Groupe de travail "Fonction zêta des courbes modulaires"

1. Courbes modulaires

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

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

$\hookrightarrow$ sans torsion si $N \geq 4$

$$Y_*(N)(\mathbb{C}) := {}_{\Gamma_*(N)}\backslash \mathbb{H} \quad \subset \quad X_*(N)(\mathbb{C}) := \frac{\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})}{\Gamma_*(N)}$$

surfaces de Riemann épointées - compacte resp.
$\hookrightarrow$ courbes alg
($j(\tau)$ mérom / $X(1)$) $= \mathbb{P}^1$

Ex. $\left[\begin{array}{l} X_1(N) \text{ genre } 0 \text{ si } N \leq 12 \text{ et } N \neq 11,\ X_1(11) \text{ genre } 1 : \text{c ell } j = -2^{12}/11 \\ X_1(13) \text{ genre } 2,\ g(X_*(N)) \xrightarrow[N\to\infty]{} \infty. \quad X_0(27) \text{ c ell CM par } \mathbb{Z}[\rho],\ \rho^3 = 1 \end{array}\right.$

- Rôle important en g alg : espaces de modules de c. ell + struct niveau, en arithm $\left\{\begin{array}{l} \text{général } X^n - 1 \\ \text{Jac}(X_1(N)) \text{ rôle universel ! Travaux en th. alg nombres Iw, Wiles,} \ldots \end{array}\right.$

Fait
$$\begin{array}{ccc} \mathbb{H} & \longrightarrow & \{(E, P),\ P \in E[N] \text{ d'ordre } N\} \\ \tau & \longmapsto & \left(E_\tau = \mathbb{C}/_{\mathbb{Z}+\tau\mathbb{Z}},\ \frac{1}{N}\right) \end{array}$$
induit une bijection $Y_1(N)(\mathbb{C}) \xrightarrow{\sim} \{ - \}/_{\simeq}$

Preuve $E_\tau \simeq E_{\tau'} \Leftrightarrow \exists \lambda \in \mathbb{C}^*$ $\lambda(\mathbb{Z} + \tau'\mathbb{Z}) = \mathbb{Z} + \tau\mathbb{Z}$ ($\mathrm{Aut}_0(\mathbb{C}) = \mathbb{C}^*$) $\left\{\begin{array}{l} \lambda = c\tau + d \\ \lambda\tau' = a\tau + b \\ \hookrightarrow \tau' = \frac{a\tau+b}{c\tau+d} \end{array}\right.$ par symétrie (λ') $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

puis $\lambda \frac{1}{N} \equiv \frac{1}{N}$ $(\mathbb{Z} + \tau\mathbb{Z}) \Leftrightarrow N \mid c$ et $d \equiv 1\ (N)$ ∎

$\lambda \frac{1}{N} = \frac{c\tau + d}{N}$

- Non seulement $Y_*(N)$ défini sur $\mathbb{Q}$ mais il y a une structure canonique :

$$\mathbb{Q}(Y_*(N)) = \left\{ f : Y_1(N)(\mathbb{C}) \xrightarrow{\text{mérom}} \mathbb{C} \ \middle|\ \tilde{f}(q) \in \mathbb{Q}((q)) \right\}$$
q-développement à coeff ds $\mathbb{Q}$, $q = e^{2i\pi\tau}$, $\tau \mapsto \tau + 1 \in \Gamma_*(N)$

ex. $\mathbb{Q}(Y_0(N)) = \mathbb{Q}(j(\tau), j(N\tau)) \subset \mathbb{Q}(Y_1(N))$ Galois gr $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$

Ex. $X_1(11)$ $y^2 + y = x^3 - x^2$ (cond 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 $\mathbb{Z}[\frac{1}{N}]$

t.q. $\forall A$ an comm, $N \in A^\times$, $Y_1(N)(A) = \{(E_{/A}, \mu_N \hookrightarrow E[N])\}/_{\simeq}$ fonctorellement en A (module fin)
c ell $/A$

ua, Katz-Mazur) On l'a vu si $A = \mathbb{C}$
On l'utilisera sur les corps fini $A = k$. Aussi un modèle pour les pointes.

Problème posé, but du GT : calculer $\# Y_1(N)(k)$ k corps fini avec $N \in k^\times$

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 courbes)

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

$$\zeta(C,s) = \prod_p \zeta_p(C,s)$$ où le p-fact. eulerien ζ_p ne dép que de $C/\mathbb{Q}_p$

on se restreindra ici aux $p \nmid N$.

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

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

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

Théorème (Hasse, Weil) $g=1$ $Z(C_{\mathbb{F}_p}, t) = \frac{P(t)}{(1-t)(1-pt)}$ P/ $P(0)=1$ ~~unitaire~~ degré $2g$, $P = \prod(1-\alpha t)$

les α sont t.q. $|\alpha| = p^{1/2}$ $\forall$ $|\cdot|$ complexe

et $\alpha \mapsto p/\alpha$ involution des racines

mieux $P(t) = \det(1 - \mathrm{Frob}_p t \mid H^1_{et}(C_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell))$
$\forall \ell \neq p$

$\simeq T_\ell(\mathrm{Pic}^0(C(\overline{\mathbb{F}}_p)))[\frac{1}{\ell}] \simeq \mathbb{Q}_\ell^{2g}$

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

Conjecture prolongement mérom. à $\mathbb{C}$, éq fonctionnelle $s \leftrightarrow 2-s$ (facteurs à ce qui ajoute) (cf $\mathbb{P}^1$)

intérêt ; répartition des nb premiers liés à C, conjectures type BSD prennent leur sens !

cette conj très largement ouverte : $g=0$ ok, $y^n = \alpha x^m + \beta$ (Weil), c ell CM (Deuring)

$g=1$ Wiles ! + C = courbe modulaires. Dans tous les cas où on sait prouver qqchose 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 CM par $\mathbb{Z}[\rho]$ sur $\mathbb{Q}(\rho)$ $\rho^3 = 1$ $(x,y) \mapsto (\rho x, y)$

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

$L(E,s) = L(\chi, s) = L(f,s)$ f pds 2 niv 27 $((\sim X_0(27))$ si $p = \pi\bar{\pi}$ ds $\mathbb{Z}[\rho]$ $\equiv 1 (3)$

χ car. de Hecke de $\mathbb{Q}(\rho)$ poids $(0,1)$ niveau (3) (unique cong près)

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

$$L(X_1(N), s) = \prod_{\pi} L(\pi, s)^{m(\pi, \Gamma_1(N))}$$

où π parcourt les rep aut. cuspidales de $GL_2(\mathbb{A})$ (ens. fini) $\Big|$ $\pi_f^{\Gamma_1(N)} \neq 0$ ($m(\pi, \Gamma_1(N))$ est la dim des invariants), π_∞ série discrète de poids 2

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

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

3. Comptage de c. ell + structure Γ_N (3 exposés : Dospinescu, Bergeret, Stroh)

Rappels Théorie de Hasse: $E/\mathbb{F}_q$ c. ell, $Z(E,t) = \dfrac{1-at+q}{(1-t)(1-qt)}$, $\# E(\mathbb{F}_q) = q+1-a$, $|a| \leq 2\sqrt{q}$

où $X^2 - aX + q$ est $\begin{cases} \text{le pol car de } \mathrm{Frob}_q \text{ comme endom. de } E/\mathbb{F}_q \\ \text{le pol car de } \mathrm{Frob}_q \text{ comme endom de } T_\ell(E) \simeq \mathbb{Z}_\ell^2 \quad \forall \ell \neq p \end{cases}$

nb Weil de E: γ_E = racine dans $\mathbb{C}$ de $X^2 - aX + q$ ($d° \leq 2$) / $\simeq$ conjugaison complexe

(q-nb de Weil poids 1)

Exemple (c. ell / $\mathbb{F}_2$)

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

NB: sur $\mathbb{F}_p$ (plutôt que $\mathbb{F}_{p^n}$, $n>1$) $d°\gamma_E = 2$ $\forall E$

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

① On va compter les c. ell par classes d'isogénie : E' isogène à E si $\exists\, E \twoheadrightarrow E'$ $/\mathbb{F}_q$, $O \mapsto O$

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

⚠ pas $E(\mathbb{F}_q)$ en général : sur $\mathbb{F}_3$, $y^2 = x^3 \pm x$ sont isogènes non isom ($a=0$, $\gamma_E = i\sqrt{3}$) $\begin{cases} + & E(\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ - & E(\mathbb{F}_3) \simeq \mathbb{Z}/4\mathbb{Z} \end{cases}$

Théorème (Deuring-Tate) $E \to \gamma_E$ induit une bijection

c. ell sur $\mathbb{F}_q$ / isogénie $\xrightarrow{\sim}$ q-nb Weil de poids 1 et $d° \leq 2$ + cond. sur val p-adique si $q \neq p$

(_/ ou /)

La condition en p dans l'énoncé s'explique par le fait que $E[p^\infty](\overline{\mathbb{F}_q}) \not\simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2$ contrairement au cas $\ell \neq p$. Il y a deux types de c ell sur $\overline{\mathbb{F}_p}$

ordinaires $E[p^\infty](\overline{\mathbb{F}_p}) \simeq \mathbb{Q}_p/\mathbb{Z}_p$ supersingulière $E[p^\infty](\overline{\mathbb{F}_p}) = \{0\}$

certains nb de prop et déf équivalentes (ex nb fini $\simeq \frac{q-1}{12}$ de c ell supersing sur $\overline{\mathbb{F}_p}$, supersingl $\Leftrightarrow$ $p \nmid a$ ... toutes isogènes sur $\overline{\mathbb{F}_p}$ (en part $\exists$ c ell isogènes / $\mathbb{F}_q$ non $\overline{\mathbb{F}_q}$ isom)

Ex $p = 2$, $j = 0$ est l'invariant supersingulier

$y^2 + y = x^3$, ordinaire mod p ssi $p \equiv 1\ (3)$

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

② L'étape qui suit est le décompte du nb de classes d'isom dans une classe d'isog (~ nb classe de $\mathcal{O}(\gamma_E)$, tenir compte de μ_N)

Elle repose sur le

Théorème (Tate) "Hom des isogénies"

$$\mathrm{Hom}_{\mathbb{F}_q}(E,E') \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_\ell[\mathrm{Frob}_q]}(T_\ell(E), T_\ell(E')) \quad \forall \ell \neq p$$

idem $\ell = p$ $T_\ell \to D_p$.

③ Récriture du cardinal d'une classe d'isogénie (~ γ_E) + μ_N structure

comme $\underbrace{O_{\gamma_E}(f^p)}_{\text{int. orbitale d'une } f^p \in C_c^\infty(GL_2(\mathbb{A}_f^p))}$ $\underbrace{TO_?(f_p')}$ ← int. orb. tordue d'une $f_p' \in C_c^\infty(GL_2(\mathbb{Q}_{p^n}))$ f à définir, mesures ...

↑ # classe p'-isog ↑ # classe de p-isogénie ← complication venant de ce que $D_p(E)$ $W(\mathbb{F}_q)$-module semi-linéaire

4 Comparaison avec formule des traces de Selberg

$p \geq 5$
$$\# Y_1(N)(\mathbb{F}_{p^n}) = \sum_{\substack{\gamma_E \\ (\text{certaines classes de} \\ \text{conj ss de } GL_2(\mathbb{Q}))}} c_{\gamma_E} O_{\gamma_E}(f^p) TO_{\tilde{\gamma}}(f_p')$$

ressemble au terme ell de la formule des traces de Selberg !

travail
(dans le désordre)

i) $TO \to O$ si $n > 1$ lemme fondamental chgt base

ii) $O_\gamma(f_\infty)$? $= 1$ lien avec les premiers coeff. séries discrètes

iii) Rappels formes aut GL_2, formule des traces

iv) Rappels rep. non ramifiées, transf. Satake

v) Gérer les pointes

Ouvertures cas plus généraux que GL_2, facteurs eulériens $\zeta_p(X_1(N))$ $p \mid N$, décomp. du motif $h^1(X_1(N))$