Serre's obstruction for genus 3 curves

Christophe Ritzenthaler

Institut de Mathématiques de Luminy, CNRS

Geocrypt, Guadeloupe, April 27 - May 1, 2009

Outline

Geometric Torelli theorem

k algebraically closed field.
A_g : space of (isom. classes of) g-dimensional p.p.a.v.
M_g : space of (isom. classes of) curves of genus g.
j canonical principal polarization on $\operatorname{Jac} X$.

Geometric Torelli Theorem (Weil)

Torelli's morphism θ :

$$\begin{array}{ccc} X & \mapsto & (\operatorname{Jac} X, j) \\ \mathsf{M}_g & \longrightarrow & \mathsf{A}_g \end{array}$$

is injective.

Arithmetic Torelli theorem

k arbitrary field. $(A, a)/k \in \mathsf{A}_g$ such that $(A, a) \simeq_{\overline{k}} (\operatorname{Jac} X_0, j_0)$.

Arithmetic Torelli theorem (Serre)

There is a model X/k of X_0 such that :

1. *If X_0 is hyperelliptic, there is a k-isomorphism*

$$(\operatorname{Jac} X, j) \xrightarrow{\sim} (A, a).$$

2. *If X_0 is not hyperelliptic, there is a quadratic character ε of $\operatorname{Gal}(k^{sep}/k)$, and a k-isomorphism*

$$(\operatorname{Jac} X, j) \xrightarrow{\sim} (A, a)_\varepsilon$$

where $(A, a)_\varepsilon$ is the twist of A by ε

(if ε is not trivial, then (A, a) is not a Jacobian).

Jacobians in dimension 2 and 3

$g = 2$ (resp. $g = 3$)

$$\dim \mathsf{M}_g = 3g - 3 = \dim \mathsf{A}_g = g(g+1)/2 = 3 \text{ (resp. } 6).$$

$(A, a)/\overline{k}$ *indecomposable* : (A, a) is not isomorphic to a product of p.p.a.v.

Curve of genus $g \leq 3$ *over* $\overline{k}$ $\overset{\text{Jac}}{\Longleftrightarrow}$ *abelian variety of dimension* g*, with an indecomposable principal polarization*

Applications to maximal curves of genus $g \leq 3$

To construct a genus g curve with many points N over $\mathbb{F}_q$:

- find an abelian variety A over $\mathbb{F}_q$ with trace of Frobenius $q + 1 - N$;

Applications to maximal curves of genus $g \leq 3$

To construct a genus g curve with many points N over $\mathbb{F}_q$:

- find an abelian variety A over $\mathbb{F}_q$ with trace of Frobenius $q + 1 - N$;
- prove that A has an indecomposable principal polarization ;

Applications to maximal curves of genus $g \leq 3$

To construct a genus g curve with many points N over $\mathbb{F}_q$:

- find an abelian variety A over $\mathbb{F}_q$ with trace of Frobenius $q + 1 - N$;
- prove that A has an indecomposable principal polarization ;
- use arithmetic Torelli to conclude.

Applications to maximal curves of genus $g \leq 3$

To construct a genus g curve with many points N over $\mathbb{F}_q$:

- find an abelian variety A over $\mathbb{F}_q$ with trace of Frobenius $q+1-N$;
- prove that A has an indecomposable principal polarization ;
- use arithmetic Torelli to conclude.

$g = 2$: all curves are hyperelliptic : ok.
$g = 3$: curves can be non hyperelliptic $\rightsquigarrow$ the quadratic twist is a Jacobian and its number of points is minimum.

Theorem (Lauter 2002)

Let $m = \lfloor 2\sqrt{q} \rfloor$. For all q there exists a genus 3 curve C over $\mathbb{F}_q$ such that

$$|\#C(\mathbb{F}_q) - q - 1| \geq 3m - 3.$$

Applications to maximal curves of genus $g \leq 3$

To construct a genus g curve with many points N over $\mathbb{F}_q$:

- find an abelian variety A over $\mathbb{F}_q$ with trace of Frobenius $q+1-N$;
- prove that A has an indecomposable principal polarization ;
- use arithmetic Torelli to conclude.

$g = 2$: all curves are hyperelliptic : ok.
$g = 3$: curves can be non hyperelliptic $\rightsquigarrow$ the quadratic twist is a Jacobian and its number of points is minimum.

Theorem (Lauter 2002)

Let $m = \lfloor 2\sqrt{q} \rfloor$. For all q there exists a genus 3 curve C over $\mathbb{F}_q$ such that

$$|\#C(\mathbb{F}_q) - q - 1| \geq 3m - 3.$$

Serre's Question (letter to Top, February 2003) : how to compute the twist ε ?

Analytic Siegel modular forms

Siegel upper half space of genus g

$$\mathbb{H}_g = \left\{\tau \in \mathbf{M}_g(\mathbb{C}) \mid {}^t\tau = \tau,\ \mathrm{Im}\,\tau > 0\right\}.$$

$\mathbf{R}_{g,h}(\mathbb{C})$: space of *analytic Siegel modular forms* of weight h on $\mathbb{H}_g$, i.e. holomorphic functions $\phi(\tau)$ on $\mathbb{H}_g$ satisfying

$$\phi(M.\tau) = \det(c\tau + d)^h \phi(\tau)$$

for any $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$.

Geometric Siegel modular forms

A_g : moduli stack of p.p.a.s. of relative dimension g

$$\pi : \mathsf{V}_g \longrightarrow \mathsf{A}_g \quad \text{(universal p.p.a.s)}$$

Ω^1 : rank g bundle induced by relative regular differential forms on $\mathsf{V}_g/\mathsf{A}_g$.
Relative canonical line bundle $\boldsymbol{\omega}_{\mathsf{V}_g/\mathsf{A}_g} = \bigwedge^g \pi_* \Omega^1$ over A_g :

$$\begin{array}{c} \boldsymbol{\omega}_{\mathsf{V}_g/\mathsf{A}_g} \\ \downarrow \\ \mathsf{A}_g \end{array} \qquad \Omega^1_k[A] = H^0(A, \Omega^1_A \otimes k), \quad \boldsymbol{\omega}_k[A] = \bigwedge^g \Omega^1_k[A].$$

Space of geometric Siegel modular forms of weight h over a ring R :

$$\mathbf{S}_{g,h}(R) = \Gamma(\mathsf{A}_g \otimes R, \boldsymbol{\omega}^{\otimes h})$$

Analytic and geometric modular forms

$A = (A, a)$ p.p.a.v. of dimension g defined over $k \subset \mathbb{C}$.

Analytic and geometric modular forms

$A = (A, a)$ p.p.a.v. of dimension g defined over $k \subset \mathbb{C}$.
$\omega_1, \ldots, \omega_g$ basis of $\Omega^1_k[A]$ and $\gamma_1, \ldots \gamma_{2g}$ symplectic basis (for a) such that

$$\Omega_a = [\Omega_1\ \Omega_2] = \begin{bmatrix} \int_{\gamma_1} \omega_1 & \cdots & \int_{\gamma_{2g}} \omega_1 \\ \cdots & & \cdots \\ \int_{\gamma_1} \omega_g & \cdots & \int_{\gamma_{2g}} \omega_g \end{bmatrix} \qquad (A, a) \simeq (\mathbb{C}^g / \Omega_a \mathbb{Z}^{2g}, J_{2g})$$

satisfies $\tau_a = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_g$.

Analytic and geometric modular forms

$A = (A, a)$ p.p.a.v. of dimension g defined over $k \subset \mathbb{C}$.
$\omega_1, \ldots, \omega_g$ basis of $\Omega^1_k[A]$ and $\gamma_1, \ldots \gamma_{2g}$ symplectic basis (for a) such that

$$\Omega_a = [\Omega_1 \ \Omega_2] = \begin{bmatrix} \int_{\gamma_1} \omega_1 & \cdots & \int_{\gamma_{2g}} \omega_1 \\ \cdots & & \cdots \\ \int_{\gamma_1} \omega_g & \cdots & \int_{\gamma_{2g}} \omega_g \end{bmatrix} \qquad (A, a) \simeq (\mathbb{C}^g / \Omega_a \mathbb{Z}^{2g}, J_{2g})$$

satisfies $\tau_a = \Omega_2^{-1} \Omega_1 \in \mathbb{H}_g$.

Proposition

Let $\omega = \omega_1 \wedge \cdots \wedge \omega_g \in \boldsymbol{\omega}_k[A]$ and $\widetilde{f} \in \mathbf{R}_{g,h}(\mathbb{C})$.

$$f((A, a)) = (2i\pi)^{gh} \frac{\widetilde{f}(\tau_a)}{(\det \Omega_2)^h} \cdot \omega^{\otimes h}.$$

Then the map $\widetilde{f} \mapsto f$ is an isomorphism $\mathbf{R}_{g,h}(\mathbb{C}) \longrightarrow \mathbf{S}_{g,h}(\mathbb{C})$.

Analytic and geometric modular forms

$A = (A, a)$ p.p.a.v. of dimension g defined over $k \subset \mathbb{C}$.
$\omega_1, \ldots, \omega_g$ basis of $\Omega^1_k[A]$ and $\gamma_1, \ldots \gamma_{2g}$ symplectic basis (for a) such that

$$\Omega_a = [\Omega_1\ \Omega_2] = \begin{bmatrix} \int_{\gamma_1} \omega_1 & \cdots & \int_{\gamma_{2g}} \omega_1 \\ \cdots & & \cdots \\ \int_{\gamma_1} \omega_g & \cdots & \int_{\gamma_{2g}} \omega_g \end{bmatrix} \qquad (A, a) \simeq (\mathbb{C}^g / \Omega_a \mathbb{Z}^{2g}, J_{2g})$$

satisfies $\tau_a = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_g$.

Proposition

Let $\omega = \omega_1 \wedge \cdots \wedge \omega_g \in \boldsymbol{\omega}_k[A]$ and $\widetilde{f} \in \mathbf{R}_{g,h}(\mathbb{C})$.

$$f((A, a)) = (2i\pi)^{gh} \frac{\widetilde{f}(\tau_a)}{(\det \Omega_2)^h} \cdot \omega^{\otimes h}.$$

Then the map $\widetilde{f} \mapsto f$ is an isomorphism $\mathbf{R}_{g,h}(\mathbb{C}) \longrightarrow \mathbf{S}_{g,h}(\mathbb{C})$.

Notation : $f((A, a), \omega) = f((A, a))/\omega^{\otimes h} \in \mathbb{C}$.

Thetanullwerte and the form $\widetilde{\chi}_h$

Thetanullwerte of characteristic $(\varepsilon, \eta) \in \{0,1\}^g \times \{0,1\}^g$:

$$\theta\begin{bmatrix}\varepsilon\\ \eta\end{bmatrix}(\tau) = \sum_{n\in\mathbb{Z}^g} \exp\left[i\pi(n+\frac{\varepsilon}{2}).\tau.(n+\frac{\varepsilon}{2})\right] \exp\left[i\pi\eta.(n+\frac{\varepsilon}{2})\right].$$

Even characteristics : $\varepsilon.\eta \equiv 0 \pmod 2$.

Theorem (Igusa-Ichikawa)

If $g \geq 3$, then

$$\widetilde{\chi}_h(\tau) = \frac{(-1)^{gh/2}}{2^{2g-1}(2^g-1)} \cdot \prod_{even} \theta\begin{bmatrix}\varepsilon\\ \eta\end{bmatrix}(\tau) \in \mathbf{R}_{g,h}(\mathbb{C}), \quad h = 2^{g-2}(2^g+1).$$

$$\chi_h((A,a)) = (2i\pi)^{gh} \frac{\widetilde{\chi}(\tau_a)}{(\det \Omega_2)^h} \cdot \omega^{\otimes h} \in \mathbf{S}_{g,h}(\mathbb{Z}).$$

Main result

Theorem (Lachaud-R.-Zykin)

Let $A = (A, a)/k$ be a p.p.a.t. defined over a field $k \subset \mathbb{C}$. Assume that a is indecomposable. Let $\omega \in \boldsymbol{\omega}_k[A]$.

1. $\chi_{18}((A, a)) = 0$ *if and only if* (A, a) *is hyperelliptic.*
2. *With the previous notation*

$$\chi_{18}((A, a), \omega) = \frac{(2\pi)^{54}}{2^{28}} \cdot \frac{\prod_{even} \theta \begin{bmatrix} \varepsilon \\ \eta \end{bmatrix} (\tau_a)}{\det(\Omega_2)^{18}}$$

is a square in k^* if and only if (A, a) is a non hyperelliptic Jacobian.

Quadratic character given on $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ by

$$\varepsilon(\sigma) = \frac{d^\sigma}{d}, \quad d = \sqrt{\chi_{18}((A, a), \omega)}$$

First ingredient of the proof : action of twists

Let $\phi : (A', a')/k \longrightarrow (A, a)/k$ be a $\overline{k}$-isomorphism of p.p.a.v.

First ingredient of the proof : action of twists

Let $\phi : (A', a')/k \longrightarrow (A, a)/k$ be a $\overline{k}$-isomorphism of p.p.a.v.
Let $\omega_1, \ldots, \omega_g \in \Omega^1_k[A]$, $\omega = \omega_1 \wedge \cdots \wedge \omega_g \in \boldsymbol{\omega}_k[A]$.

First ingredient of the proof : action of twists

Let $\phi : (A', a')/k \longrightarrow (A, a)/k$ be a $\overline{k}$-isomorphism of p.p.a.v.
Let $\omega_1, \ldots, \omega_g \in \Omega^1_k[A]$, $\omega = \omega_1 \wedge \cdots \wedge \omega_g \in \boldsymbol{\omega}_k[A]$.
Let $\gamma_i = \phi^*(\omega_i)$ and $\gamma = \gamma_1 \wedge \cdots \wedge \gamma_g \in \boldsymbol{\omega}_{\overline{k}}[A']$.

First ingredient of the proof : action of twists

Let $\phi : (A', a')/k \longrightarrow (A, a)/k$ be a $\overline{k}$-isomorphism of p.p.a.v.
Let $\omega_1, \ldots, \omega_g \in \Omega^1_k[A]$, $\omega = \omega_1 \wedge \cdots \wedge \omega_g \in \boldsymbol{\omega}_k[A]$.
Let $\gamma_i = \phi^*(\omega_i)$ and $\gamma = \gamma_1 \wedge \cdots \wedge \gamma_g \in \boldsymbol{\omega}_{\overline{k}}[A']$.
Let $\omega'_1, \ldots, \omega'_g \in \Omega^1_k[A']$ and $\omega' = \omega'_1 \wedge \cdots \wedge \omega'_g$.
Let $M_\phi \in \mathrm{GL}_g(\overline{k})$ the matrix of the basis (γ_i) in the basis (ω'_i).

First ingredient of the proof : action of twists

Let $\phi : (A', a')/k \longrightarrow (A, a)/k$ be a $\overline{k}$-isomorphism of p.p.a.v.
Let $\omega_1, \ldots, \omega_g \in \Omega^1_k[A]$, $\omega = \omega_1 \wedge \cdots \wedge \omega_g \in \boldsymbol{\omega}_k[A]$.
Let $\gamma_i = \phi^*(\omega_i)$ and $\gamma = \gamma_1 \wedge \cdots \wedge \gamma_g \in \boldsymbol{\omega}_{\overline{k}}[A']$.
Let $\omega'_1, \ldots, \omega'_g \in \Omega^1_k[A']$ and $\omega' = \omega'_1 \wedge \cdots \wedge \omega'_g$.
Let $M_\phi \in \mathrm{GL}_g(\overline{k})$ the matrix of the basis (γ_i) in the basis (ω'_i).

Proposition

$$f \in \mathbf{S}_{g,h}(k), \quad f((A, a), \omega) = \det(M_\phi)^h \cdot f((A', a'), \omega').$$

Assume g odd, h even and $\mathrm{char}\, k \neq 2$. *Let $f \in \mathbf{S}_{g,h}(k)$ and $\phi : A' \longrightarrow A$ a non trivial quadratic twist. There exists $c \in k \setminus k^2$ such that*

$$f((A, a), \omega) \equiv c^{h/2} \cdot f((A, a), \omega') \pmod{k^{*h}}.$$

Second ingredient : Teichmüller modular forms

M_g : moduli stack of smooth and proper curves of genus g

$$\pi : \mathsf{C}_g \longrightarrow \mathsf{M}_g \quad \text{(universal curve)}$$

Ω^1 : rank g bundle induced by relative regular differential forms on $\mathsf{C}_g/\mathsf{M}_g$.
Relative canonical line bundle $\boldsymbol{\lambda}_{\mathsf{C}_g/\mathsf{M}_g} = \bigwedge^g \pi_* \Omega_1$ over M_g :

$$\begin{array}{c} \boldsymbol{\lambda}_{\mathsf{C}_g/\mathsf{M}_g} \\ \downarrow \\ \mathsf{M}_g \end{array} \qquad \Omega^1_k[X] = H^0(X, \Omega^1_X \otimes k), \quad \boldsymbol{\lambda}_k[X] = \bigwedge^g \Omega^1_k[X].$$

Space of Teichmüller modular forms over R, genus g, weight h :

$$\mathbf{T}_{g,h}(R) = \Gamma(\mathsf{M}_g \otimes R, \boldsymbol{\lambda}^{\otimes h}).$$

As for Siegel modular forms, we define

$$f(X,\lambda) = f(X)/\lambda^{\otimes h} \in k$$

if $f \in \mathbf{T}_{g,h}(k)$ and λ is a basis of $\boldsymbol{\lambda}_k[X]$.

The Torelli map $\theta : \mathrm{M}_g \longrightarrow \mathrm{A}_g$ satisfies $\theta^*\boldsymbol{\omega} = \boldsymbol{\lambda}$, and induces a linear map

$$\theta^* : \mathbf{S}_{g,h}(k) \longrightarrow \mathbf{T}_{g,h}(k)$$

such that $f((\mathrm{Jac}\, X, j), \omega) = [\theta^* f](X, \theta^*\omega)$.

Theorem (Ichikawa)

There exists $\mu_{h/2} \in \mathbf{T}_{g,h/2}(\mathbb{Z})$ such that $\theta^*(\chi_h) = \mu_{h/2}^2$.

The proof

Argument 2 implies that for any X/k in M_g :

$$\chi_{18}((\operatorname{Jac} X, j), \omega) = \mu_9(X, \theta^*\omega)^2 \in k.$$

The proof

Argument 2 implies that for any X/k in M_g :

$$\chi_{18}((\operatorname{Jac} X, j), \omega) = \mu_9(X, \theta^*\omega)^2 \in k.$$

Argument 1 implies that there is a $c \in k \setminus k^2$ and

$$\chi_{18}((\operatorname{Jac} X, j)_\varepsilon, \omega') \equiv c^9 \cdot \chi_{18}(\operatorname{Jac} X, j), \omega) \equiv c^9 \cdot \mu_9(X, \theta^*\omega)^2 \pmod{k^{*18}}$$

is not a square. □

The proof

Argument 2 implies that for any X/k in M_g :

$$\chi_{18}((\operatorname{Jac} X, j), \omega) = \mu_9(X, \theta^*\omega)^2 \in k.$$

Argument 1 implies that there is a $c \in k \setminus k^2$ and

$$\chi_{18}((\operatorname{Jac} X, j)_\varepsilon, \omega') \equiv c^9 \cdot \chi_{18}(\operatorname{Jac} X, j), \omega) \equiv c^9 \cdot \mu_9(X, \theta^*\omega)^2 \pmod{k^{*18}}$$

is not a square. □

By-products :

1. Klein's formula : $\mu_9 = \pm \operatorname{Disc}$;

The proof

Argument 2 implies that for any X/k in M_g :

$$\chi_{18}((\operatorname{Jac} X, j), \omega) = \mu_9(X, \theta^*\omega)^2 \in k.$$

Argument 1 implies that there is a $c \in k \setminus k^2$ and

$$\chi_{18}((\operatorname{Jac} X, j)_\varepsilon, \omega') \equiv c^9 \cdot \chi_{18}(\operatorname{Jac} X, j), \omega) \equiv c^9 \cdot \mu_9(X, \theta^*\omega)^2 \pmod{k^{*18}}$$

is not a square. □

By-products :

1. Klein's formula : $\mu_9 = \pm \operatorname{Disc}$;
2. Beyond genus 3
   - cannot work for g even ;
   - need to find forms of weight h such that $h/2$ is odd ;
   - cannot take χ_h (because it is only a square and not more) ;
   - but another Klein's formula for a genus 4 curve X

$$\frac{\widetilde{\chi}_{68}(\tau_a)}{\det(\Omega_2)^{68}} = c \cdot \Delta(X)^2 \cdot T(X)^8.$$

The proof

Argument 2 implies that for any X/k in M_g :

$$\chi_{18}((\operatorname{Jac} X, j), \omega) = \mu_9(X, \theta^*\omega)^2 \in k.$$

Argument 1 implies that there is a $c \in k \setminus k^2$ and

$$\chi_{18}((\operatorname{Jac} X, j)_\varepsilon, \omega') \equiv c^9 \cdot \chi_{18}(\operatorname{Jac} X, j), \omega) \equiv c^9 \cdot \mu_9(X, \theta^*\omega)^2 \pmod{k^{*18}}$$

is not a square. □

By-products :

1. Klein's formula : $\mu_9 = \pm \operatorname{Disc}$;
2. Beyond genus 3
   - cannot work for g even ;
   - need to find forms of weight h such that $h/2$ is odd ;
   - cannot take χ_h (because it is only a square and not more) ;
   - but another Klein's formula for a genus 4 curve X

$$\frac{\widetilde{\chi}_{68}(\tau_a)}{\det(\Omega_2)^{68}} = c \cdot \Delta(X)^2 \cdot T(X)^8.$$

3. Still works over finite fields of char $\neq 2$ ...

. . . but how to compute it ? An example

R. 09 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \mathrm{Jac}\, C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-19})/2$.

. . . but how to compute it ? An example

R. 09 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \mathrm{Jac}\, C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-19})/2$.
- $Cl(\mathcal{O}) = 1 \Rightarrow A = E^3$.

. . . but how to compute it ? An example

R. 09 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \mathrm{Jac}\, C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-19})/2$.
- $Cl(\mathcal{O}) = 1 \Rightarrow A = E^3$.
- a_0 the product polarization on A :

$$\{a \text{ p.p. on } A\} \longleftrightarrow \{M = a_0^{-1} a \in M_3(\mathcal{O}) \text{ positive definite hermitian of determinant } 1\}.$$

. . . but how to compute it ? An example

R. 09 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \mathrm{Jac}\, C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-19})/2$.
- $Cl(\mathcal{O}) = 1 \Rightarrow A = E^3$.
- a_0 the product polarization on A :

$$\{a \text{ p.p. on } A\} \longleftrightarrow \{M = a_0^{-1} a \in M_3(\mathcal{O}) \text{ positive definite hermitian of determinant } 1\}.$$

- classification by Schiemann of such matrices for some orders. There is only one in this case :

$$M = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\overline{\tau} & 3 \end{pmatrix}.$$

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$ w.r.t. wedge product of the pull back ω_0 of the differential $dx/(2y)$ on $\tilde{E}$:

$$c_1(a_0 M) = \frac{1}{\mathrm{Im}(\omega_1 \overline{\omega_2})}\, {}^t M$$

where $[\omega_1, \omega_2]$ is a period matrix of $\tilde{E}$ w.r.t. $dx/(2y)$;

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$ w.r.t. wedge product of the pull back ω_0 of the differential $dx/(2y)$ on $\tilde{E}$:

$$c_1(a_0 M) = \frac{1}{\mathrm{Im}(\omega_1 \overline{\omega_2})}\, {}^t M$$

  where $[\omega_1, \omega_2]$ is a period matrix of $\tilde{E}$ w.r.t. $dx/(2y)$;
- compute an analytic approximation of

$$\chi_{18}((\tilde{E}^3, a_0 M), \omega_0) = (2^{19} \cdot 19^7)^2;$$

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$ w.r.t. wedge product of the pull back ω_0 of the differential $dx/(2y)$ on $\tilde{E}$:

$$c_1(a_0 M) = \frac{1}{\mathrm{Im}(\omega_1 \overline{\omega_2})}{}^t M$$

where $[\omega_1, \omega_2]$ is a period matrix of $\tilde{E}$ w.r.t. $dx/(2y)$;

- compute an analytic approximation of

$$\chi_{18}((\tilde{E}^3, a_0 M), \omega_0) = (2^{19} \cdot 19^7)^2;$$

- since it is a square (over $\mathbb{F}_{47}$), such an optimal curve C exists.

Guàrdia (09) :

$$\tilde{C} : x^4 + (1/9)y^4 + (2/3)x^2y^2 - 190y^2 - 570x^2 + (152/9)y^3 - 152x^2y = 1083.$$

Values of $\chi = \chi_{18}((\tilde{E}^3, a_0 M), \omega_0)$

$\tilde{E}$: Gross' models with discriminant d^3 (when class number is 1).

d	M, $\tau = (1+\sqrt{d})/2$	χ	$\#\,\mathrm{Aut}(\tilde{E}^3, a)$
-7	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & \overline{\tau} \\ 1 & \tau & 2 \end{pmatrix}$	$(7^7)^2$	$2 \cdot 168$
-19	$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\overline{\tau} & 3 \end{pmatrix}$	$(2^5 \cdot 19^7)^2 \cdot (-2)$	$2 \cdot 6$
-43	$\begin{pmatrix} 3 & 1 & 1-\overline{\tau} \\ 1 & 4 & 2 \\ 1-\tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 43^7)^2 \cdot (-47 \cdot 79 \cdot 107 \cdot 173)$	$2 \cdot 1$
-163	$\begin{pmatrix} 2 & 1 & -\overline{\tau} \\ 1 & 2 & 1-\overline{\tau} \\ -\tau & 1-\tau & 28 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 11^4 \cdot 163^7)^2 \cdot (-2 \cdot 7 \cdot 11 \cdot 19 \cdot 127)$	$2 \cdot 6$
-15	$\begin{pmatrix} 2 & -1 & -1+\overline{\tau} \\ -1 & 2 & 1-\overline{\tau} \\ -1+\tau & 1-\tau & 3 \end{pmatrix}$	$2276909529982214234056917164577172629 9/4+$ $10182522603020834484863085151244322675 \cdot \sqrt{5}/4+$ $44626409093538218819956956474294768 69 \cdot \sqrt{-15}/4$ $+997833061792288644382398275511420244 5 \cdot \sqrt{-3}$	$2 \cdot 24$

Values of $\chi = \chi_{18}((\tilde{E}^3, a_0 M), \omega_0)$

$\tilde{E}$: Gross' models with discriminant d^3 (when class number is 1).

d	M, $\tau = (1+\sqrt{d})/2$	χ	$\#\,\mathrm{Aut}(\tilde{E}^3, a)$
-7	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & \overline{\tau} \\ 1 & \tau & 2 \end{pmatrix}$	$(7^7)^2$	$2 \cdot 168$
-19	$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\overline{\tau} & 3 \end{pmatrix}$	$(2^5 \cdot 19^7)^2 \cdot (-2)$	$2 \cdot 6$
-43	$\begin{pmatrix} 3 & 1 & 1-\overline{\tau} \\ 1 & 4 & 2 \\ 1-\tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 43^7)^2 \cdot (-47 \cdot 79 \cdot 107 \cdot 173)$	$2 \cdot 1$
-163	$\begin{pmatrix} 2 & 1 & -\overline{\tau} \\ 1 & 2 & 1-\overline{\tau} \\ -\tau & 1-\tau & 28 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 11^4 \cdot 163^7)^2 \cdot (-2 \cdot 7 \cdot 11 \cdot 19 \cdot 127)$	$2 \cdot 6$
-15	$\begin{pmatrix} 2 & -1 & -1+\overline{\tau} \\ -1 & 2 & 1-\overline{\tau} \\ -1+\tau & 1-\tau & 3 \end{pmatrix}$	$2276909529982214234056917164577172629 9/4+$ $10182522603020834484863085151244322675 \cdot \sqrt{5}/4+$ $44626409093538218819956956474294768 69 \cdot \sqrt{-15}/4$ $+99783306179228864438239827551142024 45 \cdot \sqrt{-3}$	$2 \cdot 24$

Consequences :

$d = -19$: defect 0 curve for $q = 47, 61, 137, 277$ (see Top, Alekseenko et al.).

$d = -67$: defect 0 curve for $q = 23^3$.

Geometric interpretation of $\widetilde{\chi}_{18}$

Two remarkable geometric forms defined from even Thetanullwerte :
— the product $\widetilde{\chi}_{18}$ (0 iff at least one Thetanullwerte is 0) ;
— the 35^{th} symmetric function $\widetilde{\Sigma}_{140}$ of the 8^{th} powers (0 if two Thetanullwerte are 0).

Geometric interpretation of $\widetilde{\chi}_{18}$

Two remarkable geometric forms defined from even Thetanullwerte :
— the product $\widetilde{\chi}_{18}$ (0 iff at least one Thetanullwerte is 0) ;
— the 35^{th} symmetric function $\widetilde{\Sigma}_{140}$ of the 8^{th} powers (0 if two Thetanullwerte are 0).

Theorem (Igusa)

Let $(A, a) \simeq \mathbb{C}^3/\tau_a\mathbb{Z}^3 + \mathbb{Z}^3 \in \mathsf{A}_3(\mathbb{C})$.

1. (A, a) *is decomposable if and only if* $\widetilde{\chi}_{18}(\tau_a) = \widetilde{\Sigma}_{140}(\tau_a) = 0$.
2. (A, a) *is a hyperelliptic Jacobian if and only if*

$$\widetilde{\chi}_{18}(\tau_a) = 0 \quad \textit{and} \quad \widetilde{\Sigma}_{140}(\tau_a) \neq 0.$$

3. (A, a) *is a non hyperelliptic Jacobian if and only if* $\widetilde{\chi}_{18}(\tau_a) \neq 0$. □

An arithmetic version

Proposition (Ichikawa)

χ_{18} is primitive (i.e. it is not zero modulo any prime).

We need a similar result for $\widetilde{\Sigma}_{140}$.

An arithmetic version

Proposition (Ichikawa)

χ_{18} is primitive (i.e. it is not zero modulo any prime).

We need a similar result for $\widetilde{\Sigma}_{140}$.

Proposition

$$\Sigma_{140} = \frac{(2i\pi)^{140}}{2^{218}} \cdot \frac{\widetilde{\Sigma}_{140}(\tau_a)}{\det(\Omega_2)^{140}} (\omega_1 \wedge \omega_2 \wedge \omega_3)^{\otimes 140}$$

is a primitive Siegel modular form of weight 140 over $\mathbb{Z}$.

An arithmetic version

Proposition (Ichikawa)

χ_{18} is primitive (i.e. it is not zero modulo any prime).

We need a similar result for $\widetilde{\Sigma}_{140}$.

Proposition

$$\Sigma_{140} = \frac{(2i\pi)^{140}}{2^{218}} \cdot \frac{\widetilde{\Sigma}_{140}(\tau_a)}{\det(\Omega_2)^{140}} (\omega_1 \wedge \omega_2 \wedge \omega_3)^{\otimes 140}$$

is a primitive Siegel modular form of weight 140 *over* $\mathbb{Z}$.

Conjecture : if $\chi_{18}((A,a)) = \Sigma_{140}((A,a)) = 0$ then (A,a) is decomposable.

Corollary : if the conjecture holds then Igusa's theorem is valid over finite fields as well.

Basic results

Mestre's observation : if $12|\#Aut(\tilde{E}^3, a)$ then the primes which divide χ are the prime factors of $j(\tilde{E}) - 1728$ apart from 3.

Basic results

Mestre's observation : if $12|\#Aut(\tilde{E}^3, a)$ then the primes which divide χ are the prime factors of $j(\tilde{E}) - 1728$ apart from 3.

Let $(A, a) = (\tilde{E}^3, a)$ with a indecomposable defined over a local ring S of a number field with residue field $\mathbb{F}$ at a prime $\mathfrak{p}$.

Proposition ? : Assume that $\tilde{E}$ has CM by $\mathcal{O}$ maximal and $\tilde{E} \otimes \mathbb{F}$ is smooth. If $(A, a) \otimes \mathbb{F}$ is decomposable then $\tilde{E} \otimes \mathbb{F}$ is supersingular.
The converse is true if $\mathrm{char}\, \mathbb{F} = 2$. In particular $\mathfrak{p}|\chi$.

Basic results

Mestre's observation : if $12|\#Aut(\tilde{E}^3, a)$ then the primes which divide χ are the prime factors of $j(\tilde{E}) - 1728$ apart from 3.

Let $(A, a) = (\tilde{E}^3, a)$ with a indecomposable defined over a local ring S of a number field with residue field $\mathbb{F}$ at a prime $\mathfrak{p}$.

Proposition ? : Assume that $\tilde{E}$ has CM by $\mathcal{O}$ maximal and $\tilde{E} \otimes \mathbb{F}$ is smooth. If $(A, a) \otimes \mathbb{F}$ is decomposable then $\tilde{E} \otimes \mathbb{F}$ is supersingular.
The converse is true if $\mathrm{char}\, \mathbb{F} = 2$. In particular $\mathfrak{p}|\chi$.

Question : how to detect hyperelliptic reduction ?

$d = -15$:

$\sqrt{-3}$	$\sqrt{5}$	results over $\mathbb{F}_{19^3}$
-4	9	a defect 3 non hyperelliptic curve
-4	-9	a defect 3 non hyperelliptic curve
4	-9	a minimal defect 3 non hyperelliptic curve
4	9	a hyperelliptic curve

To move out from the border by isogeny

Let k be an arbitrary field of characteristic not 2.
$E/k : y^2 = x(x-\alpha)(x-\beta)$ an elliptic curve and $A = E^3/W$ where $W \subset E^3[2]$ is a certain isotropic subgroup.

To move out from the border by isogeny

Let k be an arbitrary field of characteristic not 2.
$E/k : y^2 = x(x-\alpha)(x-\beta)$ an elliptic curve and $A = E^3/W$ where $W \subset E^3[2]$ is a certain isotropic subgroup.
Let a_0 be the product polarization on E^3 and a be the descent indecomposable p.p. on A from $2a_0$.

Theorem (simplest case of Howe-Leprevost-Poonen (2002))

(A, a) is a Jacobian if and only if $3\alpha + \beta \in k^2$.

To move out from the border by isogeny

Let k be an arbitrary field of characteristic not 2.
$E/k : y^2 = x(x-\alpha)(x-\beta)$ an elliptic curve and $A = E^3/W$ where $W \subset E^3[2]$ is a certain isotropic subgroup.
Let a_0 be the product polarization on E^3 and a be the descent indecomposable p.p. on A from $2a_0$.

Theorem (simplest case of Howe-Leprevost-Poonen (2002))

(A, a) is a Jacobian if and only if $3\alpha + \beta \in k^2$.

Question : can we say something about this value a priori ?

To move out from the border by isogeny

Let k be an arbitrary field of characteristic not 2.
$E/k : y^2 = x(x-\alpha)(x-\beta)$ an elliptic curve and $A = E^3/W$ where $W \subset E^3[2]$ is a certain isotropic subgroup.
Let a_0 be the product polarization on E^3 and a be the descent indecomposable p.p. on A from $2a_0$.

Theorem (simplest case of Howe-Leprevost-Poonen (2002))

(A, a) is a Jacobian if and only if $3\alpha + \beta \in k^2$.

Question : can we say something about this value a priori ?

In the same spirit, when $k = \mathbb{F}_{2^n}$.

Theorem (Nart-R. (2008 and 2009))

If $n > 5$ is even then there is always a maximal curve ;
If n is odd and $\lfloor 2\sqrt{2^n} \rfloor \equiv 1, 5, 7 \pmod 8$ there is always a maximal curve.

To move out from the border by change of polarization

Can we algebraically link the Thetanullwerte on A corresponding to two non isomorphic principal polarizations ?

Thank you for your attention !