2014/04/03-04. Journées Louis-Antoine, Rennes, 3x 1heure.

Calcul de représentations galoisiennes attachées aux formes modulaires.

Travail commun avec : Jean-Marc Couveignes, Robin de Jong, Franz Merkl
+ résultats de Bosman, Bruin, Javanpeykar, Mascot, Zeng, ...

Exposé 1

1. Repr. galoisiennes. $\mathbb{C}$ alg. clos : $\forall f \in \mathbb{C}[x]_{\text{unitaire}}$ $f = x^d + f_{d-1}x^{d-1} + \dots + f_0$,
$\exists \alpha_1, \dots, \alpha_d \in \mathbb{C}$: $f = (X-\alpha_1)\cdots(X-\alpha_d)$.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ Cela se dém. en utilisant la topologie, $z \mapsto |f(z)|$...

Pour voir les "symétries des nombres", oublions la topologie ; $\mathrm{Aut}_{\text{Anneaux}}(\mathbb{C})$.

$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : (1, \alpha, \alpha^2, \dots)$ $\mathbb{Q}$-lin. dép.$\}$, nombres algébriques, sous-corps de $\mathbb{C}$.
$\overline{\mathbb{Z}} := \{\alpha \in \overline{\mathbb{Q}} : \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\alpha + \mathbb{Z}\cdot\alpha^2 + \cdots$ est un $\mathbb{Z}$-module de t.f.$\}$, entiers algébriques ; sous-anneau de $\overline{\mathbb{Q}}$, $\overline{\mathbb{Q}} = \mathrm{Frac}(\overline{\mathbb{Z}})$.

$G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \mathrm{Aut}_{\text{Anneaux}}(\overline{\mathbb{Q}})$, (+ topologie pro-fini, compact, tot. disconnexe)
$\mathrm{card}(G_{\mathbb{Q}}) = \mathrm{card}(\mathbb{R})$.

Pour $f \in \mathbb{Q}[x]_{\text{unitair}}$, $d = \deg(f)$, $f = (X-\alpha_1)\cdots(X-\alpha_d)$ dans $\overline{\mathbb{Q}}[x]$,
$K_f := \mathbb{Q}(\alpha_1, \dots, \alpha_n) \subset \overline{\mathbb{Q}}$, corps de décomp. de f dans $\overline{\mathbb{Q}}$; $\dim_{\mathbb{Q}}(K_f) \leq d!$

$\forall \sigma \in G_{\mathbb{Q}}$, $\forall \alpha \in \mathrm{Racines}(f)$: $\sigma(\alpha) \in \mathrm{Racines}(f)$: $0 = \sigma(0) = \sigma(\alpha^d + f_{d-1}\alpha^{d-1} + \dots + f_0) = \dots = f(\sigma(\alpha))$.
$\sigma : K_f \twoheadrightarrow K_f$, $\mathbb{Q} \subset K_f$ galoisienne. $\underset{\shortparallel}{\mathrm{Gal}(K_f/\mathbb{Q})} = \mathrm{Aut}(K_f)$

$G_{\mathbb{Q}} \curvearrowright \mathrm{Racines}(f)$, $G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(f) \subset \mathrm{Sym}(\mathrm{Racines}(f)) \xleftrightarrow{\sim} S_r$
si $\varphi : \{1, 2, .., r\} \xrightarrow{\sim} \mathrm{Racines}(f)$, bijection ou étiquetage.

Repr. galoisienne par permutations : $G_{\mathbb{Q}} \longrightarrow S_r$.

$\overline{\mathbb{Q}} = \bigcup\limits_{\substack{\mathbb{Q} \subset K \subset \overline{\mathbb{Q}} \\ \text{gal. finie}}} K$, $\mathbb{Q} \subset K_{f_1} \subset K_{f_1 f_2}$, $\mathbb{Q} \subset K_{f_2} \subset K_{f_1 f_2}$. $\forall K : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$.

$G_{\mathbb{Q}} = \{ (\sigma_f)_f : \sigma_f \in \mathrm{Aut}(K_f), \forall f_1, f_2 : K_{f_1} \subset K_{f_2} \Rightarrow \sigma_{f_2}|_{K_{f_1}} = \sigma_{f_1} \}$

$G_{\mathbb{Q}} \subset \prod_f \mathrm{Aut}(K_f)$, top. pr., top. discr. sur les facteurs, il est fermé.

$$\overline{\mathbb{Q}}^{\times} \ni \zeta_n^a \longleftarrow a$$

<u>Exemple</u> $f_n := X^n - 1$, $\zeta_n := e^{2\pi i/n}$, $\text{Racines}(f_n) = \langle \zeta_n \rangle \xleftarrow{\sim} \mathbb{Z}/n\mathbb{Z}$

$\text{Gal}\ \mathbb{Q}(\zeta_n) \longrightarrow \text{Aut}(\langle \zeta_n \rangle) = (\mathbb{Z}/n\mathbb{Z})^{\times}$ Gauss: surjectif! (irréd. des Φ_n).

$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(\overline{\mathbb{Q}}^{\times}_{\text{tors}}) = \lim\left((\mathbb{Z}/n\mathbb{Z})^{\times}\right)_n = \hat{\mathbb{Z}}^{\times} = \prod_p \mathbb{Z}_p^{\times}$

$\mathbb{C}^{\times\,\text{tors}} = \overline{\mathbb{Q}}^{\times}_{\text{tors}} \cong \mathbb{Q}/\mathbb{Z}$

$= \bigcup_{n \geq 1} \langle \zeta_n \rangle$ $\qquad \bigcap \quad \prod_n (\mathbb{Z}/n\mathbb{Z})^{\times}$ top. pr. avec top. discr. sur les facteurs.

Pour voir que c'est grand: $(\mathbb{Z}/2!\mathbb{Z})^{\times} \xleftarrow{3:1} (\mathbb{Z}/3!\mathbb{Z})^{\times} \xleftarrow{4:1} (\mathbb{Z}/4!\mathbb{Z})^{\times} \leftarrow \cdots$

$G_{\mathbb{Q}} \longrightarrow \text{Aut}(\langle \zeta_n \rangle) = (\mathbb{Z}/n\mathbb{Z})^{\times}$ (composé noté χ_n) notre 1er ex. de repr. gal. <u>linéaire</u>, de dim. 1 sur $\mathbb{Z}/n\mathbb{Z}$.

<u>Repr. gal. de dim. d sur $\mathbb{Z}/n\mathbb{Z}$</u>: $\rho : G_{\mathbb{Q}} \longrightarrow GL_d(\mathbb{Z}/n\mathbb{Z})$ obtenue d'un $f \in \mathbb{Q}[X]$ et bij. $\varphi : (\mathbb{Z}/n\mathbb{Z})^d \xrightarrow{\sim} \text{Racines}(f)$ t.q. $\forall \sigma \in G_{\mathbb{Q}}$, σ agit sur $(\mathbb{Z}/n\mathbb{Z})^d$ (via φ) par applic. lin: $GL_d(\mathbb{Z}/n\mathbb{Z})$.

(équivalent: ρ est continue pour la top. discr. du but.) même: anneau fini A

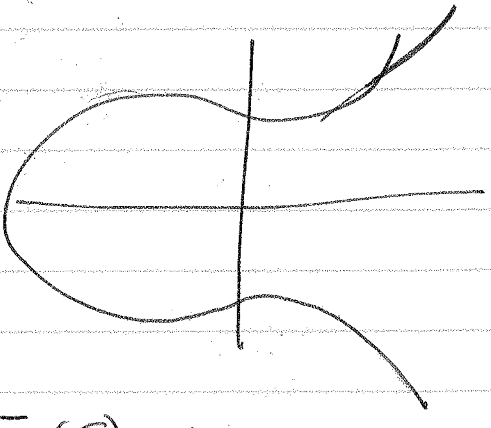
<u>Thm</u> (Kronecker–Weber) $\forall \rho : G_{\mathbb{Q}} \longrightarrow GL_1(\mathbb{Z}/n\mathbb{Z})$, $\exists\, m \geq 1$, $\exists\, \alpha : (\mathbb{Z}/m\mathbb{Z})^{\times} \to GL_1(\mathbb{Z}/n\mathbb{Z})$ t.q. $\rho = \alpha \circ \chi_m$.

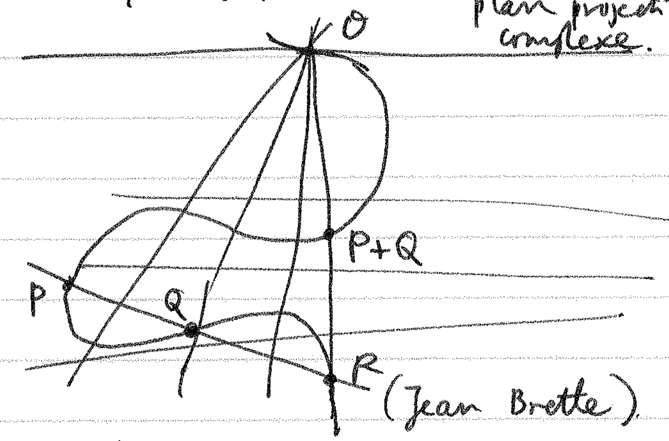
Donc $G_{\mathbb{Q}} \circlearrowright GL_1(\overline{\mathbb{Q}})^{\text{tors}}$ fournit toutes les repr. gal. de dim. 1.

2. <u>Courbes elliptiques</u>.

Pour $a, b \in \mathbb{Q}$ t.q. $4a^3 + 27b^2 \neq 0$ on pose:

$E_{a,b}(\mathbb{C}) := \{(x,y) \in \mathbb{C}^2 : y^2 = x^3 + ax + b\} \cup \{O\}$ point à l'infinie. On a besoin ici du plan projectif complexe.





$E_{a,b}(\mathbb{C})$ est un gr. commutatif, $\cong \mathbb{C}/\text{réseau}$ (fonctions de Weierstrass).

donc $E_{a,b}(\mathbb{C})_{\text{tors}} \cong \mathbb{Q}^2/\mathbb{Z}^2$, $\quad E_{a,b}(\mathbb{C})[n] \xleftarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2$

$\forall P, Q$, $\forall \sigma \in \text{Aut}(\mathbb{C})$: $\sigma(P+Q) = \sigma(P) + \sigma(Q)$ car $\sigma \in \text{Aut}(\mathbb{P}^2(\mathbb{C})$, droites, incidence, $E_{a,b}(\mathbb{C})$, $O)$

$(x,y) \mapsto (\sigma(x), \sigma(y))$

$\forall n \geq 1$, $\forall P$: $\sigma(n.P) = n.\sigma(P)$, $\sigma \circlearrowright E_{a,b}(\mathbb{C})[n] \overset{\text{car } \mathrm{Aut}(\mathbb{C})\text{-orbites finies}}{=} E_{a,b}(\overline{\mathbb{Q}})[n]$.

$$\rho_{E_{a,b},n} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E_{a,b}(\overline{\mathbb{Q}})[n]) \simeq Gl_2(\mathbb{Z}/n\mathbb{Z}).$$

$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(E_{a,b}(\overline{\mathbb{Q}})[n])$ $\quad K = \mathbb{Q}(\text{coordonnées des } P \text{ d'ordre } n)$.

Pour obtenir un $f \in \mathbb{Q}[X]$ et $\mathrm{Racines}(f) \overset{\sim}{\longrightarrow} E(\overline{\mathbb{Q}})[n]$ (bijection compatible à l'action de $G_{\mathbb{Q}}$) : choisir un $P_0 \in \mathbb{P}^2(\mathbb{Q})$ (assez générale), projeter $\mathbb{P}^2(\overline{\mathbb{Q}}) - \{P_0\}$ sur la "droite des x" : $p : \mathbb{P}^2(\overline{\mathbb{Q}}) - \{P_0\} \to \ldots$ ($/\mathbb{Q}$)

$$f = \prod_{P:\, n.P = 0} (X - p(P)).$$

La construction de f à partir de a, b, n et P_0 est explicite.
Le temps de calcul est $\leq (n + \log(|\mathrm{num}(a)| + |\mathrm{den}(a)| + |\mathrm{num}(b)| + |\mathrm{den}(b)|))^{cte}$.
(choisir P_0 assez simple).

<u>Mais</u> : les courbes ell. ne fournissent pas toutes les repr.
$\rho : G_{\mathbb{Q}} \longrightarrow Gl_2(\text{ann. finie})$, même pas les $Gl_2(\mathbb{Z}/n\mathbb{Z})$.

<u>Thm.</u> (Khare+Wintenberger + Kisin 2009 (Conj. de modularité de Serre)). Soit $\mathbb{F}$ un corps fini, $\rho : G_{\mathbb{Q}} \to Gl_2(\mathbb{F})$ t.q. $\det(\rho(\text{conj. complexe})) = -1$, ρ semi-simple.
Alors $\exists$ forme modulaire f, propre pour les opérateurs de Hecke, normalisée, t.q. $\rho \cong \rho_f$. (je n'explique pas ici comment est caractérisé ρ_f, ni ce que c'est f).

<u>Rem.</u> Dans les cas les plus intéressants, c'est même vrai avec $\mathbb{F}$ remplacé par un anneau fini. (repr. résiduelles abs. irréd.).
Cela résulte de la dém. des théorèmes "$R = T$".

<u>Thm.</u> (Couveignes, Edixhoven, de Jong, Bruin, Jarany.) Pour f comme dans le thm. précédent, un polynôme pour ρ_f peut être calculé en temps polynomial en $\#\mathbb{F}$ + niveau(f) + poids(f).

3. Formes modulaires de niveau 1.

Version brève, non-motivée. Voir aussi Serre, Cours d'arithmétique

$$GL_2(\mathbb{R})^+ \circlearrowright \mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

$\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R}) = \mathbb{C} - \mathbb{R} = \mathbb{H} \cup \overline{\mathbb{H}}$.

$\Gamma := SL_2(\mathbb{Z})$.

Pour $k \in \mathbb{Z}$: $S_k(\Gamma) := \left\{ f : \mathbb{H} \to \mathbb{C} : \begin{array}{l} 1.\ f \text{ holomorphe} \\ 2.\ \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : f\left(\frac{az+b}{cz+d}\right) \cdot (cz+d)^{-k} = f(z) \\ 3.\ n \leq 0 \Rightarrow a_n(f) = 0 \end{array} \right\}$

formes mod. cuspidales poids k

$$2 \Leftrightarrow 2' \begin{cases} f(z+1) = f(z) \\ f(-1/z) = z^k \cdot f(z) \end{cases} \qquad f = \sum_{n \in \mathbb{Z}} a_n(f) \cdot q^n, \quad q : \mathbb{H} \to \mathbb{C},\ z \mapsto e^{2\pi i z}$$

$M_k(\Gamma)$: même, avec "$n \leq 0$" remplacé par "$n < 0$".

Séries d'Eisenstein

Exemples Pour $k \in \mathbb{Z}$, $k \geq 4$, pair: $E_k : z \mapsto \dfrac{1}{2\zeta(k)} \cdot \displaystyle\sum_{\substack{(n,m) \in \mathbb{Z}^2 \\ \neq (0,0)}} \frac{1}{(n+mz)^k} \in M_k(\Gamma)$

$$E_k = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n)\, q^n \quad \text{où} \quad \frac{t e^t}{e^t - 1} = \sum_{k \geq 0} B_k \frac{t^k}{k!}, \quad \sigma_r(n) = \sum_{0 < d \mid n} d^r.$$

$$\Delta := \frac{E_4^3 - E_6^2}{1728}, \quad \Delta = q \cdot \prod_{n \geq 1} (1-q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n \qquad \tau(n) \in \mathbb{Z}, \text{ Ramanujan.}$$

discriminant

Fait $\displaystyle\bigoplus_{k \in \mathbb{Z}} M_k(\Gamma) = \mathbb{C}[E_4, E_6]$. $\qquad M_k(\Gamma) = S_k(\Gamma) \oplus \mathbb{C} \cdot E_k$, $k \geq 4$, pair.

$S_k(\Gamma) = \Delta \cdot M_{k-12}(\Gamma)$.

Déf. $M_k(\Gamma, \mathbb{Z}) := \{ f \in M_k(\Gamma) : \forall n,\ a_n(f) \in \mathbb{Z} \}$

$S_k(\Gamma, \mathbb{Z}) := \{ f \in S_k(\Gamma) : \forall n,\ a_n(f) \in \mathbb{Z} \}$.

Thm (C-E-dJ) Admettons GRH. Il existe un algorithme (déterministe) qui, donnés un entier $k \geq 0$, les coeff. $a_i(f)$ pour $0 \leq i \leq k/12$ d'un $f \in M_k(\Gamma, \mathbb{Z})$ et un entier $n \geq 1$ avec sa factorisation en nombres premiers, calcule $a_n(f)$ en temps polynomial en k, $\log n$ et $\max_{i \leq k/12} \log(1 + |a_i(f)|)$.

Conclusions importantes : 1. Les formes modulaires (plus généralement automorphes) sont cruciales pour la compréhension des propriétés analytiques des fonctions L de repr. galoisiennes

2. Les repr. gal. sont cruciales pour calculer rapidement les coeff. des formes modulaires.

4.

4. Application aux fonctions theta de réseaux.

Thm (Jacobi...) Soit $n \geq 0$, pair, $b \in M_n(\mathbb{Z})$ symétrique, définie positive, unimodulaire ($\det(b)=1$), et paire : $\forall i,\ b_{ii} \equiv 0\ (2)$.

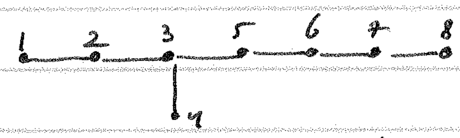
Alors $\Theta_b := \sum_{x \in \mathbb{Z}^n} q^{(x^t b x)/2} : \mathbb{H} \to \mathbb{C}$ est dans $M_{n/2}(\overset{\Gamma}{\overset{\|}{SL_2(\mathbb{Z})}})$.

Rem. Convergence de la Σ : élémentaire.

$\Theta_b(z+1) = \Theta_b(z)$: évident.

$\Theta_b(-1/z) = z^{n/2}\,\Theta_b(z)$: formule de Poisson sur $z = iy$, $y \in \mathbb{R}_{>0}$. ⊗

Exemple $E8 := \mathbb{Z}^8 +$ pr. sc. donné par



$$\begin{pmatrix} 2 & -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & 2 & -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & -1 & 2 & -1 & -1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & -1 & 2 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & -1 & \cdot & 2 & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 & 2 & -1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & 2 & -1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 & 2 \end{pmatrix}$$

Par manque de possibilités ; $\dim_{\mathbb{C}}(M_4(\Gamma)) = 1$, on a

$$\Theta_{E8} = E_4 = 1 + 240 \cdot \sum_{n \geq 1} \sigma_3(n) q^n$$

Exemple Leech, rang 24 ; $\Theta_{Leech} = E_{12} - \frac{65520}{691} \cdot \Delta = \sum_{n \geq 0} r_{Leech}(n) q^n$

Thm (C-E-dJ-M). Admettons GRH. Il existe un algor. déterministe qui, donné le rang n_L et les entiers $r_L(2i)$ pour $1 \leq i \leq n_L/24$ d'un réseau pair unimodulaire (L,b) et un entier $m > 0$ avec sa factorisation en nombres premiers, calcule $r_L(m)$ en temps polynomial en n_L et $\log m$.

On peut l'appliquer aux sommes orthog. de E8 et L.

Avec les génér. de Bruin : on peut traiter les $\mathbb{Z}^n +$ pr. sc. standard,

$r_n(m) = \#\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1^2 + \cdots + x_n^2 = m\}$.

$\exists$ des résultats classiques pour $n \in \{1, 2, 3, 4, 6, 8, 10\}$.

Exposé 2. Courbes modulaires, jacobiennes, opér. de Hecke, repr. galoisiennes.

2.1. Courbes modulaires, modèle analytique complexe.

Déf Pour $n \in \mathbb{Z}_{\geq 1}$:

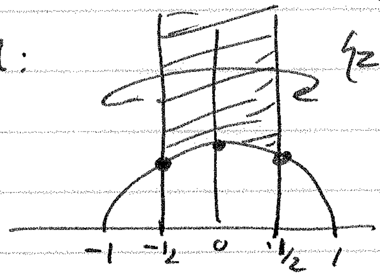
$$\begin{tikzcd} \Gamma(n) \arrow[r, hook] & SL_2(\mathbb{Z}) \arrow[r, two heads] & SL_2(\mathbb{Z}/n\mathbb{Z}) \\ & \Gamma_1(n) \arrow[u, phantom, "\cup"] \arrow[r, "\mathrm{D}"] & \left\{\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}\right\} \arrow[u, phantom, "\cup"] \end{tikzcd}$$

(eng. par $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ et $\begin{pmatrix}1&0\\1&1\end{pmatrix}$)

$\left\{\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}\right\}$ = stab. de $\begin{pmatrix}1\\0\end{pmatrix} \in (\mathbb{Z}/n\mathbb{Z})^2$.

$$SL_2(\mathbb{Z})/\Gamma_1(n) \xrightarrow[\sim]{\text{bij.}} \left\{\begin{pmatrix}a\\b\end{pmatrix} \in (\mathbb{Z}/n\mathbb{Z})^2 : \text{ordre}\begin{pmatrix}a\\b\end{pmatrix} = n\right\}, \quad \text{card} \left(\prod_{p \mid n}\left(1 - \frac{1}{p^2}\right)\right) \cdot n^2$$

Dom. fondamentale pour $SL_2(\mathbb{Z}) \curvearrowright \mathbb{H}$:



$\left\{ z \in \mathbb{H} : -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2},\ |z| \geq 1 \right\}$

$$\begin{tikzcd}
\mathbb{H} \arrow[d] & & & & \Gamma_1(n)\backslash \mathbb{P}^1(\mathbb{Q}) \arrow[d, phantom, "\parallel"] \\
\Gamma_1(n)\backslash\mathbb{H} \arrow[d] & = \{(E,P) : P \in E \text{ ordre } n\}/\cong & =: Y_1(n)(\mathbb{C}) \arrow[d] & \subset X_1(n)(\mathbb{C}) \arrow[d] & \supset \{\text{pointes}\} \arrow[d] \\
SL_2(\mathbb{Z})\backslash\mathbb{H} & = \{E \text{ c.ell.}/\mathbb{C}\}/\cong \arrow[r, "\sim"', "j"] & \mathbb{C} & \subset \mathbb{P}^1(\mathbb{C}) & \supset \{\infty\}
\end{tikzcd}$$

$z \longmapsto (E_z, \frac{1}{n})$

$z \longmapsto \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\cdot z) =: E_z$

$y^2 = x^3 + ax + b$

$j = 1728 \cdot \dfrac{4a^3}{4a^3 + 27b^2}$

$\text{genre}(X_1(n)(\mathbb{C})) \approx \dfrac{n^2}{24}$

$j(E_z) = \dfrac{1}{q(z)} + 744 + 196884 \cdot q(z) + \cdots$

Courbe elliptique universelle :

$$SL_2(\mathbb{Z}) \curvearrowright \left(\begin{tikzcd} \mathbb{Z}^2 \times \mathbb{H} \arrow[r, hook, "{(\binom{n}{m}, z) \mapsto (n+mz, z)}"] \arrow[dr] & \mathbb{C} \times \mathbb{H} \arrow[r, two heads] \arrow[d] & \mathbb{E} \arrow[dl] \\ & \mathbb{H} & \end{tikzcd}\right)$$

$\begin{pmatrix}a & b \\ c & d\end{pmatrix} : (x, z) \mapsto \left(\dfrac{x}{cz+d}, \dfrac{az+b}{cz+d}\right)$

$\left(\begin{pmatrix}n\\m\end{pmatrix}, z\right) \mapsto \left(\begin{pmatrix}a & -b \\ -c & d\end{pmatrix}\begin{pmatrix}n\\m\end{pmatrix}, \dfrac{az+b}{cz+d}\right)$

Pour $n \geq 4$, l'action de $\Gamma_1(n)$ sur $\mathbb{H}$ est libre, ce qui donne :

$$\begin{tikzcd} E_1(n)(\mathbb{C}) \arrow[d] \\ Y_1(n)(\mathbb{C}) \arrow[u, bend left, "0"] \arrow[u, bend right, "P"'] \end{tikzcd}$$

Formes modulaires : pour $\Gamma \subset SL_2(\mathbb{Z})$ d'indice finie, $k \in \mathbb{Z}$,

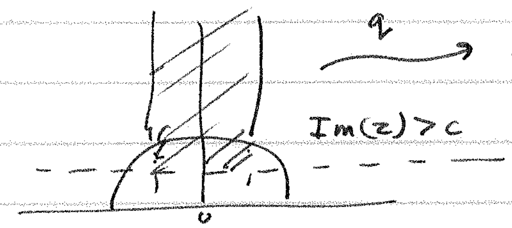
$$S_k(\Gamma) := \left\{ f : \mathbb{H} \to \mathbb{C} : \begin{array}{l} f \text{ holomorphe}, \ \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \ \forall z \in \mathbb{H} \\ f\left(\frac{az+b}{cz+d}\right) \cdot (cz+d)^{-k} = f(z), \ f \text{ hol. et} \\ \text{nulle aux pointes de } \Gamma \end{array} \right\}$$

Pour $n \geq 5$: $S_k(\Gamma_1(n)) = H^0(X_1(n)(\mathbb{C}), \underline{\omega}^{\otimes k}(-\text{pointes}))$,

où $\underline{\omega}$ = l'extension naturelle de $0^* \Omega^1_{E_1(n)/Y_1(n)}$ de $Y_1(n)$ à $X_1(n)$.

Pour $n \geq 5$ et $k = 2$: $S_k(\Gamma_1(n)) = \Omega^1(X_1(n)(\mathbb{C}))$.

Pour finir : pour $n \geq 5$ $X_1(n)(\mathbb{C})$ est recouvert par des disques autour des pointes.



$\xrightarrow{q} D^*(0, e^{-2\pi c}) \hookrightarrow X_1(n)(\mathbb{C})$ imm. ouv. si $c > ??$

2.2. Courbes modulaires, modèle algébrique.
(Tate normal form.)

Soit $n \in \mathbb{Z}_{\geq 4}$.

1. $\forall (E/_k, P)$ E courbe ell. / k avec $n \in k^\times$, $P \in E(k)$ d'ordre n, $\exists !\ s, t \in k$ t.q. $(E, P) \cong (\text{“}y^2 + sxy + ty = x^3 + tx^2\text{”}, (0,0))$, en plus l'isomorphisme est unique.

2. $\exists\, f_n \in \mathbb{Z}[\frac{1}{n}, s, t]$ t.q. $\forall\, \mathbb{Z}[\frac{1}{n}] \to A$, $\forall (E/A, P)$ courbe ell. avec point $P \in E(A)$ partout d'ordre n ($n \cdot P = 0$ et $\forall A \to k$ ...) $\exists ! (f, g)$: $P \overset{g}{\longmapsto} (0,0)$

$$\begin{array}{ccccc} E & \xrightarrow{g} & \text{“}y^2 + sxy + ty = x^3 + tx^2\text{”} & = & E_1(n)_{\mathbb{Z}[1/n]} \\ \downarrow & \square & \downarrow & & \downarrow \\ \operatorname{Spec} A & \xrightarrow[f]{} & \operatorname{Spec} \mathbb{Z}[\frac{1}{n}, s, t, 1/\delta]/(f_n) & =: & Y_1(n)_{\mathbb{Z}[1/n]} \end{array}$$

(δ = discriminant de l'éq. de W.)

Ces f_n sont les analogues des Φ_n pour les $X^n - 1$, racines d'unité.

Voir: "Homogeneous division polynomials for Weierstrass elliptic curves", Jinbi Jin, arxiv.

Voir: Derickx, van Hoeij, Zeng; Baaziz ...

2.3. Jacobiennes des courbes modulaires.

Soit X une surface de Riemann connexe, compacte, $g := \text{genre}(X)$.
Soit $\Omega^1(X)$ l'esp. vect. /$\mathbb{C}$ des 1-formes holom. sur X, $\dim_{\mathbb{C}}(\Omega^1(X)) = g$.
Alors on a : $H_1(X, \mathbb{Z}) \hookrightarrow \Omega^1(X)^\vee \twoheadrightarrow \mathrm{jac}(X)$, la jacobienne de X.

$\gamma \longmapsto \left(\omega \mapsto \int_\gamma \omega\right)$; $\mathrm{jac}(X) \hookleftarrow \mathbb{P}^N(\mathbb{C})$ (Riemann ?), variété algébrique

$\mathbb{Z}$-module libre de rang $2g$, réseau dans $\Omega^1(X)^\vee$.

Il y a aussi une construction algébrique (André Weil).

Soit k un corps, X une courbe alg. lisse et projective et géom. connexe sur k, avec $X(k) \ni P_0$.
Alors le foncteur $\mathrm{Pic}^0_{X/k}$: $\mathrm{Sch}/k \to \mathrm{Ens}$, $S \mapsto \mathrm{Pic}^0(X_S)/\mathrm{Pic}(S)$ ($\{\mathcal{O}_{X_S}$-mod. inv. de d° 0 sur les fibres$\}$/$\cong$)
est représentable, : le schéma représentant

$$\left(\begin{array}{ccc} X_S & \to & X \\ \downarrow & \square & \downarrow \\ S & \to & \mathrm{Spec}\, k \end{array}\right)$$

s'appelle la jacobienne de X ; $\mathrm{jac}(X)$.
C'est une variété abélienne, de dim. $g := \text{genre}(X)$.
$\forall$ ext. de corps $k \to l$: $\mathrm{jac}(X)(l) = \{\text{div. de d° 0 sur } X_l\} / \{\text{diviseurs principaux}\}$ (fonct. rat. $\neq 0$ sur X_l)

En fait, on a $J_1(n)_{\mathbb{Z}[1/n]}$, jac. de $X_1(n)_{\mathbb{Z}[1/n]}$, schéma ab. sur $\mathbb{Z}[1/n]$.

Nos repr. galoisiennes se trouvent dans $J_1(n)(\overline{\mathbb{Q}})_{\text{tors}}$, mais pour les "découper" il nous faut les opérateurs de Hecke.

$(P_1, \dots, P_g) \longmapsto [P_1 + \dots + P_g - g \cdot P_0]$

En fait : $X^g \twoheadrightarrow \mathrm{jac}(X)$; $X^g \searrow X^{(g)} \nearrow \mathrm{jac}(X)$ birationnelle

Weil construisait $\mathrm{jac}(X)$ à partir d'une loi de gr. birationnelle sur un ouvert de $X^{(g)}$.

$X^{(g)} = S_g \backslash X^g$.

2.4. Opérateurs de Hecke.

Pour $\Gamma_1 \subset SL_2(\mathbb{Z})$, $\Gamma_2 \subset SL_2(\mathbb{Z})$ sous-groupes de congruence (contenant un $\Gamma(n)$) et $g \in GL_2(\mathbb{Q})$, $\Gamma := \Gamma_1 \cap g^{-1}\Gamma_2 g$ est d'indice finie dans Γ_1 et dans $g^{-1}\Gamma_2 g$, d'où une correspondance de degrés finis :

$$\Gamma_1 \circlearrowright \mathbb{H}, \quad g^{-1}\Gamma_2 g \circlearrowright \mathbb{H}, \quad g^{-1}\Gamma_2 g \xrightarrow{g(\ )g^{-1}} \Gamma_2 \circlearrowright \mathbb{H}$$

$$\begin{tikzcd}
\mathbb{H} \arrow[rr, "g\cdot", "\sim"'] \arrow[dr, "\text{quot}"] \arrow[dd] & & \mathbb{H} \arrow[d, "\text{quot}"] \\
& Y_\Gamma(\mathbb{C}) \arrow[dl] \arrow[r, "g\cdot"] & Y_{\Gamma_2}(\mathbb{C}) \\
Y_{\Gamma_1}(\mathbb{C}) & &
\end{tikzcd}$$

Cela s'étend :

$$\begin{tikzcd}
& X_\Gamma(\mathbb{C}) \arrow[dl, "s"'] \arrow[dr, "b"] & \\
X_{\Gamma_1}(\mathbb{C}) & & X_{\Gamma_2}(\mathbb{C}),
\end{tikzcd}$$

Cela induit : $\operatorname{jac}(X_{\Gamma_1}(\mathbb{C})) \longrightarrow \operatorname{jac}(X_{\Gamma_2}(\mathbb{C}))$

$$[D] \longmapsto b_* s^*[D]$$

De même du côté algébrique.

Pour $J_1(n)_{\mathbb{Z}[1/n]}$: on a des T_m, $m \geq 1$, dans $\operatorname{End}(J_1(n)_{\mathbb{Z}[1/n]})$, $\quad \operatorname{End}(J_1(n)_{\mathbb{Q}}) =$

donnés par : $X_1(n)(\overline{\mathbb{Q}}) \longrightarrow \operatorname{Div}(X_1(n)(\overline{\mathbb{Q}}))$ (pour m premier, $m \nmid n$: $g := \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$)

$$(E, P) \longmapsto \sum_{\substack{G \subset E \text{ ssgr.} \\ \text{d'ordre } m \\ \text{t.q. } G \cap \langle P \rangle = 0}} (E/G, \overline{P}).$$

$\mathbb{T}_1(n) :=$ le sous anneau de $\operatorname{End}(J_1(n)_{\mathbb{Z}[1/n]})$ engendré par les T_m.
Il est commutatif, $\mathbb{Z}$-module libre, de rang $g(X_1(n))$.
Il est très important ! Il contient les relations que satisfont les T_m.
Comme $H_1(X_1(n)(\mathbb{C}), \mathbb{Z})$ est un $\mathbb{T}_1(n)$-module fidèle, on peut calculer $\mathbb{T}_1(n)$ comme anneau + ce module.
"Modular symbols algorithms".

Même : $H_1(Y_1(n)(\mathbb{C}), \mathbb{Z}) = \pi_1(Y_1(n)(\mathbb{C}))^{ab} = H_1(\Gamma_1(n), \mathbb{Z}) =$
$= H_1(SL_2(\mathbb{Z}), \operatorname{Ind}_{\Gamma_1(n)}^{SL_2(\mathbb{Z})} \mathbb{Z})$.

$$\boxed{\begin{array}{l}\text{Pour poids } k \geq 2 : \\ \mathbb{Z}[x,y]_{k-2} = \operatorname{Sym}^{k-2}(\mathbb{Z}^2).\end{array}}$$

2.5. Repr. galoisiennes.

alg. de Hecke de $S_k(SL_2(\mathbb{Z}), \mathbb{Z})$

"Thm 2.5.13 +2.5.7" de [E-C]. Soit ℓ premier, $k \in \mathbb{Z}$ t.q. $2 < k \leq \ell+1$,
$f : \mathbb{T}(1,k) \twoheadrightarrow \mathbb{F}$ avec $\mathbb{F}$ un corps fini, de car. ℓ, t.q.
la repr. y attachée $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ est abs. irréductible.
Alors $\exists ! f_2 : \mathbb{T}_1(\ell) \twoheadrightarrow \mathbb{F}$ t.q. $\forall n : f_2(T_n) = f(T_n)$,
Pour $(t_1, \dots, t_r)$ des gén. de $\ker(f_2)$ ρ_f est réalisée par

$$V_f := \bigcap_{1 \leq i \leq r} \ker(t_i, J_1(\ell)(\overline{\mathbb{Q}})[\ell]).$$

Exemple: $k=12$, $\mathbb{T}(1,12) = \mathbb{Z}$, $S_{12}(SL_2(\mathbb{Z}), \mathbb{Z}) = \mathbb{Z}\cdot\Delta$, $\Delta = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n \geq 1} \tau(n) \cdot q^n$.
Donc $\forall \ell \geq 11$, $\ell \notin \{691\}$ $\quad T_n \in \mathbb{Z}$: c'est $\tau(n)$.

$\rho_{\Delta,\ell}$ réalisée par $V_\ell := \bigcap_{i \leq \frac{\ell^2-1}{6}} \ker(T_i - \tau(i), J_1(\ell)(\overline{\mathbb{Q}})[\ell])$.

On fait comme pour une courbe elliptique.

Comment calculer un polynome P_ℓ dans $\mathbb{Q}[X]$ pour V_ℓ ?
En principe, c'est bien simple! $J_1(\ell)$ est une var. alg. proj. sur $\mathbb{Q}$, on peut la décrire avec des équations, disons plongée dans un $\mathbb{P}^N_{\mathbb{Q}}$. On écrit l'addition, les T_i $(i \leq \frac{\ell^2-1}{6})$ et on a des équations pour les ℓ^2 points de V_ℓ. On choisit une fonction rationnelle $f : J_1(\ell) \dashrightarrow \mathbb{A}^1_{\mathbb{Q}}$ définie sur $\mathbb{Q}$, qui envoie $V_\ell \hookrightarrow \overline{\mathbb{Q}}$ et alors on a $P_\ell := \prod_{x \in V_\ell} (X - f(x))$ $\in \mathbb{Q}[X]$. On calcule ces ℓ^2 points.

Problème: cela prend trop de temps. Nous voulons un temps de calcul qui est polynomial en ℓ. Mais la dim. de $J_1(\ell)$ est $\approx \ell^2/24$, résoudre les équations pour V_ℓ prend un temps exp. en cette dim.... (Nous savons bien résoudre des syst. d'éq. linéaires, mais les alg. de bases de Gröbner sont soumis au "fléau de la dimension".

Exposé 3.

3.1. Calculs, côté théorique, complexité : objectif : démontrer un théorème.

Donc on n'optimise pas le temps de calcul asymptotique, mais on cherche à minimiser la longueur des démonstrations.

On a vu : calculs exact directe prend trop de temps.

Donc : approximer.

Calcul numérique au lieu de calcul symbolique.

cas de Δ

Rappelons la situation : $V_\ell \subset J_1(\ell)(\overline{\mathbb{Q}}) \xrightarrow{f_\ell} \overline{\mathbb{Q}}$ f_ℓ rationnelle, déf. sur $\overline{\mathbb{Q}}$.

$$P_\ell := \prod_{x \in V_\ell} (X - f_\ell(x)) \in \mathbb{Q}[X], \quad P_\ell = \sum_i P_{\ell,i} X^i, \quad P_{\ell,i} \in \mathbb{Q}; \; P_{\ell,i} = \frac{a_{\ell,i}}{b_{\ell,i}}$$

$\mathrm{pgcd}(a_{\ell,i}, b_{\ell,i}) = 1$.

E-de Jong-Merkl : $\exists c \in \mathbb{N}$ t.q. pour des f_ℓ spécifiées $\forall \ell, \forall i$ $\underbrace{\log \max(|a_{\ell,i}|, |b_{\ell,i}|)}_{\text{hauteur log. de } P_{\ell,i}} \leq c \cdot \ell^{16}$.

(voir p. 252)

La démonstration : théorie d'Arakelov, Riemann-Roch arithmétique ; ≈ 70 pages.

Couveignes : Il existe un algorithme déterministe qui, donné ℓ et un $M \in \mathbb{Z}_{>0}$, calcule des $\tilde{P}_{\ell,i} \in \mathbb{Q}$ t.q. $\forall i$: $|P_{\ell,i} - \tilde{P}_{\ell,i}| < e^{-M}$, en temps polynomial en ℓ et M. (livre : p. 334).

La démonstration : 110 pages, et c'est difficile !

Pourquoi cela resoud notre problème ? Soit $x = \frac{a}{b}$, $x' = \frac{a'}{b'}$, $a, a', b, b' \in \mathbb{Z}$
$x \neq x'$. $|a|, |a'|, |b|, |b'| \leq B$.

$$\text{Alors } |x - x'| = \left|\frac{a}{b} - \frac{a'}{b'}\right| = \left|\frac{ab' - a'b}{bb'}\right| \geqslant \frac{1}{|bb'|} \geqslant \frac{1}{B^2}.$$

Donc une approximation $\underset{\in}{y} \mathbb{Q}$ de x avec $|x - y| < \frac{1}{2B^2}$ détermine x.

Même : x est un convergent de la fraction continue de y.

Donc : on peut calculer P_ℓ en temps polynomial en ℓ.

Variantes : approximation par congruences. On connaît $x = \frac{a}{b}$ si on connaît ses images dans $\mathbb{F}_p$ pour $p \in S$, t.q. $\prod_{p \in S} p > 2 \cdot \max(|a|, |b|)^2$.

On verra plus loin comment les calculs sont faits.

3.2. Éléments de Frobénius, coeff. de formes modulaires.

Donc nous savons calculer $V_\ell \xrightarrow[f_\ell]{\sim} \text{Racines}(P_\ell)$, $P_\ell \in \mathbb{Q}[x]$.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cap\, \overline{\mathbb{Q}}$

Modifier f_ℓ : $P_\ell \in \mathbb{Z}[x]$.

Alors $\text{Racines}(P_\ell) \subset \overline{\mathbb{Z}}$

$$\begin{array}{ccccc} m & \subset & \overline{\mathbb{Z}} & \xrightarrow{\varphi} & \overline{\mathbb{F}}_p \\ \vee & & \cup & & \cup \\ p\mathbb{Z} & \subset & \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p \end{array}$$

Si $p \nmid \text{discr}(P_\ell)$,

$$\text{Racines}(P_\ell, \overline{\mathbb{Z}}) \xrightarrow[\sim]{\varphi} \text{Racines}(P_\ell, \overline{\mathbb{F}}_p) \circlearrowleft \text{Frob}_p : x \mapsto x^p$$

Cela donne $\rho_\Delta(\text{Frob}_p) \in \rho_\Delta(G_{\mathbb{Q}}) \subset GL(V_\ell)$, classe de conj. dans $G_{\mathbb{Q}}$ indép. de m.

Relation de congruence d'Eichler-Shimura : $\text{tr}(\rho_\Delta(\text{Frob}_p)) = \tau(p)$ dans $\mathbb{F}_\ell$
$\qquad\qquad\qquad\qquad\qquad\qquad \det(\rho_\Delta(\text{Frob}_p)) = p^{11}$ ——— .

Deligne : $|\tau(p)| \leq 2 \cdot p^{11/2}$.

Tout ensemble : on peut calculer $\tau(p)$ en temps pol. en $\log(p)$: mod ℓ pour les $\ell \leq B$, $\prod_{\ell \leq B} \ell > 4 \cdot p^{11/2}$.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \approx e^B$.

Dans le livre avec Couveignes ... : calculer $T_p \in \mathbb{T}(1, k)$.

Si k variable : temps polynomial sous GRH ; il faut suffisamment ~~des~~ de $m \subset \mathbb{T}(1,k)$ ~~de~~ avec $\#(\mathbb{T}(1,k)/m)$ petit. Déterministe.

Bruin $T_p \in \mathbb{T}(\Gamma_1(n), k)$. (Probabiliste : car utilise corps finis).

3.3. Calculs réalisés.

$$\Omega^1(X_1(\ell)(\mathbb{C})) = \mathbb{C}\cdot\omega_1 \oplus \cdots \oplus \mathbb{C}\cdot\omega_g$$

Bosman (2006–2008)

$$X_1(\ell)(\mathbb{C})^g \longrightarrow J_1(\ell)(\mathbb{C}) = \mathbb{C}^g/\Lambda \supset \tfrac{1}{\ell}\Lambda/\Lambda \supset V_\ell$$

$$(P_1,\dots,P_g) \longmapsto \sum_{i=1}^{g} \int_{P_0}^{P_i} (\omega_1,\dots,\omega_g) \qquad \Lambda = H_1(X_1(\ell)(\mathbb{C}),\mathbb{Z})$$

$$\omega_i = \sum_{n\geq 1} a_{i,n} q^n \cdot \frac{dq}{q}$$

$X_1(\ell)(\mathbb{C}) = \bigcup$ disques autour des pointes.

"Homotopy continuation method".

Montrer la table page 170 : polynômes certifiés

repr. projectives $PGL_2(\mathbb{F}_\ell) \circlearrowleft \mathbb{P}(V_\ell)$

$(\# \mathbb{P}^1(\mathbb{F}_\ell) = \ell+1)$

Montrer aussi les congruences au début.

Mascot. (2013) Doctorant de Couveignes, va bientôt soutenir.

Methode complexe de Couveignes :

$x \in V_\ell$, $\tilde{x} \in \frac{1}{\ell}\Lambda$, appr. $\frac{\tilde{x}}{2^m}$ avec intégr. comme Bosman, convergence beaucoup meilleure, ensuite 2· dans jac. avec diviseurs, à la Khuri-Makdisi.

Innovations : ① fonction $f_\ell : J_1(\ell) \dashrightarrow \mathbb{A}^1_{\mathbb{Q}}$ plus simple (moins de poles)

② $GL_2(\mathbb{F}_\ell)$ / partie impaire de $\mathbb{F}_\ell^\times$: on trouve les congr. sans ambiguïté de signes.

③ utilisation des ~~resolvantes~~ résolvantes des Dokchitser.

Montrer ses tables ! Ses polynômes (non publiés) ne sont pas encore certifiés : trop grand pour "polred".

Zeng, Jinxiang: (doctorant de Yin Linsheng à Tsinghua) avec Maarten Derickx et Mark van Hoeij.

Methode des corps finis, suivant des algorithmes de Florian Hess (≈ 2000) : analogue au calcul ~~de~~ de en theorie des nombres: ~~mais~~ $X_1(\ell) \xrightarrow{f} \mathbb{P}^1$.

Il utilise aussi les améliorations ①②③ de Mascot, $(K \hookrightarrow \mathbb{Q})$ mais arrive bien à travailler dans des jacobiennes de quotients de $X_1(\ell)$:

$$\begin{array}{ccc} \mathbb{F}_\ell^\times & \circlearrowright & X_1(\ell) \\ \cup & & \downarrow \\ H & & X_1(\ell)/H. \end{array}$$

avantage:

Bons modèles des $X_1(\ell)/H$ fournis par Derickx + van Hoeij: Polynômes certifiés pour repr. projectives.

Peng, Tian: ~~doc~~ doctorant de René Schoof. A ~~ete~~ généralisé le code de Bosman pour traiter quelques $X_1(\ell)/H$.