NOMBRES p-ADIQUES ET FONCTIONS ZETA: ÉLÉMENTS CLÉFS

COURS DONNÉ PAR GAUTAMI BHOWMIK ET RAF CLUCKERS
LILLE, JANVIER – MAI 2021
LISTE DES ÉLÉMENTS CLÉFS PAR R. CLUCKERS

Version de 08 février 2021

1. Motivation

La motivation de ce cours sur les nombres p-adiques sont certains quantités de comptage, ou encore, de sommation, comme suit.

Soit f un polynôme en n variables avec coefficients en $\mathbb{Z}$. Soit $N > 0$ entier.

Voici des quantités centrales de ce cours:

$$\#\{x \in (\mathbb{Z}/N\mathbb{Z})^n \mid f(x) = 0\}, \tag{1.0.1}$$

et

$$\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^n} \exp(2\pi i \frac{f(x)}{N}).$$

Par le théorème des restes Chinois, le cas le plus important c'est quand $N = p^e$ avec p premier et $e > 0$ entier.

En effet, si on écrit a_N pour la quantité en Equation (1.0.1), et si on écrit $N = \prod p_i^{e_i}$ pour des nombres premiers p_i différents, des entiers $e_i > 0$, alors on a

$$a_N = \prod_{i=1}^{\ell} a_{N_i}$$

avec $N_i = p_i^{e_i}$.

Ces nombres de solutions de f modulo N ont été étudiés par Igusa, Denef, Loeser, et beaucoup d'autres. Ils seront traîtés dans ce cours par Raf Cluckers.

Les nombres a_{p^e} se laissent étudier avec les nombres p-adiques, avec de la géométrie et de l'analyse p-adique. Parfois, 'comptage' deviendra 'intégration'. La géométrie p-adique mentionnée est reliée à la géométrie algébrique, et à la théorie des modèles.

A part les quantités mentionnées, il y a aussi

$$\#\{x \in \mathbb{F}_{p^m}^n \mid f(x) = 0\},$$

avec $\mathbb{F}_{p^m}$ le corps fini à p^e éléments, étudiés en profondeur par Grothendieck, Weil, Dwork, Deligne et beaucoup d'autres. Ils seront traîtés dans ce cours par Gautami Bhowmik.

1: Les nombres p-adiques.

On s'inspire partiellement sur les notes de cours de Serge Cantat [1], qui suit le livre de Koblitz [4]. Il y a aussi le très gentil livre de Svetalena Katok [3] qui traîte les mêmes notions de base.

Voici je liste les notions cléfs.

valuation et norme p-adique sur $\mathbb{Q}$.

la distance p-adique.

$|\cdot|_p$ est un norme ultramétrique sur $\mathbb{Q}$.

Cette norme est spéciale et légèrement contre-intuitif par son aspect ultramétrique (aussi appelée non-archimédienne).

Regardons une boule p-adique dans $\mathbb{Q}$

$$B = \{x \mid \mathbb{Q} \mid |x - a|_p < r\}$$

avec a dans $\mathbb{Q}$ et $r > 0$. Alors, on a que chaque point a' dans B peut servir comme centre de la boule, c'est à dire $B = \{x \mid \mathbb{Q} \mid |x - a'|_p < r\}$.

Cette norme sur $\mathbb{Q}$ est très naturelle et importante, par le théorème d'Ostrowski.

La Section 4 de Koblitz:

Avec les suites de Cauchy, on construit la complétion de $\mathbb{Q}$. On le dénote par $\mathbb{Q}_p$, avec la norme donnée par le norme p-adique.

La norme p-adique sur $\mathbb{Q}_p$ donne alors une topologie sur $\mathbb{Q}_p$, avec base d'ouverts les boules dans $\mathbb{Q}_p$. Cette topologie sur $\mathbb{Q}_p$ est Hausdorff et localement compacte.

Le norme p-adique prend ses valeurs dans $p^{\mathbb{Z}} \cup \{0\}$, il est appelé discret parce que son groupe de valeurs (l'image de $\mathbb{Q}_p^\times$ sous la valuation p-adique) est $\mathbb{Z}$.

Chaque boule en $\mathbb{Q}_p$ est à la fois ouvert et fermé.

Ecriture de Teichmuller d'éléments de $\mathbb{Q}_p$. (L'expansion en 'digits' p-adiques.)

La boule $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ est un sous-anneau de $\mathbb{Q}_p$. C'est un anneau principal avec un unique idéal maximal qui est la boule $p\mathbb{Z}_p$. Un anneau avec un idéal maximal unique est appelé un anneau local.

Une boule ouverte $\{x \in \mathbb{Q}_p \mid |x - a|_p < p^e\}$ avec $e \in \mathbb{Z}$ est appelé de rayon ouvert (normatif) p^e. Son rayon valuatif est e.

Une boule ouverte de rayon ouvert normatif p^e peut être partitionnée en p boules ouvertes de rayon ouvert p^{e-1}.

Une somme $\sum_{i \in \mathbb{N}} a_i$ avec $a_i \in \mathbb{Q}_p$ converge dans $\mathbb{Q}_p$ si et seulement si $|a_i|$ tend vers zéro quand i tend vers l'infini.

Chaque boule dans $\mathbb{Q}_p$ est compacte (toute suite admet une sous-suite convergente).

Pour x dans $\mathbb{Q}_p^n$, on définit $|x| = |(x_1, \ldots, x_n)|_p$ par $\max_i |x_i|_p$. Ceci donne une distance sur $\mathbb{Q}_p^n$.

On met alors sur $\mathbb{Q}_p^n$ la topologie produit. Une boule dans $\mathbb{Q}_p^n$ est un ensemble de la forme $\{x \in \mathbb{Q}_p^n \mid |x - a|_p < r\}$ avec a and $\mathbb{Q}_p^n$ et $r > 0$.

La topologie sur $\mathbb{Q}_p^n$ est complète: chaque suite de Cauchy a une limite. Chaque boule dans $\mathbb{Q}_p^n$ est compacte, ouverte, et fermée (pour la topologie). Les opérations de corps $+, \cdot$ son continue sur $\mathbb{Q}_p^2$, et l'inverse $\cdot^{-1}$ est continue sur $\mathbb{Q}_p^\times$. $\mathbb{Q}_p$ est appelé un corps localement compact (c'est à dire Hausdorff, localement compact, et opérations continues).

Il n'y en a pas beaucoup, de corps localement compacts!

Chaque boule dans $\mathbb{Q}_p^n$ est de la forme $a + p^n\mathbb{Z}_p$ avec a dans $\mathbb{Q}_p$ et $n \in \mathbb{Z}$.

Trouver des zéros de polynôme dans $\mathbb{Q}_p$ est différent pour chaque p, et diffère aussi des cas $\mathbb{R}$ et $\mathbb{C}$.
Par exemple, regardons l'équation $x^2 = -1$ en $\mathbb{Q}_2$, en $\mathbb{Q}_3$ et en $\mathbb{Q}_5$ (donc $\mathbb{Q}_p$ avec $p = 2$, resp. avec $p = 3$ et $p = 5$). Trouvez-vous des suites de Cauchy de nombres rationels qui résoudent cette équation dans chaque cas?

Lemme de Hensel: deux variantes, l'une avec $|f'(a)| = 1$ et $|f(a)| < 1$ et l'autre avec $|f(a)| < |f'(a)|^2$.

2: Excursion sur les corps valués

On suit les sections 3.1 et 3.2 du texte de Cantat sur les corps valués (sans preuves à partir du lemme 3.8).

3: Intégration avec mesure de Haar

4: Varitétés analytiques, changements de variables, Invariant de Serre

5: Rationalité de la fonction zeta d'Igusa

Reconsidérons la fonction zeta d'Igusa

$$Z_{f,p}(s) := \int_{x \in \mathbb{Z}_p^n} |f(x)|^s |dx|$$

pour f un polynôme et $s \geq 0$ réel. Parfois on note $Z_f(s)$ ou $Z_{f,\mathbb{Q}_p}(s)$ pour $Z_{f,p}(s)$.

Avec la résolution des singularités comme démontrée par Hironaka (voir le texte de Popa et le livre d'Igusa, théorème 3.2.1, pour la version avec les variétés analytiques p-adiques), on peut tranformer l'intégrale (par des changements de variables, après avoir pris une partition finie) en une somme finie d'intégrales de la forme

$$\int_{x \in \mathbb{Z}_p^n} |m_1(x)|^s \cdot |m_2(x)||dx|$$

où les m_i sont des momones. Le m_2 viens de la Jacobienne de la transformation.

Ceci nous permet de conclure:

Theorem 1.0.1 (Igusa)**.** *Pour chaque polynôme f dans $\mathbb{Z}[x_1, \ldots, x_n]$, la fonction zeta d'Igusa $Z_f(s)$ est une fonction rationelle en la variable $t = p^{-s}$.*

Donc en particulier, $Z_f(s)$ est méromorphe en t sur $\mathbb{C}$, avec un nombre fini de pôles. En plus, Igusa a formulé une série de conjectures qui sont les analogues des conjectures de Weil pour la fonction zeta de Hasse-Weil.

Aussi dans le cas réel (et également dans le cas complex), on peut considérer les fonctions zeta locale, comme suit:

$$Z_{f,\mathbb{R}}(s) := \int_{x \in \mathbb{R}^n} \phi(x)|f(x)|^s dx$$

Ceux-ci sont aussi méromorphe sur $\mathbb{C}$, avec la même preuve passant par la résolution des singularités. En cas réel et complex, il y a une preuve alternative qui n'existe pas dans le cas p-adique. Cette preuve alternative utilise le polynôme de Bernstein-Sato $b_f(s)$ de f. Rappelons-le. (Voir chapitre 4 du livre d'Igusa.)

Theorem 1.0.2. *Il existe P dans $\mathbb{R}[x, \partial/\partial x_1, \ldots, \partial/\partial x_n]$ et polynômes $b(s)$ tel que P aggissant de gauche sur $f^{s+1}(x)$ donne $b(s) \cdot f^s(x)$, pour tout nombre naturel s. Tels b forment un idéal dans $\mathbb{R}[s]$, qui est généré par un polynôme unique monique de degré minimal. Celui-ci est appelé le polynôme de Bernstein-Sato, et il est noté $b_f(s)$.*

Exemple:

Si $f(x) = x_1$, alors on prend $P = \partial/\partial x_1$ et on trouve $b_f(s) = s + 1$.

Dans le cas réel, le P et b_f peuvent être utilisé avec l'intégration par parties pour calculer $Z_{f,\mathbb{R}}(s)$ et obtenir la rationalité. En Plus, cette preuve alternative donne un lien fort entre les pôles de $Z_{f,\mathbb{R}}(s)$ et les zéros de $b_f(s)$.

Dans le cas p-adique, ce lien est completement ouvert (sauf pour f spéciale, par exemple en deux variables seuelement), mais la question est très simple:

Conjecture 1 (Conjecture forte de monodromie d'Igusa)**.** *Pour chaque pôle $t_0 = p^{-s_0}$ (dans $\mathbb{C}$) de la fonction zeta p-adique d'Igusa $Z_{f,p}(s)$, on a que la partie réelle $\Re(s_0)$ de s_0 est un zéro de $b_f(s)$.*

Notez que $\Re(s_0)$ est un nombre rationel négatif: vérifier ceci sur les monômes, et réduisez au cas de monômes par la résolution.

Les zéros de $b_f(s)$ et les pôles de $Z_{f,p}(s)$ sont très difficile à étudier, mais on sais la chose suivante:

Theorem 1.0.3. *Les zéros de $b_f(s)$ sont des nombres rationels négatifs. Les parties réelles des pôles de $Z_{f,p}(s)$ sont des nombres rationels négatifs. Soit s_0 le zéro de $b_f(s)$ le plus grand (le plus proche de zéro). Alors la partie réelle s_1 d'un pôle de $Z_{f,p}(s)$ satisfie $s_1 \leq s_0$.*

Il y a une troixième stratégie, qui marche dans tout les cas, facilitée par la théorie des modèles, et qui généralise les résultats de rationalité.

Avant de l'aborder, considérons le corps $\mathbb{F}_p((t))$ de caractéristique p.

$\mathbb{F}_p(\!(t)\!)$ est le corps des séries formelles de Laurent avec coefficients dans $\mathbb{F}_p$. Plusieurs choses marches pareil comme pour $\mathbb{Q}_p$ (comme la topologie locallement compact et Hausdorff donc la mesure de Haar), mais aucune des technique pour démontrer la rationalité de $Z_f(s)$ s'adapte au cas de $\mathbb{F}_p(\!(t)\!)$. La résolution de singularités n'est pas connue en caractéristique positive et l'intégration par parties avec le polynôme de Bernstein-Sato a les mêmes problèmes que pour QQ_p...

6: Un peu de théorie des modèles

Langages et structures.

Exemple cléf: Le langage $\mathcal{L}_{\text{ring}}$ des anneaux avec symboles $+, -, \cdot, 0, 1$. Les structures sont naturellement les anneaux.

Les formules dans un langage sont construites avec les symboles du langage et avec les symboles $=, \wedge, \vee, \neg, \exists, \forall, (,)$ et les variables x_i. Tout les variables (ceux qui sont libres et aussi sont qui ne sont pas libre, c'est à dire sous control d'un quantificateur) parcourent la même structure.

Donc, la formule $\exists y(y^2 = x)$ a comme ensemble de solutions dans la structure $\mathbb{R}$ la semi-droite positive $\mathbb{R}_{\geq 0}$. Dans la structure $\mathbb{C}$, l'ensemble de solutions est $\mathbb{C}$ tout entier.

Un sousensemble X de R^n avec R une structure pour un langage $\mathcal{L}$ est appelé *définissable* si c'est l'ensemble de solutions d'une formule en $\mathcal{L}$. Donc, $\mathbb{R}_{\geq 0}$ est un ensemble définissable dans la structure $\mathbb{R}$ pour $\mathcal{L}_{\text{ring}}$.

Une fonctions $f : X \subset R^n \to R^m$ est appelé *définissable* si le graphe de f est définissable.

Theorem 1.0.4 (Tarski/Chevalley)**.** *Dans $\mathbb{C}$ avec $\mathcal{L}_{\text{ring}}$, tout ensemble définissable est donné par une formule sans quantificateurs; ce sont appelés les descriptions algébriques de ces ensembles, ou encore, des ensembles algébriques.*

Ce résultat est une forme d'élimination de quantificateurs (dans une structure avec un langage).

Dans $\mathbb{R}$ ce n'est pas le cas: la demi-droite positive $\mathbb{R}_{\geq 0}$ est définissable mais ne peut pas être décrit par une formule sans quantificateurs. Pourtant on a le suivant:

Theorem 1.0.5 (Tarski: élimination de quantificateurs pour $\mathbb{R}$)**.** *Dans $\mathbb{R}$ avec $\mathcal{L}_{\text{ring},<}$ le langage des anneaux ordonnés $+, -, \cdot, 0, 1, <$, tout ensemble définissable est donné par une formule sans quantificateurs; ce sont appelés les descriptions semi-algébriques de ces ensembles, ou encore tout simplement, des ensembles semi-algébriques dans $\mathbb{R}$.*

Theorem 1.0.6 (Macintyre: élimination de quantificateurs pour $\mathbb{Q}_p$)**.** *Dans $\mathbb{Q}_p$ avec le langage de Macintyre $+, -, \cdot, 0, 1, P_1, P_2, P_3, \ldots, P_n, \ldots$, avec P_n pour $n > 0$ signifiant dans $\mathbb{Q}_p$ le sous ensemble $\{x \in \mathbb{Q}_p \mid \exists y(y^n = x)\}$, tout ensemble définissable est donné par une formule sans quantificateurs; ce sont appelés les descriptions semi-algébriques de ces ensembles, ou encore tout simplement, des ensembles semi-algébriques dans $\mathbb{Q}_p$.*

Exemple d'ensemble définissable:

$$\{(x, y) \in \mathbb{Q}_p^2 \mid \operatorname{ord} x \leq \operatorname{ord} y\}$$

Question ouverte: Quel langage pour $\mathbb{F}_p((t))$ a l'élimination de quantificateurs?

7: Série de Serre - Poincaré

Au lieu de classicalement

$$N_m := \#\{x \in (\mathbb{Z}/p^m\mathbb{Z})^n \mid f(x) = 0\},$$

considérons à sa place

$$\tilde{N}_m := \#\{x \in (\mathbb{Z}/p^m\mathbb{Z})^n \mid \exists y_1 \ldots \exists y_n f(y) = 0 \wedge y \equiv x \bmod p^m\}.$$

Avec $y \equiv x \bmod p^m$ on veut dire que $y_i \equiv x_i \bmod p^m$ pour tout $i = 1, \ldots, n$.

Prenons la fonction de Poincaré introduit par Serre:

$$\tilde{P}_f(t) := \sum_{m=0}^{\infty} \tilde{N}_m t^m.$$

Serre a posé la question sur la méromorphie et la rationalité de $\tilde{P}_f(t)$.

Denef l'a résolu, à deux façons, les deux utilisant l'élimination de quantificateurs pour $\mathbb{Q}_p$: La résolution de singularités, et, avec une décomposition cellullaire.

Les deux techniques réduisent au cas (légèrement généralisé) de monômes.

8: Sommes exponentielles

Au lieu de

$$N_m := \#\{x \in (\mathbb{Z}/p^m\mathbb{Z})^n \mid f(x) = 0\}$$

on peut aussi regarder les sommes exponentielles finies de la forme

$$E_m := \sum_{x \in (\mathbb{Z}/p^m\mathbb{Z})^n} \exp(2\pi i f(x)/p^m).$$

Cas le plus simple: f de degré ≤ 1.

References

1. S. Cantat, course text on https://perso.univ-rennes1.fr/serge.cantat/Cours-Actuel.html.
2. J. Igusa, *An introduction to the theory of local zeta functions*, Studies in advanced mathematics, AMS, 2000.
3. S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007.
4. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Graduate Texts in Mathematics, vol. 58, Springer-Verlag, 1977.
5. M. Popa, course text on https://sites.math.northwestern.edu/ mpopa/571/chapter3.pdf.