dans l'anneau $A = \mathbf{Z}_p[t]$. Autrement dit, la série formelle $f_0(x)$ est de type $p - T$ sur A, ce qui prouve que ses coefficients $P_{n-1}(t)$ vérifient les congruences de Honda. ∎

La preuve de Honda [21][5].- Comme dans la preuve précédente, considérons la série formelle

$$f_0(x) = \sum_{n \geq 1} P_{n-1}(t)\frac{x^n}{n},$$

pour laquelle

$$\frac{d}{dx} f_0(x) = \frac{1}{\sqrt{1 - 2tx + x^2}}.$$

[5]Il s'agit plutôt, ici, d'une traduction de la preuve de Honda, dans le langage du LEF de Hazewinkel.

Le changement de variables

$$x = \varphi(s) = \frac{2s(1-st)}{1-s^2} = 2s + \cdots \in \mathbf{Z}[t][[s]],$$

$$s = \varphi^{-1}(x) = \frac{x}{2} + \cdots \in \mathbf{Z}_p[t][[x]], (p \neq 2),$$

donne lieu à l'identité

$$f_0(\varphi(s)) = \log \frac{1-s}{1+s} = \log(1-s) - \log(1+s).$$

Ainsi, la série formelle

$$f_0(x) = \log\left(1 - \varphi^{-1}(x)\right) - \log\left(1 + \varphi^{-1}(x)\right)$$

est de type $p-T$, sur l'anneau $\mathbf{Z}_p[t]$[6]. En effet, $\log(1+x)$ est de type $p-T$ et $\varphi^{-1}(x)$ est à coefficients dans $\mathbf{Z}_p[t]$. Le point (iii) du LEF montre, alors, que

$$\log\left(1 \pm \varphi^{-1}(x)\right)$$

sont, toutes deux, de type $p-T$ sur $\mathbf{Z}_p[t]$. ∎

Corollaire 4.2.4 *Le polynôme de Legendre $P_{n-1}(t)$ est une pseudo-puissance n dans $\mathbf{Z}_p[t]$, si $p \neq 2$.*

Preuve.- Par induction sur $\nu = ord_p(n)$ et en utilisant la congruence du théorème 4.2.3. ∎

Remarque.- Comme précédemment, on dispose de la relation [28], plus précise

$$P'_{n-1}(t) = n \cdot \frac{tP_{n-1}(t) - P_n(t)}{1-t^2}.$$

Ici aussi, le changement de variables, $t \mapsto 1+2t$, permet un énoncé valable pour tout p premier, ($p=2$ compris).

Théorème 4.2.4 *Pour tout p premier et tout $n \geq 1$, les polynômes de Legendre satisfont à la relation de congruence*

$$P_{np-1}(1+2t) \equiv P_{n-1}(1+2t^p) \ mod\ np\,\mathbf{Z}_p[t].$$

[6]Bien que, contrairement à ce que prétend Honda, $\mathbf{Z}_p[t]$ ne soit pas un anneau de valuation discrète.

Preuve.- Si l'on considère la série formelle

$$f_0(x) = \sum_{n\geq 1} P_{n-1}(1+2t)\frac{x^n}{n}.$$

alors le lemme 4.1.1 donne la formule explicite

$$f_0(x) = \log\left(\frac{1-x+2t-\sqrt{1-2(1+2t)x+x^2}}{2t}\right).$$

Il s'agit de montrer que

$$Y(x) := \exp(f_0(x)) - 1 = \frac{1-x-\sqrt{(1-x)^2-4tx}}{2t}$$

a ses coefficients dans $\mathbf{Z}[t]$; plus précisément, dans $\mathbf{Z}_p[t]$ pour tout p (ce qui est clair pour $p \neq 2$). Remarquons que la série Y est solution de l'équation quadratique

$$tY^2 - (1-x)Y + x = 0,$$

ou, mieux encore, de l'équation

$$(tY)^2 - (1-x)(tY) + tx = 0.$$

On en déduit (par induction sur ses coefficients) que la série formelle

$$tY(x) \in \mathbf{Z}[t][[x]];$$

ce qui implique (par la définition de Y) que

$$Y(x) \in \mathbf{Z}[t][[x]].$$

■

Preuve à la main.- Partant de la formule explicite

$$P_m(t) = \sum_{k=0}^{m}\binom{m}{k}\binom{m+k}{k}t^k,$$

on calcule la différence

$$\begin{aligned} P_{np-1}(1+2t) \;-\; & P_{n-1}(1+2t^p) \\ &= \sum_{k=0}^{np-1}\binom{np-1}{k}\binom{np+k-1}{k}t^k - \sum_{k=0}^{n-1}\binom{n-1}{k}\binom{n+k-1}{k}t^{pk} \\ &= \sum_{k=1}^{n-1}\left\{\binom{np-1}{kp}\binom{np+kp-1}{kp} - \binom{n-1}{k}\binom{n+k-1}{k}\right\}t^{pk} + \\ &\quad + \sum_{\substack{k=1 \\ \text{p ne divise pas k}}}^{np-1}\binom{np-1}{k}\binom{np+k-1}{k}t^k. \end{aligned}$$

Comme, pour p ne divisant pas k, on a

$$\binom{np+k-1}{k} = \frac{np}{k}\binom{np+k-1}{k-1} \equiv 0 \ mod\ np\mathbf{Z}_p,$$

la dernière somme est nulle $mod\ np\mathbf{Z}_p[t]$. Maintenant pour $k, n \geq 1$ fixés, posons

$$\begin{aligned} a &= \binom{np}{kp}\binom{np+kp}{kp} - \binom{n}{k}\binom{n+k}{k}; \\ b &= \binom{np-1}{kp}\binom{np+kp-1}{kp} - \binom{n-1}{k}\binom{n+k-1}{k}; \\ c &= \binom{np-1}{kp-1}\binom{np+kp-1}{kp-1} - \binom{n-1}{k-1}\binom{n+k-1}{k-1}. \end{aligned}$$

En utilisant les identités

$$\binom{n+k-1}{k} = \frac{(n+k-1)\cdots(n+1)}{(k-1)!}\cdot\frac{n}{k} = \frac{n}{k}\binom{n+k-1}{k-1}, \tag{1}$$

$$\binom{n-1}{k} = \binom{n}{k} - \binom{n-1}{k-1} = \left(\frac{n}{k}-1\right)\binom{n-1}{k-1} = \frac{n-k}{k}\binom{n-1}{k-1}, \tag{2}$$

on obtient

$$\begin{aligned} a &= \frac{n}{k}\cdot\frac{n+k}{k}\left\{\binom{np-1}{kp-1}\binom{np+kp-1}{kp-1} - \binom{n-1}{k-1}\binom{n+k-1}{k-1}\right\} = \frac{n(n+k)}{k^2}\cdot c, \\ b &= \frac{n-k}{k}\cdot\frac{n}{k}\left\{\binom{np-1}{kp-1}\binom{np+kp-1}{kp-1} - \binom{n-1}{k-1}\binom{n+k-1}{k-1}\right\} = \frac{n(n-k)}{k^2}\cdot c. \end{aligned}$$

Il s'ensuit

$$\begin{aligned} b &= \frac{n-k}{n+k}\cdot a \\ &= \frac{n-k}{n+k}\left\{\binom{np}{kp}\binom{np+kp}{kp} - \binom{n}{k}\binom{n+k}{k}\right\} \\ &= \frac{n-k}{n+k}\left[\left\{\binom{n}{k} + unp\right\}\left\{\binom{n+k}{k} + v(n+k)p\right\} - \binom{n}{k}\binom{n+k}{k}\right] \end{aligned}$$

$$
\begin{aligned}
& \text{avec } u, v \in \mathbf{Z}_p \\
= \; & \frac{n-k}{n+k}\binom{n}{n-k}v(n+k)p + \frac{n-k}{n+k}unp\binom{n+k}{k} + \frac{n-k}{n+k}(n+k)uvnp^2 \\
\equiv \; & n\binom{n-1}{n-k-1}vp + unp\frac{n+k-2k}{n+k}\binom{n+k}{k} \; mod\; np\,\mathbf{Z}_p \\
\equiv \; & unp\binom{n+k}{k} - 2unp\frac{k}{n+k}\binom{n+k}{k} \; mod\; np\,\mathbf{Z}_p \\
\equiv \; & -2unp\binom{n+k-1}{k-1} \; mod\; np\,\mathbf{Z}_p \\
\equiv \; & 0 \; mod\; np\,\mathbf{Z}_p.
\end{aligned}
$$

■

Remarque.- A nouveau, il convient de constater que le théorème 4.2.3 se déduit du théorème 4.2.4. En effet, supposons p impair et effectuons la substitution

$$t = \frac{x-1}{2} \in \mathbf{Z}_p[x]$$

dans la congruence

$$P_{np-1}(1+2t) \equiv P_{n-1}(1+2t^p) \; mod\; np\,\mathbf{Z}_p[t].$$

Puisque $P_{n-1}(t)$ est pseudo-puissance n dans $\mathbf{Z}_p[t]$, la dernière congruence s'écrit, grâce au *théorème des accroissements finis*

$$
\begin{aligned}
P_{np-1}(x) &\equiv P_{n-1}\left(1 + 2^{1-p}(x-1)^p\right) \\
&\equiv P_{n-1}(x^p + pr(x)), \quad \text{avec } r(x) \in \mathbf{Z}_p[x] \\
&\equiv P_{n-1}(x^p) \; mod\; np\,\mathbf{Z}_p[x].
\end{aligned}
$$

■

Corollaire 4.2.5 *La série formelle*

$$f_0(x) = \sum_{n\geq 1} P_{n-1}(1+2t)\frac{x^n}{n}$$

est le logarithme d'un groupe formel défini sur $\mathbf{Z}[t]$. *Ce groupe formel est strictement isomorphe au groupe mutiplicatif, via l'isomorphisme*

$$h(x) = \frac{1 - x - \sqrt{(1-x)^2 - 4tx}}{2t}.$$

Preuve.- Comme la série formelle $f_0(x)$ est de type $p-T$ sur $\mathbf{Z}_p[t]$ pour tout p, la loi $F_0(x,y) = f_0^{-1}(f_0(x)+f_0(y))$ est à coefficients dans $\mathbf{Z}[t]$. Pour le reste de l'assertion, il suffit de vérifier que

$$\begin{aligned} h(x) &= \exp(f_0(x)) - 1 \\ &= \frac{1-x-\sqrt{(1-x)^2-4tx}}{2t} \\ &\equiv x \ mod \ \deg 2. \end{aligned}$$

■

Remarque.- L'article [21], dans lequel T. Honda démontre les congruences des théorèmes 4.2.1 et 4.2.3, se veut une application de la théorie des groupes formels commutatifs sur un anneau de valuation discrète, qu'il a développée dans [20]. Malheureusement, il se trouve que l'anneau $\mathbf{Z}_p[t]$ n'est pas de valuation discrète.
Dans [26], N. Yui corrige l'erreur de Honda, en plongeant $\mathbf{Z}_p[t]$ dans un anneau de valuation discrète. Mais elle ne parvient pas[7] à énoncer le résultat général, analogue au corollaire 4.2.5 (que nous avons établi à l'aide du LEF).

Terminons cette section par un corollaire des théorèmes 4.2.1 et 4.2.3.

Proposition 4.2.2 *Quels que soient les entiers* $m \geq 1$ *et* $k \in \mathbf{Z}$, *la suite*

$$(P_{mp^\nu+k}(a))_{\nu \geq \nu_0}, \quad (p \neq 2),$$

converge en tout point de la lemniscate L_{r_4}. *De plus, la limite*

$$f_{m,k}(a) := \lim_{\nu \to \infty} P_{mp^\nu+k}(a)$$

satisfait à la relation de récurrence

$$k f_{m,k}(a) = (2k-1)a f_{m,k-1}(a) - (k-1) f_{m,k-2}(a).$$

Preuve.- Puisque les polynômes $P_n(t)$ et $P_{n-1}(t)$ sont des pseudo-puissances n et vérifient les congruences de Honda dans $\mathbf{Z}_p[t]$, le *théorème des accroissements finis* permet d'établir la convergence des suites

$$(P_{mp^\nu}(a))_{\nu \geq 0} \quad \text{et} \quad (P_{mp^\nu-1}(a))_{\nu \geq 0}.$$

La formule de récurrence

$$nP_n(t) = (2n-1)tP_{n-1}(t) - (n-1)P_{n-2}(t),$$

[7] Elle ne fait aucune référence aux travaux de Hazewinkel.

à laquelle satisfont les polynômes de Legendre (cf. [28]), s'exprime, pour $n = mp^\nu + k$ et $t = a$, sous la forme

$$(mp^\nu+k)P_{mp^\nu+k}(a) = (2mp^\nu+2k-1)\cdot a\cdot P_{mp^\nu+k-1}(a)-(mp^\nu+k-1)P_{mp^\nu+k-2}(a). \quad (1)$$

On en déduit, par induction, la convergence de la suite

$$(P_{mp^\nu+k}(a))_{\nu\geq\nu_0}\,, \quad k\in\mathbf{Z},$$

en tout $a \in L_{r_\epsilon}$ ainsi que la formule de récurrence que vérifie sa limite, à savoir, l'expression de (1) pour $\nu \to \infty$

$$kf_{m,k}(a) = (2k-1)af_{m,k-1}(a) - (k-1)f_{m,k-2}(a).$$

4.3 Les congruences de Kazandzidis

Comme nous l'annoncions dans la section 2.2, la congruence

$$\binom{np}{kp} \equiv \binom{n}{k} \ mod\ np\mathbf{Z}_p$$

ne représente qu'une version plus faible du résultat[8] suivant, dû à G.S. Kazandzidis [22], [23], [24], qui s'énonce comme suit.

Théorème 4.3.1 *Soit p premier impair; si l'on dénote $\bar{p}(a)$ la plus haute puissance de p qui divise l'entier a, alors les coefficients binomiaux vérifient les congruences*

$$\binom{np}{kp} - \binom{n}{k} \equiv \begin{cases} p^2kn(n-k)\binom{n}{k} & si\ p=3 \\ 0 & si\ p>3 \end{cases} \quad mod\ p^3\bar{p}\left\{kn(n-k)\binom{n}{k}\right\}.$$

On effectue, alors, immédiatement, la traduction.

Corollaire 4.3.1 *Pour tout p premier impair, on a les congruences*

$$\binom{np}{kp} \equiv \binom{n}{k} \ mod\ p^2nk(n-k)\binom{n}{k}\mathbf{Z}_p.$$

On déduit de ce corollaire, le résultat suivant, concernant les deux congruences qui font l'objet de la section précédente.

[8] Cité dans [27], p. 350 et dans [29].

Théorème 4.3.2 *Si, pour p premier impair et $n \geq 1$, on pose*

$$\begin{aligned} H_1 &= P_{np-1}(1+2t) - P_{n-1}(1+2t^p) \equiv 0 \ mod\ np\,\mathbf{Z}_p[t]; \\ H_2 &= P_{np}(1+2t) - P_n(1+2t^p) \equiv 0 \ mod\ np\,\mathbf{Z}_p[t]; \end{aligned}$$

alors la congruence suivante est vérifiée

$$H_1 + H_2 \equiv 0 \ mod\ n^2p^2\,\mathbf{Z}_p[t].$$

Preuve.- Comme nous l'avons observé en section 3.2, H_1 et H_2 admettent le développement

$$H_1 = \sum_{k=0}^{np-1} \binom{np-1}{k}\binom{np+k-1}{k} t^k - \sum_{k=0}^{n-1} \binom{n-1}{k}\binom{n+k-1}{k} t^{pk},$$

$$H_2 = \sum_{k=0}^{np} \binom{np}{k}\binom{np+k}{k} t^k - \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k} t^{pk}.$$

Si l'on pose

$$H_1 + H_2 = \sum_{k=0}^{np} d_k t^k,$$

alors on a

a) $d_0 = 0$;
b) Si p ne divise pas $k \geq 1$, alors

$$\begin{aligned} d_k &= \binom{np}{k}\binom{np+k}{k} + \binom{np-1}{k}\binom{np+k-1}{k} \\ &= \frac{np}{k}\binom{np-1}{k-1}\left\{\binom{np+k-1}{k-1} + \binom{np+k-1}{k}\right\} + \\ &\quad + \left\{\binom{np}{k} - \binom{np-1}{k-1}\right\}\frac{np}{k}\binom{np+k-1}{k-1} \\ &= \frac{np}{k}\binom{np-1}{k-1}\binom{np+k-1}{k} + \frac{np}{k}\binom{np}{k}\binom{np+k-1}{k-1} \\ &= 2\frac{n^2p^2}{k^2}\binom{np-1}{k-1}\binom{np+k-1}{k-1}, \end{aligned}$$

et donc

$$d_k \equiv 0 \ mod\ n^2p^2\mathbf{Z}_p.$$

c) Etudions, maintenant, le coefficient d_{pk}, avec $k < n$. Celui-ci s'écrit

$$d_{pk} = \binom{np}{kp}\binom{np+kp}{kp} - \binom{n}{k}\binom{n+k}{k} + \binom{np-1}{kp}\binom{np+kp-1}{kp} - \binom{n-1}{k}\binom{n+k-1}{k}$$

ou encore, avec les notations de la seconde preuve du théorème 4.2.4

$$d_{pk} = a + b = a + \frac{n-k}{n+k}a = \frac{2n}{n+k}a.$$

Par le corollaire 4.3.1, il existe u et v dans $\mathbf{Z}_p$ tels que

$$\begin{aligned} d_{pk} &= \frac{2n}{n+k}\left\{\binom{n}{k} + up^2nk(n-k)\binom{n}{k}\right\}\cdot\left\{\binom{n+k}{k} + vp^2(n+k)kn\binom{n+k}{k}\right\} - \\ &\quad - \frac{2n}{n+k}\binom{n}{k}\binom{n+k}{k} \\ &= 2n^2p^2\left\{u(n-k)\binom{n}{k}\binom{n+k-1}{k-1} + vk\binom{n}{k}\binom{n+k}{k}\right\} \\ &\equiv 0 \ mod\ n^2p^2\mathbf{Z}_p. \end{aligned}$$

d) Finalement, encore une fois grâce au corollaire 4.3.1, on obtient

$$\begin{aligned} d_{np} &= \binom{2np}{np} - \binom{2n}{n} \\ &\equiv 0 \ mod\ p^2 2n\cdot n\cdot n\binom{2n}{n}\mathbf{Z}_p \\ &\equiv 0 \ mod\ 2n^3p^2\,\mathbf{Z}_p. \end{aligned}$$

Conjecture 4.3.1 *Le théorème 4.3.2 est aussi valable pour $p = 2$.*

Bibliographie

[1] M. Abramowitz, I. A. Stegun, *Handbook of Mathematical Functions*, Dover Publications, Inc., New York, 1975.

[2] Y. Amice, *Les nombres p-adiques*, P.U.F., collection Sup., Paris, 1975.

[3] G. Bachmann, *Introduction to p-Adic Numbers and Valuation Theory*, Academic Press, New York and London, 1964.

[4] D. Barsky, *Congruences des coefficients des polynômes de Legendre*, Exposé présenté au colloque de l'Institut de mathématiques, Neuchâtel, 1989.

[5] Z. I. Borevitch, I. R. Chafarevitch, *Théorie des nombres*, Gauthier-Villars, Paris, 1967.

[6] J. Brillhart, *On the Euler and Bernoulli polynomials*, J. Reine Angewandte Math. 234, 1969, p. 45-64.

[7] J.-L. Brylinski, *Legendre Polynomials and the Elliptic Genus*, Journal of Algebra 145, 1992, p. 83-93.

[8] L. Carlitz, *Congruences for the coefficients of the Jacobi elliptic functions*, Duke Math. J. 16, 1949, p. 297-302.

[9] L. Carlitz, *Congruences for the coefficients of hyperelliptic and related functions*, Duke Math. J. 19, 1952, p. 329-337.

[10] L. Carlitz, *A note on the Staudt-Clausen theorem*, American mathematical monthly 64, 1957, p. 19-21.

[11] L. Carlitz, *Congruence properties of the polynomials of Hermite, Laguerre and Legendre*, Math. Zeitschrift, Bd 59, 1954, p. 474-483.

[12] L. Carlitz, *A note on Euler numbers and polynomials*, Nagoya Math. J., Vol. 7, 1954, p. 35-43.

[13] L. Carlitz, *Note on irreducibility of the Bernoulli and Euler polynomials*, Duke University, 1952, p. 475-481.

[14] P. Cartier, D. Foata, *Problèmes combinatoires de commutation et réarrangements*, Lecture Notes in Mathematics 85, Springer Verlag, Berlin, Heidelberg, New York, 1969.

[15] M. Coster, *Congruence properties of coefficients of certain algebraic power series*, Compositio Mathematica 68-69, 1988-1989, p. 41-57.

[16] J. Dieudonné, *On the Artin-Hasse exponential series*, Proc. Amer. Math. Soc., Vol. 8, 1957, p.210-214.

[17] R. K. Guy, (éditeur), *Reviews in Number Theory 1973-83*, Volume 1A, American Mathematical Society, Providence, Rhode Island, 1984.

[18] M. Hazewinkel, *Formal groups and applications*, Academic Press, Mathematics 78, New York, San Francisco, London, 1978.

[19] J.B. Holt, *The irreducibility of Legendre's Polynomials*, Proc. of the London Math. Soc. 2, Vol. 11, 1913, p. 351-356.

[20] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan, Vol. 22, No. 2, 1970, p. 213-246.

[21] T. Honda, *Two congruence properties of Legendre polynomials*, Osaka J. Math. 13, 1976, p. 131-133.

[22] G. S. Kazandzidis, *A commentary on Lagrange's congruence*, D. Phil. Thesis, Oxford University, Oxford, 1948, version publiée: Dept. of Mathematics, Univ. of Ioannina, Ioannina, 1970.

[23] G. S. Kazandzidis, *Congruences on the binomial coefficients*, Bull. Soc. Grèce (N. S.) 9, 1968, p. 1-12.

[24] G.S. Kazandzidis, *On congruences in number theory*, Bull. Soc. Math. Grèce (N. S.) 10, fasc. 1, 1969, p. 35-40.

[25] N. Koblitz, *P-adic numbers, p-adic analysis and zeta-functions*, Graduate Texts in Mathematics 58, Springer Verlag, 1977.

[26] P.S. Landweber, (éditeur) *Elliptic Curves and Modular Forms in Algebraic Topology*, Proceedings, Princeton 1986, Lecture Notes in Mathematics 1326, Springer Verlag, 1986.

[27] W. J. Leveque, (éditeur), *Reviews in Number Theory*, Volume 1, American Mathematical Society, Providence, Rhode Island, 1974.

[28] W. Magnus, F. Oberhettinger, R. P. Soni, *Formulas and Theorems for the Special Functions of Mathematical Physics*, Die Grundlehren der mathematischen Wissenscaften in Einzeldarstellungen, Band 52, Third Edition, Sringer Verlag, 1966.

[29] R.J. Mc Intosh, *A Generalization of a congruential Property of Lucas*. American mathematical monthly, March 1992, p. 231-238.

[30] M. Pourahmadi, *Taylor expansion of* $\exp\left(\sum_{k=0}^{\infty} a_k z^k\right)$ *and some applications*, American mathematical monthly, Vol. 91, Number 5, May 1984, p. 303-307.

[31] D.C. Ravenel, *Complex Cobordism and Stable Homotopy Groups of Spheres*, Academic Press, 1986.

[32] A. Robert, *A note on the numerators of the Bernoulli numbers*, Expo. Math. 9. 1991, p. 189-191.

[33] A. Robert. *Cours d'analyse ultramétrique*, Troisième cycle romand de mathématiques, Lausanne et Berne, 1990-1991.

[34] A. Robert, *Polynômes de Legendre mod p*, Séminaire d'Analyse, Publication du Département de Mathématiques Pures, Université Blaise Pascal, Clermont II, (à paraître).

[35] A. Robert, *Systèmes de Polynômes*, Queen's papers in pure and applied Mathematics, No. 35, Queen's University, Kingston, Ontario, Canada, 1973.

[36] W. H. Schikhof, *Ultrametric calculus - An introduction to p-adic analysis*, Cambridge studies in advanced mathematics 4, Cambridge University Press, 1984.

[37] C. Vonlanthen, *Polygones de Newton*, Comptes-rendus de l'Académie des Sciences de Paris, tome 315, Série I, 1992, p. 873-876.

[38] J. Wahab, *New cases of irreducibility for Legendre polynomials*, Duke Math. J. 19, 1952, p. 165-176.

[39] M. Zuber, *Propriétés de congruence de certaines familles classiques de polynômes*, Comptes-rendus de l'Académie des Sciences de Paris, tome 315, Série I, 1992, p. 869-872.