Vatsal
27/4

Divisibilité de valeurs spéciales de fonctions L

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$$

$$\pi^{-s/2}\,\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{(1-s)}{2}}\,\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

On déduit : $\zeta(-k) = 0$ pour k pair $k \geq 1$,
$\zeta(-k) \in \mathbb{Q}$ ——— impair $k \geq 1$

Ex. $\zeta(-1) = -\frac{1}{12}$, $\zeta(-3) = \frac{1}{60}$

En general : $\zeta(1-2k) = -\frac{B_k}{k}$

où $\displaystyle\sum_k \frac{B_k t^k}{k!} = \frac{t}{e^t - 1}$ (Euler)

Kummer : p nbre premier impair ≥ 5
$K = \mathbb{Q}(\underbrace{e^{2i\pi/p}}_{\zeta_p})$

On a $p \mid h(K) \iff \exists\, k \in \{2, \dots, p-3\}$
$p \mid$ numerateur de B_k

Plus généralement si on a un caractère de Dirichlet

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

$$L(s,\chi) = \sum \chi(n)\, n^{-s}$$

Si $n \geq 1$ et $\chi(-1) = (-1)^{n+1}$, on a

$$L(1-n,\chi) = -B_{\chi,n}/n$$

où

$$\sum_{n\geq 1} \frac{B_{\chi,n}\, t^n}{n!} = \sum_{a=1}^{N} \frac{\chi(a)\, t\, e^{at}}{e^{Nt} - 1}$$

Si $K = \mathbb{Q}(\sqrt{-p})$, on a
$$h(K) = \frac{\sqrt{p}}{\pi} L(1, \chi) \approx B_{0,\chi}$$
(après équation fonctionnelle, où χ est le caractère de Kronecker)

<u>Question générale</u>:

soit S une famille de caractères de Dirichlet, n entier, p un nombre premier. Combien de $\chi \in S$ vérifient
$$\mathfrak{p} \mid L(1-n, \chi) \quad \text{où } \mathfrak{p} \mid p$$
ds le corps de nombres correspondant.

On sait peu de choses.

Ici on va regarder des "familles p-adiques" :
$$S = \{ \chi : (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times \}$$
où p est fixé, $n \to \infty$.

On regarde <u>alors</u> $L(1-n, \chi)$ $\begin{cases} \text{mod } p \\ \text{mod } \ell \neq p \end{cases}$

Les nombres $\prod_{\chi \bmod p^n} L(0, \chi)$, $\chi \in S$, sont essentiellement les nbres de classes de $K_n = \mathbb{Q}(\zeta_{p^n})$.

Un théorème d'Iwasawa dit que si e_n est défini par $p^{e_n} \| h(K_n)$, on a
$$e_n = \lambda n + \mu p^n + \nu$$
avec λ, μ, ν constantes, n assez grand.

Conjecture d'Iwasawa : - on a $\mu = 0$

Washington a remarqué qu'~~[illegible]~~ expérimentalement on a $\mathrm{ord}_\ell\, h(K_n) \ll 1$.

Ces énoncés ont été démontrés dans les années 80 par Ferraro - Washington, en introduisant de l'ergodicité.

Le point est qu'il faut étudier la divisibilité de $L(0, \chi)$ et pour cela on a besoin d'une formule plus explicite.

Iwasawa a montré :

$B_{0,\chi}$ est lié aux décimales p-adiques des racines $(p-1)$-èmes de l'unité

$$\mathbb{Q}_p \ni \alpha = a_0 + a_1 p + a_2 p^2 + \cdots$$

$$0 \leq a_i \leq p-1$$

et de cela il découle que la divisibilité de ces $B_{n,\chi}$ devient une question sur les décimales de nbres p-adiques.

Comme $\zeta_p \notin \mathbb{Q}$, on s'attend à ce que ces chiffres soient aléatoires, et cela donnerait ce qu'on veut.

On définit $x_n(\alpha) = \frac{1}{p^n}\left(a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}\right)$

$\in [0, 1]$.

Déf. α est normal si $(a_0, \ldots, a_n, \ldots)$ contient toute sous-suite de longueur k avec même fréquence p^{-k}.

Fait : α normal $\iff (x_n(\alpha))_{n\geq 1}$ est équirépartie modulo 1.

Lemme 1. (Ferraro-Washington)
Supposons $\gamma_1, \dots, \gamma_r \in \mathbb{Z}_p$ sont $\mathbb{Q}$-linéairement indépendants. Alors pour presque tout $\beta \in \mathbb{Z}_p$ la suite de vecteurs $x_n(\beta) = (x_n(\beta\gamma_1), \dots, x_n(\beta\gamma_r))$ est équirépartie dans $[0,1]^r$.

C'est un analogue du :
Th. de Kronecker
Soient $\gamma_1, \dots, \gamma_r \in \mathbb{R}$ qui sont $\mathbb{Q}$-linéairement indépendants. Alors
$$\{t(\gamma_1, \dots, \gamma_r) \mid t \in \mathbb{R}\} \subset (\mathbb{R}/\mathbb{Z})^r$$
a image dense.
Plus généralement, l'adhérence de $\{t(\gamma_1, \dots, \gamma_r)\}$ est un sous-tore de $(\mathbb{R}/\mathbb{Z})^r$ de dimension
$$\dim_{\mathbb{Q}} \mathbb{Q}(\gamma_1, \dots, \gamma_r)$$

[cf. Washington, "Cyclotomic fields", § 7.5

Sinnott en 1985 donna une seconde preuve du th. de Ferraro-Washington sans utiliser le lemme 1 (apparemment) : il relie les valeurs de $L(0,\chi)$ à des dérivées de fonction rationnelles. Son lemme clé est :

Lemme 2. Soit $\mathbb{F} = \mathbb{F}_p$, $\mathbb{F}((T-1)) = L$ le corps des series formelles de Laurent en $T-1$.
Si $a \in \mathbb{Z}_p$, on définit
$$L \ni T^a = \sum_{n\geq 0} (T-1)^n \binom{a}{n}$$
extension p-adique

Supposons que $(\gamma_1, \dots, \gamma_r) \in \mathbb{Z}_p^r$ sont $\mathbb{Q}$-linéairement indépendants.
Alors $(T^{\gamma_1}, \dots, T^{\gamma_r})$ sont algébriquement indépendantes dans L.

Concrètement : $$\begin{array}{c} \mathbb{F}_p(T^{\gamma_1}, \dots, T^{\gamma_r}) \simeq \mathbb{F}_p(X_1, \dots, X_r) \\ \cap \\ \mathbb{F}_p((T-1)) \end{array}$$

La preuve est élémentaire (th. d'Artin sur l'indépendance linéaire des caractères).

Il y a ici de la théorie ergodique cachée : $\mathbb{F}_p((T-1))$ est "1-dimensionnel" et $\mathbb{F}_p(X_1, \dots, X_r)$ est de dimension r : un objet de dimension 1 un peu chaotique est dense dans un objet de dimension r.

Cela semble un principe assez général.

K a 2 extensions de type $\mathbb{Z}_p$ suivant signe de la conjugaison complexe

<u>Second exemple</u> : famille anticyclotomique et Rohrlich

Soit $E/\mathbb{Q}$ une courbe elliptique de conducteur N

$K = \mathbb{Q}(\sqrt{-D})$ corps quadratique

p = premier impair ≥ 5

(N, D, p) deux à deux premiers entre eux.

χ : caractère de Hecke de K d'ordre fini

t.q.

(1) $\rho_\chi = \mathrm{Ind}_K^{\mathbb{Q}} \chi$ est diédral

(2) Cond ρ est une puissance de p

On regarde

$$L(E\otimes\rho_\chi, s) = L(E,\chi,s)$$

qui est une convolution de Rankin-Selberg, de degré 4.

L'équation fonctionnelle dit :

$$L^\infty(E,\chi,s) = \varepsilon\, L^\infty(E,\chi,1-s)$$

avec $\varepsilon = \pm 1$.

Avec les hyp. ci-dessous, cela ne dépend que de N, D, p.

Donc $L(E,\chi,s)$ ont un signe fixé pour tout les χ ci-dessous.

<u>Conj.</u> <u>Mazur</u> (84) : $L(E,\chi,\frac{1}{2}) = \begin{cases} 0 & \text{si } \varepsilon = +1 \\ 1 & \text{si } \varepsilon = -1 \end{cases}$

pour "presque tout" χ (tous sauf un nombre fini), où $n \to \infty$, D, N, p fixés !

(<u>ex.</u> χ = trivial)

(On peut aussi le regarder mod p...)

Cela a été démontré par Vatsal et Cornut.

L'ingrédient clé est un théorème de Ratner.

<u>1° étape</u> : relier $L(E,\chi,\frac{1}{2})$ ou $L'(E,\chi,\frac{1}{2})$ à des points CM (Gross-Zagier-Waldspurger...)

<u>2° étape</u> : montrer que les pts CM sont équirépartis.

<u>Th.</u> (Ratner) Soit $G = SL(2,\mathbb{Q}_p)$, $\Gamma_1, \Gamma_2 \subset G$ des sous-groupes discrets cocompacts.

Alors $\Gamma_1\cdot\Gamma_2 = \{\gamma_1\gamma_2 \mid \gamma_i \in \Gamma_i\} \subset G$ est <u>dense</u> dans G si et seulement si $\Gamma_1\cap\Gamma_2$ est d'indice infini ds Γ_1 et Γ_2.

Analogie : $G = \mathbb{R}$

$\Gamma_1 = \mathbb{Z}$

$\Gamma_2 = \gamma\mathbb{Z}$

$\Gamma_1 + \Gamma_2$ est dense $\overset{\text{Kronecker}}{\Longleftrightarrow}$ $\gamma \notin \mathbb{Q}$

$\Longleftrightarrow$ $\Gamma_1 \cap \Gamma_2$ est d'indice infini ds Γ_1 et Γ_2.

Aussi : $G^r = G \times \dots \times G$

$\Gamma = \Gamma_1 \times \dots \times \Gamma_r$

$\Gamma_i \subset G$ discret cocompact

$X = \Gamma \backslash G^r$ compact

Ratner : l'adhérence de $\Delta \{(g, \dots, g)\} \hookrightarrow \Gamma \backslash G^r$ est isomorphe à l'orbite d'un ~~[illegible]~~ groupe contenant Δ.

En particulier : si Γ_i, Γ_j ne sont pas commensurable, l'adhérence de $\Gamma\Delta$ est dense.