

Smaller class invariants for constructing curves of genus 2

Marco Streng



The 15th workshop on Elliptic Curve Cryptography
ECC 2011
INRIA, Nancy, France
Sep 19 21, 2011

Overview

	genus 1	genus 2
constructing curves	part 1	part 2
smaller class invariants	part 3	part 4

Part 1: The Hilbert class polynomial

Definition: The *j-invariant* is

$$j(E) = \frac{2^8 3^3 b^3}{2^2 b^3 + 3^3 c^2} \quad \text{for } E : y^2 = x^3 + bx + c.$$

Fact: $j(E) = j(F) \iff E \cong_k F$

Definition: Let K be an imaginary quadratic number field. Its *Hilbert class polynomial* is

$$H_K = \prod_{\substack{E/\mathbf{C} \\ \text{End}(E) \cong \mathcal{O}_K}} (X - j(E)) \in \mathbf{Z}[X].$$

Application 1: roots generate Hilbert class field of K

Application 2: elliptic curves of prescribed order

Elliptic curves of prescribed order

Algorithm: (given $\pi \in \mathcal{O}_K$ imag. quadr. with $p = \pi\bar{\pi}$ prime)

1. Compute $H_K \bmod p$, it splits into linear factors.
2. Let $j^0 \in \mathbf{F}_p$ be a root and let E^0/\mathbf{F}_p have $j(E^0) = j^0$.
3. Select the twist E of E^0 with “Frob = π ”. It satisfies

$$\#E(\mathbf{F}_p) = N(\pi - 1) = p + 1 - \text{tr}(\pi).$$

By choosing K and p well, get elliptic curves for cryptography, even for pairing based cryptography.

The size

- ▶ The Hilbert class polynomial of $K = \mathbf{Q}(\sqrt{-71})$ is

$$\begin{aligned} & X^7 + 313645809715X^6 - 3091990138604570X^5 \\ & + 98394038810047812049302X^4 \\ & - 823534263439730779968091389X^3 \\ & + 5138800366453976780323726329446X^2 \\ & - 425319473946139603274605151187659X \\ & + 737707086760731113357714241006081263. \end{aligned}$$

- ▶ Weber (around 1900) replaces this by

$$X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X - 1.$$

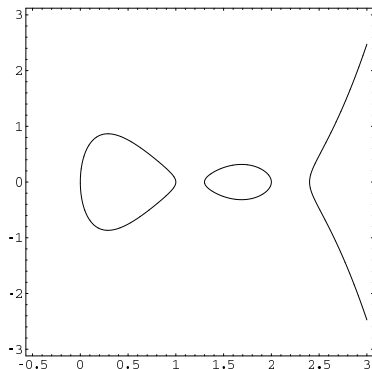
Part 2: curves of genus 2

“Definition” (char. $\neq 2$):

A curve of genus 2 is

$$y^2 = f(x), \quad \deg(f) \in \{5, 6\},$$

where f has no double roots.



Igusa invariants

Igusa gave a **genus-2 analogue** of the j -invariant,

- ▶ i.e., a model for the moduli space of genus-2 curves.
- ▶ Mestre's algorithm (available in Magma and soon in Sage) constructs an equation for the curve from its invariants.
- ▶ Generically, it suffices to use a triple of *absolute Igusa invariants* $i_1, i_2, i_3 \in \mathbf{Q}(\mathcal{M}_2)$.
- ▶ See my preprint "Computing Igusa class polynomials" arXiv:0903.4766 for the "best" triple.

Complex multiplication

Abelian varieties:

- ▶ An elliptic curve is a 1-dim. ab. var.
- ▶ The *Jacobian* of a genus-2 curve is a 2-dim. ab. var.

CM-fields:

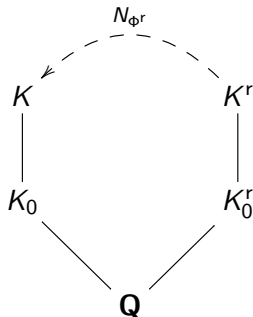
- ▶ A *CM-field* is a field $K = K_0(\sqrt{r})$ with K_0 a totally real number field and $r \in K_0$ totally negative.
- ▶ Let A/\mathbf{C} be a g -dim. ab. var. We say that A has *CM* if $\mathcal{O} = \text{End}(A)$ is an order in a CM-field K of degree $2g$.

Examples:

- ▶ $g = 1$, $K_0 = \mathbf{Q}$, K imaginary quadratic
- ▶ $g = 2$, K_0 is real quadratic, $K = \mathbf{Q}[X]/(X^4 + AX^2 + B)$

CM-types

- ▶ To every CM abelian variety, we associate a *CM type* Φ .
- ▶ To Φ , we associate the *reflex field* K^r and *reflex type norm*



- ▶ If $\deg K = 2$, then $N_{\Phi^r} : K \rightarrow K^r$ is an isomorphism, so we don't talk about it.

Igusa class polynomials

Preliminary definition:

Let K be a CM field of degree 4. Its Igusa class polynomials are

$$H_{i_1} = \prod_C (X - i_1(C)) \in \mathbf{Q}[X]$$

$$H_{i_1, i_n} = \sum_C i_n(C) \prod_{D \neq C} (X - i_1(D)) \in \mathbf{Q}[X] \quad (n \in \{2, 3\})$$

with products and sums taken over all isom. classes of C/\mathbf{C} with CM by \mathcal{O}_K .

Assume: (simplicity only, and true in practice) H_{i_1} no double roots.

$$\text{Then } H_{i_1}(i_1(C)) = 0 \quad \text{and} \quad i_n(C) = \frac{H_{i_1, i_n}(i_1(C))}{H'_{i_1}(i_1(C))}.$$

Igusa class polynomials

Definition:

Let K be a CM field of degree 4. Its Igusa class polynomials are

$$H_{i_1} = \prod_C (X - i_1(C)) \in K_0'[X]$$

$$H_{i_1, i_n} = \sum_C i_n(C) \prod_{D \neq C} (X - i_1(D)) \in K_0'[X] \quad (n \in \{2, 3\})$$

with products and sums taken over
isom. classes of C/\mathbf{C} with CM by \mathcal{O}_K of a given CM-type Φ .

Assume: (simplicity only, and true in practice) H_{i_1} no double roots.

$$\text{Then } H_{i_1}(i_1(C)) = 0 \quad \text{and} \quad i_n(C) = \frac{H_{i_1, i_n}(i_1(C))}{H'_{i_1}(i_1(C))}.$$

Igusa class polynomials

Definition:

Let K be a CM field of degree 4. Its Igusa class polynomials are

$$H_{i_1} = \prod_C (X - i_1(C)) \in K_0^r[X]$$

$$H_{i_1, i_n} = \sum_C i_n(C) \prod_{D \neq C} (X - i_1(D)) \in K_0^r[X] \quad (n \in \{2, 3\})$$

with products and sums taken over *one* $\text{Gal}(\overline{K^r}/K^r)$ -orbit of isom. classes of C/\mathbf{C} with CM by \mathcal{O}_K *of a given CM-type* Φ .

Assume: (simplicity only, and true in practice) H_{i_1} no double roots.

$$\text{Then } H_{i_1}(i_1(C)) = 0 \quad \text{and} \quad i_n(C) = \frac{H_{i_1, i_n}(i_1(C))}{H'_{i_1}(i_1(C))}.$$

Example

$$K = \mathbf{Q}(\sqrt{-14 + 2\sqrt{5}}), \quad \omega = \sqrt{11}, \quad K^r = \mathbf{Q}(\sqrt{-7 + 2\omega})$$

$$H_{i_1} = y^4 - 16906968y^3 + 54245326531032y^2 \\ + 6990615303516000y - 494251688841750000$$

$$7^4 H_{i_1, i_2} = 1181176456752y^3 - 6134558308934655456y^2 \\ - 1236449605135697928000y \\ + 79084224228190734000000$$

$$7^4 H_{i_1, i_3} = 1782128620567774368y^3 \\ - 9232752428041223776093632y^2 \\ - 1189728258050864079984816000y \\ + 84118511880173912009148000000$$

Example

$$K = \mathbf{Q}(\sqrt{-14 + 2\sqrt{5}}), \quad \omega = \sqrt{11}, \quad K^r = \mathbf{Q}(\sqrt{-7 + 2\omega})$$

$$H_{i_1} = y^2 + (1250964\omega - 8453484)y \\ + 374134464\omega - 1022492484$$

$$7^4 H_{i_1, i_2} = (-139899783096\omega + 590588228376)y \\ - 45253281038112\omega \\ + 143469827584272$$

$$7^4 H_{i_1, i_3} = (-211915358558075664\omega \\ + 891064310283887184)y \\ - 44591718318414329664\omega \\ + 138345299573665361184$$

Genus-2 curves with prescribed Frobenius

Fix a CM-type Φ and let H_{i_1} be Igusa class polynomials for Φ .

Algorithm: (given $\pi \in \mathcal{O}_K$ quartic CM with $p = \pi\bar{\pi}$ prime)

1. write $(\pi) = N_{\Phi^r}(\mathfrak{P})$ for some $\mathfrak{P} \subset \mathcal{O}_{K^r}$
2. compute $(H_{i_1} \bmod \mathfrak{P})$, which splits into linear factors over \mathbf{F}_p
3. let i_1^0 be a root, let

$$i_n^0 = \frac{H_{i_1, i_n}(i_1^0)}{H'_{i_1}(i_1^0)}, \quad \text{and let } i_n(C^0) = i_n^0;$$

then a twist C of C^0 has “Frob = π ”. It satisfies

$$\#J(C)(\mathbf{F}_p) = N(\pi - 1) \quad \text{and} \quad \#C(\mathbf{F}_p) = p + 1 - \text{tr}(\pi).$$

Note: with our definitions, any root i_1^0 is ok (instead of only half of them).

Part 3: back to genus 1

Over \mathbf{C} , every elliptic curve is \mathbf{C}/Λ .

By choosing a \mathbf{Z} -basis of Λ (and scaling \mathbf{C}), get

$\Lambda = \tau\mathbf{Z} + \mathbf{Z}$, $\text{Im } \tau > 0$.

Compute H_K numerically as

$$H_K = \prod_{\substack{\tau \text{ with CM by } \mathcal{O}_K \\ \text{up to change of basis}}} (X - j(\tau)) \in \mathbf{Z}[X]$$

- ▶ j is a function of τ , invariant under all changes of bases.
- ▶ Weber: get smaller polynomial by replacing j by a “smaller” modular function f .
- ▶ f is invariant only under *some* changes of bases, so something needs to be done.

Modular forms

Definition:

- ▶ Let $\mathcal{H} = \{\tau \in \mathbf{C} : \text{Im } \tau > 0\}$.
- ▶ For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbf{Z})$, let $A\tau = \frac{a\tau+b}{c\tau+d}$.
- ▶ A *modular form* of weight k and level N is a holomorphic map $f : \mathcal{H} \rightarrow \mathbf{C}$ satisfying

$$f(A\tau) = (c\tau + d)^k f(\tau)$$

for all $A \in \text{SL}_2(\mathbf{Z})$ with $A \equiv 1 \pmod{N}$,
and a convergence condition at the cusps.

- ▶ It has a *q-expansion* $f(\tau) = \sum_{n=0}^{\infty} a_n q^{n/N}$ with $q = e^{2\pi i\tau}$.

Example: $\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$ for $N = 24, k = 1/2$

Modular functions

Definition:

Let $\mathcal{F}_N = \left\{ \begin{array}{l} g_1 \\ g_2 \end{array} : \begin{array}{l} g_i \text{ of level } N \text{ and of equal weight, with} \\ q\text{-expansion coefficients in } \mathbf{Q}(\zeta_N) \end{array} \right\}$

- ▶ recall $g_i(A\tau) = (c\tau + d)^k g_i(\tau)$ if $A \equiv 1 \pmod{N}$
- ▶ so $f(A\tau) = f(\tau)$ if $f \in \mathcal{F}_N$ and $A \equiv 1 \pmod{N}$

Fact:

Action of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ on \mathcal{F}_N by $f^A(\tau) := f(A\tau)$

Examples:

- ▶ $\mathcal{F}_1 = \mathbf{Q}(j)$
- ▶ Weber used $f(z) = \zeta_{48}^{-1} \frac{\eta(\frac{z+1}{2})}{\eta(z)} \in \mathcal{F}_{48}$, where $\zeta_{48} = e^{2\pi i/48}$.

Galois groups of modular functions

Actions:

- ▶ $SL_2(\mathbf{Z}/N\mathbf{Z})$ acts on \mathcal{F}_N by $f^A(\tau) := f(A\tau)$
- ▶ $\text{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) = (\mathbf{Z}/N\mathbf{Z})^*$ acts on \mathcal{F}_N by acting on the q -expansion coefficients: $v : \zeta_N \mapsto \zeta_N^v$
- ▶ Let $(\mathbf{Z}/N\mathbf{Z})^* \subset GL_2(\mathbf{Z}/N\mathbf{Z})$ via $v \mapsto \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix}$.

Note:

Given $A \in GL_2(\mathbf{Z}/N\mathbf{Z})$, let $v = \det(A)$. Then $A = \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix} \left[\begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix}^{-1} A \right]$.

Fact:

$$\text{Gal}(\mathcal{F}_N/\mathcal{F}_1) = GL_2(\mathbf{Z}/N\mathbf{Z})/\{\pm 1\}$$

Class invariants

- ▶ Let $\mathcal{H}_1 = K(j(\tau))$, where $\mathbf{Z}\tau + \mathbf{Z}$ has CM by \mathcal{O}_K .
- ▶ \mathcal{H}_1 is the *Hilbert class field* of K .
- ▶ For $f \in \mathcal{F}_N$, we call $f(\tau)$ a *class invariant* if $K(f(\tau)) = \mathcal{H}_1$.

Examples:

- ▶ $j(\tau)$
- ▶ Weber: if $\text{disc}(K) \equiv 1, 17 \pmod{24}$, then $\exists \tau$ such that $f(\tau)$ is a class invariant

Galois groups of values of modular functions

- ▶ Let $\mathcal{H}_N = K(f(\tau) : f \in \mathcal{F}_N)$, where $\tau \mathbf{Z} + \mathbf{Z}$ has CM by \mathcal{O}_K .
- ▶ \mathcal{H}_N is the *ray class field of K mod N* .
- ▶ $\text{Gal}(\mathcal{H}_N/\mathcal{H}_1) = (\mathcal{O}_K/N\mathcal{O}_K)^*/\mathcal{O}_K^*$.

$$\begin{array}{ccc} \mathcal{F}_N - \frac{\tau}{N} \succcurlyeq \mathcal{H}_N & & \\ \text{GL}_2(\mathbf{Z}/N\mathbf{Z})/\pm 1 \Big| & & \Big| (\mathcal{O}_K/N\mathcal{O}_K)^*/\mathcal{O}_K^* \\ \mathbf{Q}(j) - \frac{\tau}{N} \succcurlyeq \mathcal{H}_1 & & \end{array}$$

Galois groups of values of modular functions

$$\begin{array}{ccc} \mathcal{F}_N - \frac{\tau}{N} \succ \mathcal{H}_N & & \\ \text{GL}_2(\mathbf{Z}/N\mathbf{Z})/\pm 1 \Big| & & \Big| (\mathcal{O}_K/N\mathcal{O}_K)^*/\mathcal{O}_K^* \\ \mathbf{Q}(j) - \frac{\tau}{N} \succ \mathcal{H}_1 & & \end{array}$$

Shimura's reciprocity law:

We have $f(\tau)^x = f^{g_\tau(x)}(\tau)$ for some map

$$g_\tau : (\mathcal{O}_K/N\mathcal{O}_K)^* \rightarrow \text{GL}_2(\mathbf{Z}/N\mathbf{Z})$$

Explicitly: $g_\tau(x)$ is the transpose of the matrix of multiplication by x w.r.t. the \mathbf{Q} -basis $\tau, 1$ of K

Note: If f is fixed under $g_\tau((\mathcal{O}_K/N\mathcal{O}_K)^*)$, then $f(\tau) \in \mathcal{H}_1$.

The minimal polynomial of a class invariant

The full version of Shimura's reciprocity law also gives the action of $G = \text{Gal}(\mathcal{H}_1/K)$ on $f(\tau) \in \mathcal{H}_1$.

This allows us to

- ▶ check if $f(\tau)$ is a class invariant, i.e., $K(f(\tau)) = \mathcal{H}_1$ (assume this is the case from now on),
- ▶ compute the minimal polynomial of $f(\tau)$ over K :

$$H_f = \prod_{x \in G} (X - f(\tau)^x) \in K[X]$$

In the CM method, go from $f^0 \in \mathbf{F}_p$ to $j^0 \in \mathbf{F}_p$ using a *modular polynomial*.

Part 4: class invariants for any $g \geq 1$

- ▶ For general principally polarized abelian varieties, have $A = \mathbf{C}^g / (\tau \mathbf{Z}^g + \mathbf{Z}^g)$ with τ in $\mathcal{H}_g = \{\tau \in \text{Mat}_g(\mathbf{C}) : \tau \text{ symmetric and } \text{Im } \tau > 0\}$
- ▶ Changes of bases correspond to the action of

$$\text{Sp}_{2g}(\mathbf{Z}) = \left\{ A \in \text{GL}_{2g}(\mathbf{Z}) : A^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\},$$

acting via $A\tau = (a\tau + b)(c\tau + d)^{-1}$ if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Example: $\text{Sp}_2 = \text{SL}_2$

Siegel modular forms

- ▶ A *(Siegel) modular form* of level N and weight k is a holomorphic $f : \mathcal{H}_g \rightarrow \mathbf{C}$ satisfying

$$f(A\tau) = \det(c\tau + d)^k f(\tau)$$

for all $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$ with $A \equiv 1 \pmod{N}$
(and a holomorphicity condition at the cusps if $g = 1$).

- ▶ Let $\mathcal{F}_N = \left\{ \begin{array}{l} g_1 \\ g_2 \end{array} : \begin{array}{l} g_i \text{ of level } N \text{ and of equal weight, with} \\ q\text{-expansion coefficients in } \mathbf{Q}(\zeta_N) \end{array} \right\}$
- ▶ $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ acts on \mathcal{F}_N via $f^A(\tau) := f(A\tau)$.

Example: For $g = 2$, we have $\mathcal{F}_1 = \mathbf{Q}(i_1, i_2, i_3)$.

Theta constants

Definition:

For $c_1, c_2 \in \mathbf{Q}^g$, the *theta constant* with characteristic c_1, c_2 is

$$\theta[c_1, c_2](\tau) = \sum_{v \in \mathbf{Z}^g} \exp(\pi i(v + c_1)\tau(v + c_1)^t + 2\pi i(v + c_1)c_2^t).$$

Explicit action:

Given $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$, there is a holomorphic $\rho = \rho_A : \mathcal{H}_g \rightarrow \mathbf{C}^*$ such that for all c_1, c_2 ,

$$\theta[c_1, c_2](A\tau) = \rho(\tau) \exp(2\pi i r) \theta[d_1, d_2](\tau),$$

where

$$\begin{pmatrix} d_1 \\ d_2 \end{pmatrix} = A^t \begin{pmatrix} c_1 - \frac{1}{2} \mathrm{diag}(cd^t) \\ c_2 - \frac{1}{2} \mathrm{diag}(ab^t) \end{pmatrix}, \quad \text{and}$$

$$r = \frac{1}{2} ((dd_1 - cd_2)^t(-bd_1 + ad_2 + \mathrm{diag}(ab^t)) - d_1^t d_2),$$

Theta constants

Conclusion:

$$\frac{\theta[c_1, c_2]}{\theta[c'_1, c'_2]} \in \mathcal{F}_{2D^2} \quad \text{if } D \in 2\mathbf{Z} \text{ and } Dc_1, Dc_2, Dc'_1, Dc'_2 \in \mathbf{Z}^g$$

Explicit action:

Given $A \in \text{Sp}_{2g}(\mathbf{Z}/2D^2\mathbf{Z})$, we have for all c_1, c_2, c'_1, c'_2 ,

$$\frac{\theta[c_1, c_2]}{\theta[c'_1, c'_2]}(A\tau) = \frac{\exp(2\pi ir)}{\exp(2\pi ir')} \frac{\theta[d_1, d_2]}{\theta[d'_1, d'_2]}(\tau),$$

where

$$\begin{pmatrix} d_1 \\ d_2 \end{pmatrix} = A^t \begin{pmatrix} c_1 - \frac{1}{2}\text{diag}(cd^t) \\ c_2 - \frac{1}{2}\text{diag}(ab^t) \end{pmatrix}, \quad \text{and}$$

$$r = \frac{1}{2}((dd_1 - cd_2)^t(-bd_1 + ad_2 + \text{diag}(ab^t)) - d_1^t d_2),$$

Galois groups of modular functions

Actions:

- ▶ $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ acts on \mathcal{F}_N by $f^A(\tau) := f(A\tau)$
- ▶ $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) = (\mathbf{Z}/N\mathbf{Z})^*$ acts on \mathcal{F}_N by acting on the coefficients of the q -expansion.
- ▶ Let $(\mathbf{Z}/N\mathbf{Z})^* \subset \mathrm{GL}_{2g}(\mathbf{Z}/N\mathbf{Z})$ via $v \mapsto \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix}$.

Together, these groups generate $\mathrm{GSp}_{2g}(\mathbf{Z}) \subset \mathrm{GL}_{2g}(\mathbf{Z})$.

Together, these actions induce an action of $\mathrm{GSp}_{2g}(\mathbf{Z})$ on \mathcal{F}_N .

The CM class fields for $g \geq 1$

The field $\mathcal{H}_1 := K^r(f(\tau) : f \in \mathcal{F}_1)$ is a *subfield* of the Hilbert class field of K^r .

The CM class fields for $g \geq 1$

The field $\mathcal{H}_N := K^r(f(\tau) : f \in \mathcal{F}_N)$ is a *subfield* of the ray class field mod N of K^r .

Class field theoretic description:

Let I_N be the group of fractional \mathcal{O}_{K^r} -ideals coprime to N , and let

$$H_N = \left\{ \mathfrak{a} \in I_N : \exists \mu \in K \text{ with } \begin{array}{l} N_{\Phi^r}(\mathfrak{a}) = (\mu) \\ \mu \bar{\mu} = N(\mathfrak{a}) \in \mathbf{Q} \\ \mu \equiv 1 \pmod{*N} \end{array} \right\}.$$

Then \mathcal{H}_N is the class field of K^r with Galois group I_N/H_N .

New: also a version for non-maximal orders!

Shimura's reciprocity law for any $g \geq 1$

$$\begin{array}{ccc} \mathcal{F}_N - \frac{\tau}{\gg} \mathcal{H}_N & & \\ \text{GSp}_{2g}(\mathbf{Z}/N\mathbf{Z})/\pm 1 \Big| & & \Big| \frac{(H_1 \cap I_N(K^r))}{H_N} \\ \mathcal{F}_1 - \frac{\tau}{\gg} \mathcal{H}_1 & & \end{array}$$

- ▶ My explicit version of Shimura's reciprocity law:

$$f(\tau)^{\mathfrak{a}} = f^{g(\mathfrak{a})}(\tau),$$

where $g(\mathfrak{a})$ is the transpose of the matrix of multiplication by $\mu \in K$, and μ is given by $(\mu) = N_{\Phi^r}(\mathfrak{a})$ and $\mu\bar{\mu} \in \mathbf{Q}$.

- ▶ Again, the full version also gives the action of $\text{Gal}(\mathcal{H}_1/K^r)$.

Example 1 (the first field that I tried)

For $c_1 = \frac{1}{2}(a, b)$, $c_2 = \frac{1}{2}(c, d)$, write $\theta_{c+2d+4a+8b} = \theta[c_1, c_2]$.

- ▶ The function

$$f = i \frac{\theta_{12}^6}{\theta_8^2 \theta_9^2 \theta_{15}^2} \in \mathcal{F}_8$$

is a class invariant for a certain τ for

$$K = [521, 27, 52] = \mathbf{Q}[X]/(X^4 + 27X^2 + 52).$$

For comparison:

$$i_1 = \frac{\text{hom. pol. of degree 20 in } \theta\text{'s}}{(\theta_0 \theta_1 \theta_2 \theta_3 \theta_4 \theta_6 \theta_8 \theta_9 \theta_{12} \theta_{15})^2}$$

Example 1 (the first field that I tried)

$$\text{without } f = i \frac{\theta_{12}^6}{\theta_8^2 \theta_9^2 \theta_{15}^2} \in \mathcal{F}_8$$

$$\begin{aligned} H_{i_1} = & 2 \cdot 101^2 y^7 + (-310410324232717295510\sqrt{13} \\ & + 1119200340441877774220)y^6 \\ & + (-304815375394920390351841501071188305100\sqrt{13} \\ & + 1099027465536189912517941272236385718800)y^5 \\ & + (-2201909580030523730272623848434538048317834513875\sqrt{13} \\ & + 7939097894735431844153019089320973153011210882125)y^4 \\ & + (-2094350525854786365698329174961782735189420898791141250\sqrt{13} \\ & + 7551288209764401665731458692859504138760400195691473750)y^3 \\ & + (-907392914800494855136752991106041311116404713247380607234375\sqrt{13} \\ & + 3271651681305911192688931423723753094763461200379169938284375)y^2 \\ & + (-30028332099313039720091760445942488226781301051810139974908125000\sqrt{13} \\ & + 108268691100734381571211968891173879786167063702810731956822125000)y \\ & + (-320854170291151322128777010521751890513120770505490537777676328984375\sqrt{13} \\ & + 1156856162931200670387093211443242850125709667683265459917987279296875) \end{aligned}$$

Example 1 (the first field that I tried)

with $f = i \frac{\theta_{12}^6}{\theta_8^2 \theta_9^2 \theta_{15}^2} \in \mathcal{F}_8$

$$\begin{aligned} H_f = & 3^8 101^2 y^7 + (21911488848 \sqrt{13} \\ & - 76603728240) y^6 \\ & + (-203318356742784 \sqrt{13} \\ & + 733099844294784) y^5 \\ & + (-280722122877358080 \sqrt{13} \\ & + 1012158088965439488) y^4 \\ & + (-2349120383562514432 \sqrt{13} \\ & + 8469874588158623744) y^3 \\ & + (-78591203121748770816 \sqrt{13} \\ & + 283364613421131104256) y^2 \\ & + (250917334141632512 \sqrt{13} \\ & - 904696010264018944) y \\ & + (-364471595827200 \sqrt{13} \\ & + 1312782658043904) \end{aligned}$$

Obtaining curves via interpolation

Modular polynomials for $g > 1$ would need

- ▶ solving of the modular polynomials (Groebner bases),
- ▶ having 3 alg. indep. modular functions to use for class invariants.

But we need just one class invariant $f(\tau)$ if we use

$$H_f = \prod_x (X - f(\tau)^x) \in K^r[X],$$

$$H_{f,i_n} = \sum_x i_n(\tau)^x \prod_{y \neq x} (X - f(\tau)^y) \in K^r[X] \quad (n \in \{1, 2, 3\}),$$

with products and sums taken over $x, y \in \text{Gal}(\mathcal{H}_1/K^r)$

Note:

The size of f plays the biggest role in the size of the polynomials.

Example 1 (continued)

Terminal — vim

```
20402xy^7 + (-318418324232717295510xw + 11920034044187774220)xy^6 + (-304815375394920390351841501071188305100xw + 1099027465536189912517941272236385718800)xy^5 + (-220919095800030523730272623848434538048317834513875xw + 793909789473543184415301980932097315011218882125)xy^4 + (-20943505258547863656983291749617827351894200898791141250xw + 7551288289764401665731458692859504138760400195691473750)xy^3 + (-907392914800494855136752991106041311116404713247380687234375xw + 3271651681305911296889314237237353094763461200379169938284375)xy^2 + (-30028332899313039720091760445942488226781301051810139974908125000xw + 108268691100734381571211968891737879786167063702810731956822125000)xy - 320854170291151322128777018952175189051312877505490537777676328984375xw + 1156856162931200670387093211443242850125709667683265459917987279296875  
(1048060401, (155942160719197448511497600xw - 562257456400820026589520000)xy^6 + (10915460249997911281051048769982462340880000xw - 39356251626656444452197645346830542580480000)xy^5 + (16837314627754982776274874332708320623750230856441200000xw - 6070700123149046224875881752742722561309748289200000)xy^4 + (2386524358008138594036975343648095732900253983810440818000000xw - 8604735943206219380903096450425313402473195975766590178000000)xy^3 + (104322262281490071026402121264030948196570781298335683612123780000000xw - 376139265828315347221671384362808264396213840032027706818473000000)xy^2 + (342297875984824099435381776597567613874765530287217882549834450000000xw - 12341725426738324424199494569900641042064837165414213925317002945000000)xy + 254448518301571719798504716559584579677190202948541991757945905090500000000xw - 9174271797021413695420921800929165552409449453935704933267034790000000000  
(1048060401, (-40129374358272356893172649634983059328000000xw + 144688516901840080323524823696416410496000000)xy^6 + (-1506913225655983606143240718922355336207754357058564640000000xw + 543325290277748600487298477762721832123795770308636000000000)xy^5 + (-1088556219655951950859335956510553063925800398625862826001713920000000xw + 392484526619476048638313800493740279776268138086785283572856420000000)xy^4 + (-103538233892861564314128927980153110010287160788676047819381245658252000000000xw + 37331241126881145175459299800879200809853049219412289891898381721200000000)xy^3 + (-4485870855187365891380048995017652628982071200311182672264363181081146760000000000xw + 161740373834875403999008140658405308702506346444494976170181843406011298948000000000)xy^2 + (-1484508172777843749088966910029547251011082696451685368788333734587930536739580000000000xw + 53524703357958071899540254341317800567789741426378653706826376130489367192830000000000)xy - 15862841104773197671854025783150400399822071745834087836031268955736122838373431000000000000 + 571914025367722899121206158831376151381382868131288660643553486027577666420399  
0000000000)
```

□

```
66928761xy^7 + (21911488848xw - 766037828240)xy^6 + (-203318356742784xw + 733099844294784)xy^5 + (-280722122877358000xw + 1012158088965439488)xy^4 + (-234912038345214432xw + 8469874588158623744)xy^3 + (-78591203121748770816xw + 283364613421131104256)xy^2 + (2589173344141632512xw - 904696010264018944)xy - 364471595827200xw + 1312782658043984  
(275427, (4196539377141683489385xw - 151092045959653109951970)xy^6 + (115924845820199844109248000xw - 417972975704981422669661760)xy^5 + (1295188009825641552288310406400xw - 44698667807925077086400110720)xy^4 + (1008510250000054276041031863193600xw - 392467952062857421837428213760)xy^3 + (36208158541186385252194215690240xw - 1385503722180376909182866768035840)xy^2 + (-115601486821683049919513806720xw + 416007088255452616573918904320)xy + 167832146481204715187077120xw - 605127409809396328308544000)  
(227580096987, (34108558492884819894645251200xw - 122965705732353398151280240000)xy^6 + (-1212339586631649695664592441344000xw + 437115254065586502857225842636800)xy^5 + (-60174769222720407232764436308377600xw + 219636215937956870593684710631814400)xy^4 + (-49693242047739485540786106502886656000xw + 17917153224716783917797429054269038400)xy^3 + (-1692114847085814085723345406849869414400xw + 610100684514181009633461419358684492800)xy^2 + (540239499861757896485617121466777600xw - 194786121778258755719671614359470000)xy - 78432775975057009436933294489600xw + 282793395454944533497544074854400)  
(936543609, (-36116436922455121203855384671484753365000000xw + 13021965521093672911723413267747694468000000)xy^6 + (-150399848217266707112766880548446406345728000000xw + 542274364569356660549158078961225519811993600000)xy^5 + (-1262616656442949497088155623385310730289152000000xw + 4565409808651624497583377524074531773623828480000000xw + 1071970293080147480744883997967330898862407860000000xw + 385046121223258474110919166281408462602155959910400000)xy^3 + (-35318536625249626711752236524908529712749346616000000xw + 12731395036648669971224220106014884544473413888000000)xy^2 + (1127357258815829104580082141649199935617236992000000xw - 40674444024699931584044743368681596818761318400000)xy - 16367166736734542144373309962382760987852800000xw + 5901265898196965955371033765785353595125760000000)
```

Example 2 (a record breaking field)

For $c_1 = \frac{1}{2}(a, b)$, $c_2 = \frac{1}{2}(c, d)$, write $\theta_{c+2d+4a+8b} = \theta[c_1, c_2]$.

► The functions

$$t = \frac{\theta_0\theta_8}{\theta_4\theta_{12}} \in \mathcal{F}_8, \quad u = \left(\frac{\theta_2\theta_8}{\theta_6\theta_{12}} \right)^2 \in \mathcal{F}_2, \quad v = \left(\frac{\theta_0\theta_2}{\theta_4\theta_6} \right)^2 \in \mathcal{F}_2$$

are class invariants for a certain τ for Enge and Thomé's $K = X^4 + 310X^2 + 17644$. Moreover,

$$y^2 = x(x-1)(x-t(\tau)^2)(x-u(\tau))(x-v(\tau))$$

has CM by \mathcal{O}_K .

Next

- ▶ preprint and code online in a few weeks
- ▶ a more thorough search with theta's
- ▶ ask around for other useful modular forms (hint...)
- ▶ Shimura reciprocity for Hilbert modular forms (i.e. fix K_0)
- ▶ examples come in families, make this precise