Modular curves of $\mathcal{D}$-elliptic sheaves and applications

Mihran Papikian

Pennsylvania State University

Motivation: Shimura curves

B=indefinite division quaternion algebra over $\mathbb{Q}$.

$\mathcal{O}$=maximal order in B.

$\Gamma = \{\gamma \in \mathcal{O} \mid \mathrm{Nr}(\gamma) = 1\}$.

$\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.

$\Gamma \hookrightarrow B \otimes \mathbb{R} \approx M_2(\mathbb{R})$ acts on $\mathcal{H}$.

$X_\Gamma = \Gamma \setminus \mathcal{H}$ is a compact Riemann surface.

X_Γ is a moduli space of abelian surfaces with multiplication by $\mathcal{O}$, so

$$X_\Gamma \to \mathrm{Spec}(\mathbb{Z}).$$

X_Γ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/d])$.

Questions about X_Γ

1.1) Fundamental domain of X_Γ in $\mathcal{H}$.

1.2) Explicit generators of Γ in $\mathrm{SL}_2(\mathbb{R})$.

These are computationally difficult problems; only for a few Γ the answer is known, cf.

M. Alsina and P. Bayer:
"Quaternion orders, quadratic forms and Shimura curves" Amer. Math. Soc. 2004

2) Equation of X_Γ as a curve in $\mathbb{P}^2_{\mathbb{Q}}$.

Such equations are known only for finitely many Γ, cf.

A. Kurihara: "On some examples of equations defining Shimura curves and the Mumford uniformization"

3) $X_\Gamma(K)$ for "interesting" K.

K finite (Ihara, Shimura, Cherednik, Drinfeld).

$X_\Gamma(\mathbb{R}) = \emptyset$ (Shimura).

K=local non-archimedean such that $X_\Gamma(K) = \emptyset$ are classified (Jordan-Livné).

K=number field - partial results (Jordan,...)

Function field analogue of X_Γ

$F = \mathbb{F}_q(T)$, $A = \mathbb{F}_q[T]$, $\infty = 1/T$.

For $x \in |F|$, $\mathbb{F}_x$=residue field at x,
$\deg(x) = [\mathbb{F}_x : \mathbb{F}_q]$, $q_x = \#\mathbb{F}_x$.

$F_\infty = \mathbb{F}_q(\!(1/T)\!)$=completion of F w.r.t. $|\cdot|_\infty$.

$\mathbb{C}_\infty = \hat{\bar{F}}_\infty$.

$\Omega = \mathbb{C}_\infty - F_\infty$=Drinfeld's half-plane.

D=division quaternion algebra split at ∞, i.e., $D \otimes_F F_\infty \approx M_2(F_\infty)$.

$\mathcal{D}$=maximal A-order in D.

R=places where D ramifies ($\#R$ is even).

$\Gamma = \mathcal{D}^\times$

$$\Gamma \hookrightarrow D^\times(F) \hookrightarrow D^\times(F_\infty) \cong \mathrm{GL}_2(F_\infty).$$

$X^{\mathcal{D}} = \Gamma \setminus \Omega$ (this is a Mumford curve).

$\mathcal{D}$-elliptic sheaves

$X^{\mathcal{D}}$ is a coarse modular curve of $\mathcal{D}$-*elliptic sheaves* (Drinfeld, Stuhler)

$\mathcal{D}$-elliptic sheaves are a generalization of Drinfeld modules.

Let K be an A-field, i.e. there is a non-zero homomorphism $\gamma : A \to K$.

Drinfeld module (a.k.a. *elliptic module*) over K is an embedding

$$A \hookrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}) = K\{\tau\}, \quad (\tau b = b^q \tau)$$

such that the induced action of A on the tangent space is via γ.

$\mathcal{D}$-*elliptic module* over K is (more-or-less) an embedding

$$\mathcal{D} \hookrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^2)$$

with a condition on the induced action of A on the tangent space. (The actual definition is in terms of sheaves equipped with an action of $\mathcal{D}$ and a Frobenius modification.)

Remark. $\mathcal{D}$-elliptic sheaf gives rise to a left $\mathcal{D}^{\text{opp}} \otimes_{\mathbb{F}_q} K\{\tau\}$-module which is a t-motive of A-rank 4 and τ-rank 2 equipped with an action of $\mathcal{D}$.

$X^{\mathcal{D}}$ has a canonical model over F with good reduction at every place $v \notin R \cup \infty$ (Laumon-Rapoport-Stuhler).

$X^{\mathcal{D}}$ has totally degenerate reduction at every place $v \in R \cup \infty$ (Hausberger, Stuhler).

Remark. [LRS] introduces higher dimensional versions of $X_I^{\mathcal{D}}$ with level structures and uses them to prove the local Langlands correspondence in positive characteristic.

Fundamental domains for $X^{\mathcal{D}}$

$\mathcal{T}$=Bruhat-Tits tree of $\mathrm{PGL}_2(F_\infty)$.

Γ acts on $\mathcal{T}$. By Serre-Bass theory, knowing the quotient graph $\Gamma \setminus \mathcal{T}$ is equivalent to having a presentation for Γ.

Let $\mathrm{Odd}(R) = 1$ if all places in R have odd degrees, and $\mathrm{Odd}(R) = 0$ otherwise.

Theorem.
(1) $\Gamma \setminus \mathcal{T}$ is a finite graph with no loops.

$$(2) \quad h_1(\Gamma \setminus \mathcal{T}) = 1 + \frac{1}{q^2-1} \prod_{x \in R} (q_x - 1) - \frac{q}{q+1} \cdot 2^{\#R-1} \cdot \mathrm{Odd}(R)$$

(3) Every vertex of $\Gamma \setminus \mathcal{T}$ has degree either 1 or $q+1$, and

$$V_1 = 2^{\#R-1} \cdot \mathrm{Odd}(R)$$

$$V_{q+1} = \frac{2}{q-1} \left(h_1(\Gamma \setminus \mathcal{T}) - 1 + 2^{\#R-2} \cdot \mathrm{Odd}(R) \right)$$

Although the statement of the theorem is purely combinatorial, the proof of its key parts is arithmetic:

$\Gamma \setminus \mathcal{T}$ is the dual graph of $X^{\mathcal{D}} \otimes \mathbb{F}_\infty$;

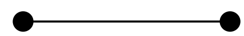
$h_1(\Gamma \setminus \mathcal{T})$=genus of $X^{\mathcal{D}}$;

Vertices of $\Gamma \setminus \mathcal{T}$ of degree 1 are in bijection with Galois orbits of elliptic points on $X^{\mathcal{D}}$.

Examples.

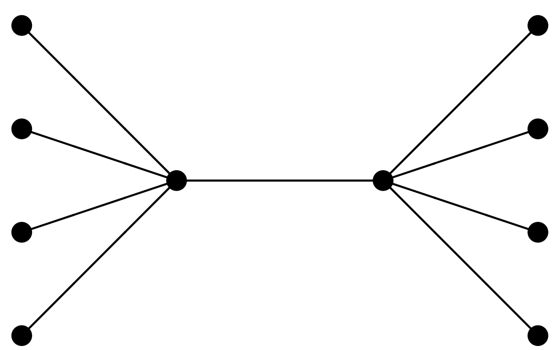
(1) $R = \{x, y\}$ and $\deg(x) = \deg(y) = 1$.

Then $h_1 = 0$, $V_1 = 2$, $V_{q+1} = 0$, so $\Gamma \setminus \mathcal{T}$ is



(2) $R = \{x, y, z, w\}$, $\deg(x) = \cdots = \deg(w) = 1$, and $q = 4$.

Then $h_1 = 0$, $V_1 = 8$, $V_5 = 2$, so $\Gamma \setminus \mathcal{T}$ is

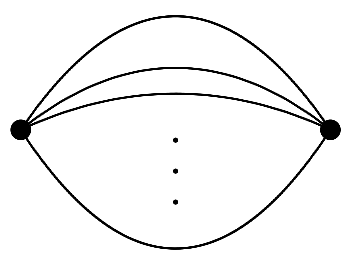


(1) and (2) are the only cases when $\Gamma \setminus \mathcal{T}$ is a tree.

(3) "Hyperelliptic case":

$R = \{x, y\}$, $\deg(x) = 1$ and $\deg(y) = 2$.

Then $h_1 = q$, $V_1 = 0$, $V_{q+1} = 2$, so $\Gamma \setminus \mathcal{T}$ is



Corollary. Γ can be generated by

$$2^{\#R-1} + h_1(\Gamma \setminus \mathcal{T})$$

elements. $\Gamma/\Gamma_{\mathrm{tor}}$ is a free group on $h_1(\Gamma \setminus \mathcal{T})$ generators.

Corollary. Γ can be generated by torsion elements if and only if one of the following holds:

(1) $R = \{x, y\}$ and $\deg(x) = \deg(y) = 1$. In this case, Γ has a presentation

$$\langle \gamma_1, \gamma_2 \mid \gamma_1^{q^2-1} = \gamma_2^{q^2-1} = 1,\ \gamma_1^{q+1} = \gamma_2^{q+1} \rangle.$$

(2) $R = \{x, y, z, w\}$, $\deg(x) = \cdots = \deg(w) = 1$, and $q = 4$. In this case, Γ has a presentation

$$\langle \gamma_1, \ldots, \gamma_8 \mid \gamma_1^{15} = \cdots = \gamma_8^{15} = 1,\ \gamma_1^{5} = \cdots = \gamma_8^{5} \rangle.$$

Explicit sets of generators of Γ

Assume q is odd. If $\Gamma = \Gamma_{\mathrm{tor}}$, then can write down the explicit matrices generating Γ as a subgroup of $\mathrm{GL}_2(F_\infty)$.

Example. Let $q = 3$, $R = \{(T), (T-1)\}$.
Denote $\mathfrak{d} = T(T-1)$.
Γ is isomorphic to the subgroup of $\mathrm{GL}_2(F_\infty)$ generated by the matrices

$$\gamma_1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$\gamma_2 = \begin{pmatrix} 1 & (T+1) - \sqrt{\mathfrak{d}} \\ -(T+1) - \sqrt{\mathfrak{d}} & 1 \end{pmatrix}$$

both of which have order 8 and satisfy
$\gamma_1^4 = \gamma_2^4 = -1$.

In the general case, D has a presentation

$$i^2 = \mathfrak{p}, \quad j^2 = \mathfrak{d}, \quad ij = -ji,$$

where $\mathfrak{p}$ is an appropriate irreducible polynomial in A and $\mathfrak{d}$ is the discriminant of D.

$$\mathcal{D} = A \oplus Ai \oplus Aj \oplus Aij$$

is an Eichler order of level $\mathfrak{p}$ (so it is maximal if only if $\mathfrak{p} \in \mathbb{F}_q^\times$ is a constant).

Theorem. Let $\Gamma = \mathcal{D}^\times$. The finite set of elements

$$\gamma = a + bi + cj + dij \in \Gamma$$

satisfying

$$\max(\deg(a), \deg(b), \deg(c), \deg(d))$$
$$\leq q^{\deg(\mathfrak{p}) + \deg(\mathfrak{d})}$$

generates Γ.

$X^{\mathcal{D}}$ over finite fields

Let X be a smooth, geometrically irreducible projective curve over $\mathbb{F}_q$ of genus $g(X)$.

Drinfeld and Vladut proved

$$\limsup_{g(X)\to\infty} \frac{\#X(\mathbb{F}_{q^n})}{g(X)} \leq q^{n/2} - 1$$

Weil's bound only gives $\leq 2q^{n/2}$ (in particular, curves of large genus never have as many points as the Weil bound allows).

Definition. A sequence of curves $\{X_i\}_{i\in\mathbb{N}}$ over $\mathbb{F}_{q^n}$ is called *asymptotically optimal* if

$$\lim_{i\to\infty} \frac{\#X_i(\mathbb{F}_{q^n})}{g(X_i)} = q^{n/2} - 1.$$

Theorem. (Ihara, Tsfasman, Vladut, Zink)
If q^n is a square, then asymptotically optimal sequences of curves exist.

It is still not known whether D-V is the best possible upper bound when q^n is not a square (even for a single q^n).

If q^n is a square then every <u>known</u> asymptotically optimal sequence has the property that for all sufficiently large i the curve X_i is a classical, Shimura or Drinfeld modular curve.

Theorem. Let $v \notin R \cup \infty$.
$\{X^{\mathcal{D}}\}_D$ and $\{X_I^{\mathcal{D}}\}_I$ are asymptotically optimal over $\mathbb{F}_v^{(2)}$.

Let D be a central division algebra over F of dimension d^2. Fix some place $v \notin R \cup \infty$. Assume I is coprime to v. Denote the reduction of $X_I^{\mathcal{D}}$ at v by $X_{I,v}^{\mathcal{D}}$. The finite group $(A/I)^\times$ acts on $X_{I,v}^{\mathcal{D}}$ via its natural action on the level structures. Denote the quotient variety by X_I.

Theorem. There is an infinite subset $\{\mathfrak{p} \lhd A\}$ of prime ideals in A such that each $X_\mathfrak{p}$ is a smooth, projective, geometrically irreducible, $(d-1)$-dimensional variety defined over $\mathbb{F}_v$ and

$$\lim_{\deg(\mathfrak{p})\to\infty} \frac{\# X_\mathfrak{p}(\mathbb{F}_v^{(d)})}{h(X_\mathfrak{p})} = \frac{1}{d} \prod_{i=1}^{d-1} (q_v^i - 1),$$

where $h(X_\mathfrak{p})$ is the sum of ℓ-adic Betti numbers.

Moreover, the limit of the Weil-Deligne bound for $\# X_\mathfrak{p}(\mathbb{F}_v^{(d)})$ is $q_v^{d(d-1)/2}$.

$\underline{X^{\mathcal{D}} \text{ over local fields}}$

Let $v \in |F|$.

K= finite extension of F_v.

$f = f(K/F_v)$= relative degree of K/F_v.

$e = e(K/F_v)$= ramification index of K/F_v.

$A \ni \wp_v$= monic generator of (v) for $v \neq \infty$.

$$X^{\mathcal{D}}(K) \stackrel{?}{=} \emptyset$$

Places of good reduction.

Theorem. Assume $v \in |F| - R - \infty$.

- If f is even, then $X^{\mathcal{D}}(K) \neq \emptyset$.
- If f is odd, then $X^{\mathcal{D}}(K) = \emptyset$ if and only if for every α satisfying a polynomial of the form

  $$X^2 + aX + c\wp_v^f \quad \text{with } a \in A \text{ and } c \in \mathbb{F}_q^\times,$$

  either some place in $(R \cup \infty)$ splits in the quadratic extension $F(\alpha)$ of F, or $\wp_v$ divides α and v splits in $F(\alpha)$.

Remark. To decide whether $X^{\mathcal{D}}(K) = \emptyset$ one needs to consider only finitely many quadratic polynomials. If q is even, then $X^{\mathcal{D}}(K) \neq \emptyset$. If q is odd and $\deg(a) > f \deg(v)/2$, then ∞ splits in $F(\alpha)$.

Finite places of bad reduction.

Theorem. Assume $v \in R$.

1. If f is even, then $X^{\mathcal{D}}(K) \neq \emptyset$.
2. If f is odd and e is even, then $X^{\mathcal{D}}(K) = \emptyset$ if and only if in every quadratic extension $F(\sqrt{c\wp_v})/F$, with $c \in \mathbb{F}_q^{\times}$, some place in $(R - v) \cup \infty$ splits.
3. If f and e are both odd, then $X^{\mathcal{D}}(K) = \emptyset$.

Corollary. $X^{\mathcal{D}}(F) = \emptyset$.

Place at infinity.

Theorem. If $[K : F_\infty] > 0$, then $X^{\mathcal{D}}(K) \neq \emptyset$. $X^{\mathcal{D}}(F_\infty) = \emptyset$ if and only if $\mathrm{Odd}(R) = 1$.

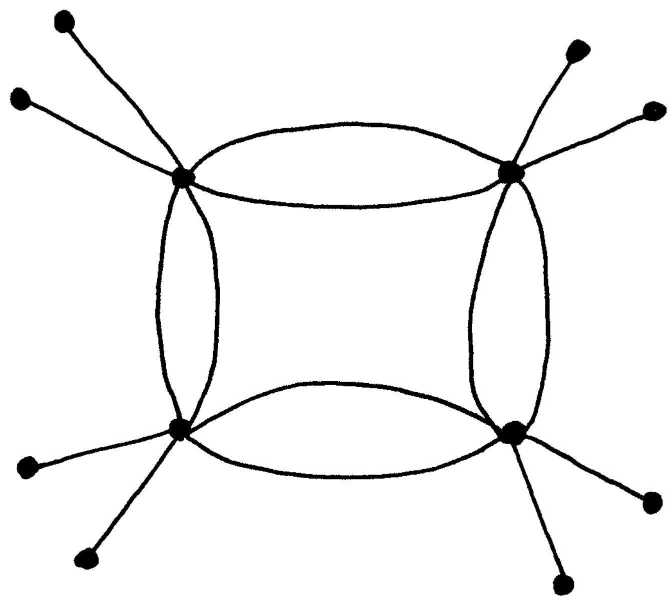
Corollary. Assume q is odd, $R = \{v, w\}$, and $\deg(v) = \deg(w) = 1$.
Let $\xi \in \mathbb{F}_q^\times$ be a non-square and $\mathfrak{d} = \wp_v \wp_w$. Then $X^{\mathcal{D}}$ is isomorphic to the conic in $\mathbb{P}^2_F$

$$X^2 - \xi Y^2 - \mathfrak{d} Z^2 = 0.$$

Ralf Butenuth

$q = 5 \qquad R = \{x, y, z, w\}$

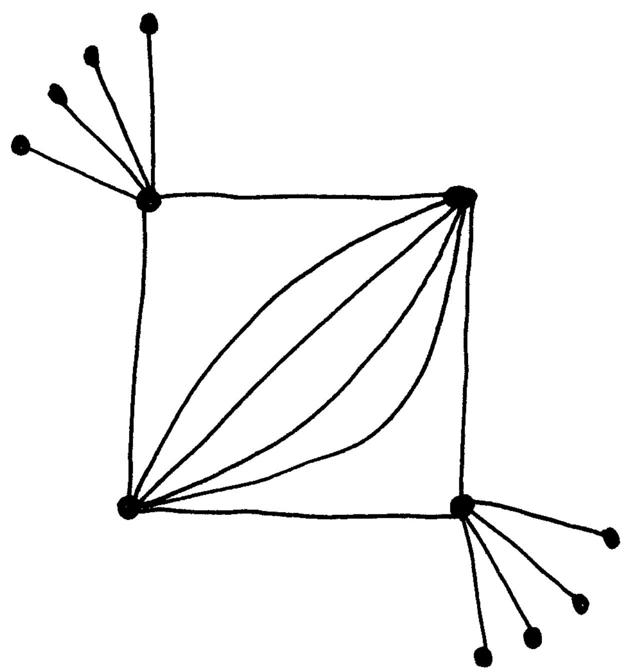
$\deg(x) = \deg(y) = \deg(z) = \deg(w) = 1$



$h_1 = 5$

$V_1 = 8$

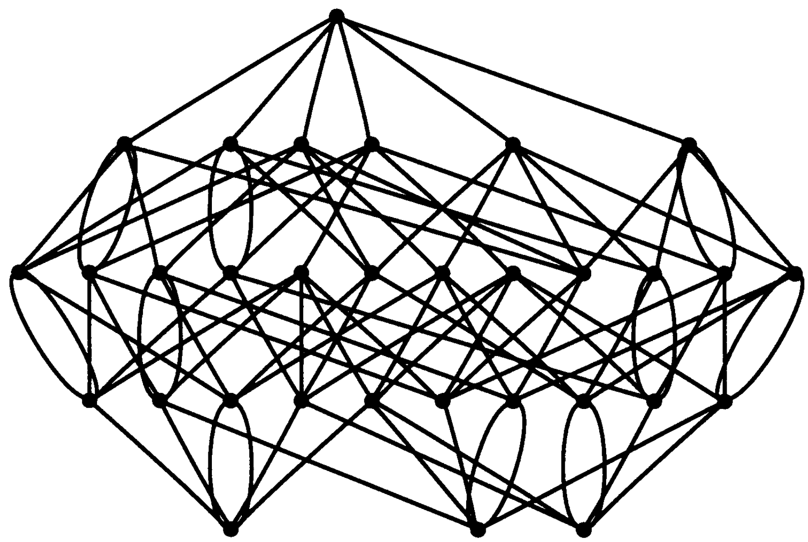
$V_6 = 4$



Has the same h_1, V_1, V_6 but does not occur as $\Gamma \backslash \mathcal{J}$

$q = 5$

$\mathrm{disc} = T(T+1)(T+2)(T^2+2)$



$q = 5$

$\mathrm{disc} = T(T+1)(T+2)(T^2+3)$