

Groupe de travail "Fonction zêta des courbes modulaires"

1. Courbes modulaires

• \mathbb{H} demi-plan de Poincaré $\cong SL_2(\mathbb{R})$. Soit $N \geq 1$ un entier, ses groupes de congruence :

$$\Gamma_1(N) = \left\{ \gamma \in SL_2(\mathbb{Z}), \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}, \quad \Gamma_0(N) = \left\{ \gamma \in SL_2(\mathbb{Z}), \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

↳ sans torsion si $N \geq 4$

surfaces de Riemann
épointées - compacta resp.
↳ courbes alg.
($j(\tau)$ mérom / $X(1)$)
"IP"

$$Y_x(N)(\mathbb{C}) := \mathbb{H} / \Gamma_x(N) \subset X_x(N)(\mathbb{C}) := \frac{\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})}{\Gamma_x(N)}$$

Ex $X_1(N)$ genre 0 si $N \leq 12$ et $N \neq 11$, $X_1(11)$ genre 1: cell $j = -\frac{2^{12}}{11}$
 $X_1(13)$ genre 2, $g(X_2(N)) \xrightarrow{N \rightarrow \infty} \infty$, $X_0(27)$ cell par $\mathbb{Z}[j]$, $j^3 = 1$

• Rôle important en g. alg : espaces de modules de c. ell + struct. niveau, en arithm. } général $X^N - 1$
} Jac $(X(N)/\mathbb{Q}$
} universel! travaux
} en th. alg. nombres
} $\mathbb{Z}, \mathbb{Z}[j], \dots$

Fait $\mathbb{H} \rightarrow \{ (E, P), P \in E[N] \text{ d'ordre } N \}$ induit une bijection
 $\tau \mapsto (E_\tau = \mathbb{C}/\langle \tau, 1 \rangle, \frac{1}{N}) \quad Y_1(N)(\mathbb{C}) \xrightarrow{\sim} \{ -j/2 \}$

Preuve $Aut_0(\mathbb{C}) = \mathbb{C}^*$
 $E_\tau = E_{\tau'} \Leftrightarrow \exists \lambda \in \mathbb{C}^* \quad \lambda(\mathbb{Z} + \tau\mathbb{Z}) = \mathbb{Z} + \tau'\mathbb{Z}$
 puis $\lambda \frac{1}{N} \equiv \frac{1}{N} \pmod{\mathbb{Z} + \tau\mathbb{Z}} \Leftrightarrow N | c \text{ et } d \equiv 1 \pmod{N}$
 " $\frac{c\tau + d}{N}$ par symétrie ($\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$)
 $\Rightarrow \tau' = \frac{a\tau + b}{c\tau + d}$ ■

• Non seulement $Y_x(N)$ défini sur \mathbb{Q} mais il y a une structure canonique :
 $\mathbb{Q}(Y_x(N)) = \left\{ f: Y_x(N)(\mathbb{C}) \rightarrow \mathbb{C} \mid \tilde{f}(q) \in \mathbb{Q}((q)) \right\}$ } q -développement à coeff ds \mathbb{Q}
} $q = e^{2\pi i \tau}$, $\tau \mapsto \tau + 1 \in \Gamma_x(N)$

ex $\mathbb{Q}(Y_0(N)) = \mathbb{Q}(j(\tau), j(N\tau)) \subset \mathbb{Q}(Y_1(N))$
 Soit $q = \frac{x^2 + y^2}{x^2 - y^2}$

ex $X_1(11)$ $y^2 + y = 2^3 - x^2$ (ord 11), $X_0(11)$ isog., $X_0(27)$ isog. à $y^2 + y = x^3$

• Mieux, si $N \geq 5$, $Y_1(N)$ admet un modèle lisse canonique sur $\mathbb{Z}[\frac{1}{N}]$

é.g. $\forall A$ an. comm, $N \in A^*$, $Y_1(N)(A) = \left\{ (E_{A,N}, P_N \hookrightarrow E[N]) \right\}_{\mathbb{Z}} / N$ fonctionnellement en A .
 (modèle lisse)

ua, Katz-Mazur) On l'a vu si $A = \mathbb{C}$

On l'utilisera sur les corps fini $A = \mathbb{k}$. Aussi un modèle pour les pointes.

Problème posé, but du GT: calculer $\#Y_1(N)(k)$ le cas fini avec $N \in \mathbb{N}$

Plus généralement calculer la fonction zêta de Hasse-Weil de $X_1(N)/\mathbb{Q}$

2. Fonction zêta de Hasse-Weil (on se restreint ici aux casels)

Soit C/\mathbb{Q} courbe alg projective lisse, lisse sur $\mathbb{Z}[\frac{1}{N}]$ $N \geq 1$.

$\zeta(C, s) = \prod_p \zeta_p(C, s)$ où le p -fact. eulérien ζ_p ne dépend que de C/\mathbb{Q}_p on se restreindra ici aux $p \nmid N$.

Fixons $p \nmid N$. On regarde $\log Z(C_{\mathbb{F}_p}, t) = \sum_{n \geq 1} \frac{\#C(\mathbb{F}_{p^n})}{n} t^n$, $\zeta_p(C, s) = Z(C_{\mathbb{F}_p}, t^{-s})$

Ex. $C = \mathbb{P}^1, N=1, \log Z(t) = \sum_{n \geq 1} \frac{p^n + 1}{n} t^n = -\log(1+t) - \log(1-pt)$, $Z(C_{\mathbb{F}_p}, t) = \frac{1}{(1-t)(1-pt)}$, $\zeta(\mathbb{P}^1, s) = \zeta(s)\zeta(s-1)$

Soit $g = \text{genre de } C(\mathbb{C})$

Théorème (Hasse, Weil) $Z(C_{\mathbb{F}_p}, t) = \frac{P(t)}{(1-t)^{2g}(1-pt)^{2g}}$ $P(t)$ ~~est~~ degré $2g$, $P = \prod (1-\alpha t)$
 les α sont $2g$ $|\alpha| = p^{g/2} \forall i$ complex
 et $\alpha \leftrightarrow \bar{\alpha}$ involution des racines

preuve $P(t) = \det(1 - \text{Frob}_p t \mid H^1_{\text{ét}}(C_{\mathbb{F}_p}, \mathbb{Q}_\ell))$
 $\forall \ell \neq p \quad \sim \text{Tr}(\text{Pic}^0(C(\mathbb{F}_p)) \otimes \mathbb{Z}[\frac{1}{\ell}]) \otimes \mathbb{Q}_\ell^{2g}$

Conclaire $\zeta(C, s) = \frac{\zeta(s)\zeta(s-1)}{L(C, s)}$ "fonction L de C", converge si $\text{Re } s > \frac{3}{2}$.

Conjecture prolongement mérom. à \mathbb{C} , eq fonctionnelle $s \leftrightarrow 2-s$ (façon à $\alpha \leftrightarrow \bar{\alpha}$) (cf B')

Intérêt; réparation des mt premières liées à C, conjectures type BSD prennent leur sens!

cette conj très largement ouverte: $g=0$ de, $y^m = ax^m + b$ (Weil), c. ell CM (Deuring)

$g=1$: Wiles! + C = courbes modulaires. Dans tous les cas où on sait prouver qq chose c'est car il y a un lien avec les c. mod. (ou les f. automorphes) plus généralement

Ex. $E: y^2 + y = x^3$, c. ell sur $\mathbb{Z}[\frac{1}{3}]$ ou $\mathbb{Q}[\frac{1}{3}]$ $(x, y) \mapsto (9x, y)$

$L_3(E, s) = 1$, $L_p(E, s) = \frac{1}{1+p^{-2s}}$ $\sim p \equiv 2(3)$, $L_p(E, s) = \frac{1}{(1-\pi p^{-s})(1-\bar{\pi} p^{-s})}$

$L(E, s) = L(X, s) = L(f, s)$ f $\frac{p \equiv 2(3)}{27}$ ($\sim X_0(27)$) $\sim p = \pi \bar{\pi}$ de $\mathbb{Z}[\frac{1}{3}]$ $= 1(3)$

X car de Hecke de $\mathbb{Q}[\frac{1}{3}]$ (unique conj) $p \equiv 2(3)$
 poids (21) niveau (3)

Théorème (Eichler-Selmer, Ihara, Deligne, Langlands, Carayol, ...)

$$L(X_1(N), s) = \prod_{\pi} L(\pi, s)^{m(\pi, \Gamma(N))}$$

où π parcourt les rep. aut. irréductibles de $GL_2(\mathbb{A})$ (ens. fini) | $\frac{\Gamma(N)}{\Gamma_0(N)} \neq 0$ ($m(\pi, \Gamma(N))$ est la dim de invariants)
 π a série discrète de parain ρ

(on introduira ce π dans un esp. , $L(\pi, s) = L(f, s)$ où f est la nouvelle forme "pape" dans π normalisée)

\Rightarrow La conj. Hasse-Weil vraie pour $X_1(N)$. (cf. ex. requise)

3. Comptage de cell + structure P_N (3 exposés : Daspineau, Beuzant, Stroth)

Rapports
 Théorie de Hasse E/\mathbb{F}_q cell, $Z(E, t) = \frac{1-at+q}{(1-t)(1-qt)}$, $\#E(\mathbb{F}_q) = q+1-a$
 $|a| \leq 2\sqrt{q}$

ici $X^2 - aX + q$ et $\left\{ \begin{array}{l} \text{le pol car de } \text{Frob}_q \text{ comme endom. de } E/\mathbb{F}_q \\ \text{le pol car de } \text{Frob}_q \text{ comme endom. de } T_\ell(E) \simeq \mathbb{Z}_\ell^2 \\ \forall \ell \neq p \end{array} \right.$

nb Weil de E : $\alpha_\ell =$ racine de $X^2 - aX + q$ ($d^\circ \leq 2$) / \simeq conjugaison complexe.
 (q -nb de Weil pds 1)

Exemple (cell / \mathbb{F}_2)

E	$y^2 + y = x^3$	$y^2 + y = x^3 + x + 1$	$y^2 + y = x^3 + x$	$y^2 + xy = x^3 + x$	$y^2 + xy = x^3 + x + 2$
$\#E(\mathbb{F}_2)$	3	1	5	4	2
a (i.e. α_ℓ)	0	2	-2	-1	1
j invariant	0	0	0	1	1

on voit que tous les nb Weil sont atteints ($a^2 \leq 8$)

① On va compter les cell par classes d'isogénie : E' isogène à E si $\exists E \rightarrow E' / \mathbb{F}_q$
 $0 \mapsto 0$

Fact $\#E(\mathbb{F}_q)$ (i.e. α_ℓ , ou a) est invariant par isogénies

Δ pas $E(\mathbb{F}_q)$ en général : sur \mathbb{F}_3 , $y^2 = x^3 \pm x$ sont isogènes ($\alpha_\ell = i\sqrt{3}$) non isom
 $\left\{ \begin{array}{l} + E(\mathbb{F}_3) \simeq \frac{7}{20} \times \frac{7}{20} \\ - E(\mathbb{F}_3) \simeq \frac{7}{4} \end{array} \right.$

Théorème $E \rightarrow \alpha_\ell$ induit une bijection

(Deserling-Tate) $\begin{array}{c} \text{c. ell} / \text{isogénie} \\ \text{sur } \mathbb{F}_q \end{array} \xrightarrow{\sim} \begin{array}{l} q\text{-nb Weil} \\ \text{de poids } 1 \text{ et } d^\circ \leq 2 \\ + \text{ cond. sur val } \uparrow\text{-adique} \\ \times q \neq p \\ (\quad / \text{ ou } \quad /) \end{array}$

La condition en p dans l'énoncé s'explique par le fait que $E[p^\infty](\overline{\mathbb{F}}_q) \neq (\mathcal{O}_{\mathbb{F}_q})^2$ contrairement au cas $l \neq p$. Il y a deux types de cell sur $\overline{\mathbb{F}}_p$

ordinaire $E[p^\infty](\overline{\mathbb{F}}_p) \cong \mathcal{O}_{\mathbb{F}_p}$ supersingulière $E[p^\infty](\overline{\mathbb{F}}_p) \neq \{0\}$

certains mt de prop et déf équivalentes (ex: mt fini de cell supersing. sur $\overline{\mathbb{F}}_p$, $\approx \frac{q-1}{2}$ \Rightarrow $p \nmid a$... toutes les racines sur $\overline{\mathbb{F}}_p$ (en part \exists cell isogènes / \mathbb{F}_q non $\overline{\mathbb{F}}_q$ isom))

Ex: $p=2$, $f=0$ est l'invariant supersingulier
 $y^2 + y = x^3$, ordinaire mod p ssi $p \equiv 1 \pmod{3}$

Dans l'étude de $E[p^\infty] \rightsquigarrow$ remplacer $T_\ell(E)$ par module de Hecke $D_p(E)$ qui est un $W(\mathbb{F}_q)[F, V]$ module ... complication si $q \neq p$

② L'étape qui suit est le décompte du nb de classes d'isom. dans une classe d'isom. (\sim nb classe de $\mathcal{O}(\mathcal{X}_E)$, tenu compte de p_N)

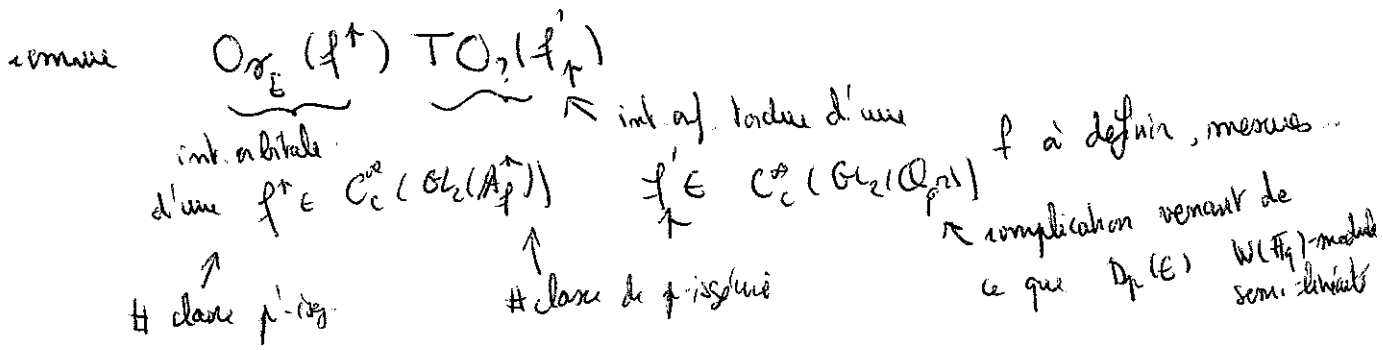
Elle repose sur le

Théorème (Tate)
 "Hom des isogènes"

$$\text{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Z}_\ell \cong \text{Hom}_{\mathbb{Z}_\ell[F, V]}(T_\ell(E), T_\ell(E')) \quad \forall \ell \neq p$$

idem $\ell = p$ $T_\ell \rightarrow D_p$

③ Réécriture du cardinal d'une classe d'isogène ($\sim \mathcal{X}_E$) + p_N structure



4. Comparaison avec formule des traces de Selberg

$p \geq 5$ $\# Y_1(N)(\overline{\mathbb{F}}_p^\times) = \sum_{\substack{\mathcal{X}_E \\ \text{(classes de} \\ \text{isogènes de } \text{GL}_2(\mathbb{Q})}}$ $\tau_{\mathbb{Z}_2} O_{\mathbb{Z}_2}(f^\uparrow) TO_{\mathbb{Z}_2}(f^\uparrow)$ ressemble au terme cell. de la formule des traces de Selberg!

- travail (dans le séminaire)
- i) $TO \rightarrow 0$ si $N > 1$: lemme fondamental ch_1 base
 - ii) $O_{\mathbb{Z}_2}(f^\uparrow) ? \cong 1$: lien avec les pseudo coeff. séries d'unités
 - iii) Rappels form. aut GL_2 , formule des traces
 - iv) Rappels rep. non ramifiées, th. Satake.
 - v) Grâce les points
- Ouvrages: cas plus généraux que GL_2 , facteurs eulériens $\xi_p(X, N)$ $p|N$, décomp. du motif $h^1(X, N)$