Smaller class invariants for constructing curves of genus 2

Marco Streng

THE UNIVERSITY OF WARWICK

LFANT Seminar
Bordeaux, France
March 29th, 2012

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

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

Fact: $j(E) = j(F) \iff E \cong_{\overline{k}} F$

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

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

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 $p = \pi\overline{\pi}$ prime)

1. Compute H_K mod 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 $= \pi$". It satisfies

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

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

$$X^7 + 313645809715X^6 - 3091990138604570X^5$$
$$+ 98394038810047812049302X^4$$
$$- 823534263439730779968091389X^3$$
$$+ 5138800366453976780323726329446X^2$$
$$- 425319473946139603274605151187659X$$
$$+ 737707086760731113357714241006081263.$$

- Weber (around 1900) replaces this by

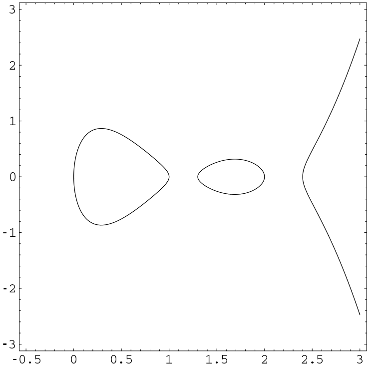
$$X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X - 1.$$

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.



Complex multiplication and invariants

- Elliptic curves E have CM if $\mathrm{End}(E) \ni \sqrt{-a}$ with $a > 0$
- Curves C of genus 2 have CM if $\mathrm{End}(J(C)) \ni \sqrt{-(a+b\sqrt{d})}$ with $d > 0$ non-square and $a + b\sqrt{d} > 0$.

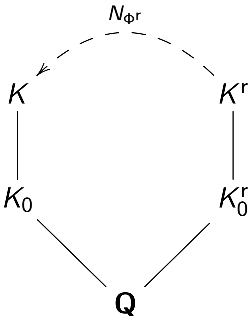
Igusa gave a genus-2 analogue of the j-invariant,

- Need three *absolute Igusa invariants* i_1, i_2, i_3 to specify a genus-two curve (instead of just one j-invariant).
- See "Computing Igusa class polynomials" arXiv:0903.4766 for the "best" triple.

The genus-two analogue of the Hilbert class polynomial is a triple of *Igusa class polynomials*.

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 $N_{\Phi^{\mathrm{r}}} : K \to K^{\mathrm{r}}$ 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

$$\begin{aligned} H_{i_1} &= \prod_C (X - i_1(C)) \in \mathbf{Q}[X] \\ H_{i_1,i_n} &= \sum_C i_n(C) \prod_{D \not\cong C} (X - i_1(D)) \in \mathbf{Q}[X] \qquad (n \in \{2,3\}) \end{aligned}$$

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.

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

Igusa class polynomials

Definition:

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

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

$$H_{i_1,i_n} = \sum_C i_n(C) \prod_{D \not\cong C} (X - i_1(D)) \in K_0^{\mathrm{r}}[X] \qquad (n \in \{2,3\})$$

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.

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

Igusa class polynomials

Definition:

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

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

$$H_{i_1,i_n} = \sum_C i_n(C) \prod_{D \not\cong C} (X - i_1(D)) \in K_0^{\mathrm{r}}[X] \qquad (n \in \{2,3\})$$

with products and sums taken over *one $Gal(\overline{K^r}/K^r)$-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.

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

Example

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

$$\begin{aligned}
H_{i_1} &= y^4 - 16906968y^3 + 54245326531032y^2 \\
&\quad + 6990615303516000y - 494251688841750000 \\
7^4 H_{i_1,i_2} &= 1181176456752y^3 - 6134558308934655456y^2 \\
&\quad - 12364496051356979280000y \\
&\quad + 7908422422819073400000 \\
7^4 H_{i_1,i_3} &= 178212862056777436 8y^3 \\
&\quad - 923275242804122377609363 2y^2 \\
&\quad - 118972825805086407998481600 0y \\
&\quad + 841185118801739120091480000 00
\end{aligned}$$

Example

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

$$\begin{aligned}
H_{i_1} &= y^2 + (1250964\omega - 8453484)y \\
&\quad + 374134464\omega - 1022492484 \\
7^4 H_{i_1,i_2} &= (-139899783096\omega + 590588228376)y \\
&\quad - 45253281038112\omega \\
&\quad + 143469827584272 \\
7^4 H_{i_1,i_3} &= (-2119153585580756 64\omega \\
&\quad + 891064310283887184)y \\
&\quad - 445917183184143296 64\omega \\
&\quad + 1383452995736653611 84
\end{aligned}$$

Genus-2 curves with prescribed Frobenius

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

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

1. write $(\pi) = N_{\Phi^{\mathrm{r}}}(\mathfrak{P})$ for some $\mathfrak{P} \subset \mathcal{O}_{K^{\mathrm{r}}}$
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

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

then a twist C of C^0 has "Frob $= \pi$". It satisfies

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

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 $\mathbf{C}/\Lambda$.
By choosing a $\mathbf{Z}$-basis of Λ (and scaling $\mathbf{C}$), get
$\Lambda = \tau\mathbf{Z} + \mathbf{Z}$, $\operatorname{Im}\tau > 0$.

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 $\mathfrak{f}$.
- $\mathfrak{f}$ is invariant only under *some* changes of bases, so something needs to be done.

Modular forms

Definition:

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

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

  for all $A \in \mathrm{SL}_2(\mathbf{Z})$ with $A \equiv 1 \bmod N$,
  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: $\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \quad \text{for } N = 24, k = 1/2$

Modular functions

Definition:

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

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

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 $\mathfrak{f}(z) = \zeta_{48}^{-1} \frac{\eta(\frac{z+1}{2})}{\eta(z)} \in \mathcal{F}_{48}$, where $\zeta_{48} = e^{2\pi i/48}$.

Galois groups of modular functions

Actions:

- $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ 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 q-expansion coefficients: $v : \zeta_N \mapsto \zeta_N^v$
- Let $(\mathbf{Z}/N\mathbf{Z})^* \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ via $v \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)$.

Note:

Given $A \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, let $v = \det(A)$. Then $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)[\left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)^{-1} A]$.

Fact:

$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) = \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\{\pm 1\}$

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 $\mathrm{disc}(K) \equiv 1, 17 \bmod 24$, then $\exists\tau$ such that $\mathfrak{f}(\tau)$ 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*.
- $\mathrm{Gal}(\mathcal{H}_N/\mathcal{H}_1) = (\mathcal{O}_K/N\mathcal{O}_K)^*/\mathcal{O}_K^*$.

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

Galois groups of values of modular functions

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

Shimura's reciprocity law:
We have $f(\tau)^x = f^{g_\tau(x)}(\tau)$ for some map

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

Explicitly: $g_\tau(x)$ is the transpose of the matrix of multiplication by x w.r.t. the $\mathbf{Q}$-basis τ, 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 $G = \mathrm{Gal}(\mathcal{H}_1/K)$ 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*. E.g.

$$(\mathfrak{f}^{24} - 16)^3 - j\mathfrak{f}^{24} = 0$$

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 $\mathcal{H}_g = \{\tau \in \mathrm{Mat}_g(\mathbf{C}) : \tau \text{ symmetric and } \mathrm{Im}\,\tau > 0\}$
- Changes of bases correspond to the action of

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

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

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

Siegel modular forms

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

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

  for all $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$ with $A \equiv 1 \bmod N$
  (and a holomorphicity condition at the cusps if $g = 1$).
- Let $\mathcal{F}_N = \left\{ \frac{g_1}{g_2} : \begin{array}{c} g_i \text{ of level } N \text{ and of equal weight, with} \\ q\text{-expansion coefficients in } \mathbf{Q}(\zeta_N) \end{array} \right\}$
- $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ acts on $\mathcal{F}_N$ via $f^A(\tau) := f(A\tau)$.

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

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 $v \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)$.

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 $\mathcal{F}_N$.

Example: theta constants

Definition:

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

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

Explicit action:

Given $A \in \mathrm{Sp}_{2g}(\mathbf{Z})$, there is a holomorphic $\rho = \rho_A : \mathcal{H}_g \to \mathbf{C}^*$ 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

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

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

Example: theta constants

In fact:

$$\frac{\theta[c_1, c_2]}{\theta[c_1', c_2']} \in \mathcal{F}_{2D^2} \quad \text{if } c_1, c_2, c_1', c_2' \in \frac{1}{D}\mathbf{Z}^g \text{ with } 2|D$$

Explicit action:

Given $A \in \mathrm{GSp}_{2g}(\mathbf{Z}/2D^2\mathbf{Z})$, we have for all c_1, c_2, c_1', c_2',

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

where $v(a^{\mathrm{t}}d - c^{\mathrm{t}}b) = 1$,

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

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

and d_1', d_2', r' are defined analogously.

The CM class fields for $g \geq 1$

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

The CM class fields for $g \geq 1$

The field $\mathcal{H}_N := K^{\mathrm{r}}(f(\tau) : f \in \mathcal{F}_N)$ 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 $\mathcal{O}_{K^{\mathrm{r}}}$-ideals coprime to N, and let

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

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

Also a version for non-maximal orders!

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

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

- 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 $\mu\overline{\mu} \in \mathbf{Q}$.
- Again, the full version also gives the action of $\mathrm{Gal}(\mathcal{H}_1/K^r)$.
- "An explicit version of Shimura's reciprocity law for Siegel modular functions" arXiv:1201.0020

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

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)

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

$$\begin{aligned}
H_{i_1} = 2\cdot 101^2 y^7 &+(-310410324232717295510\sqrt{13} \\
&\quad + 111920034044187774220)y^6 \\
&+(-304815375394920390351841501071188305100\sqrt{13} \\
&\quad + 1099027465536189912517941272236385718800)y^5 \\
&+(-2201909580030523730272623848434538048317834513875\sqrt{13} \\
&\quad + 7939097894735431844153019089320973153011210882125)y^4 \\
&+(-2094350525854786365698329174961782735189420898791141250\sqrt{13} \\
&\quad + 7551288209764401665731458692859504138760400195691473750)y^3 \\
&+(-907392914800494855136752991106041311116404713247380607234375\sqrt{13} \\
&\quad + 3271651681305911192688931423723753094763461200379169938284375)y^2 \\
&+(-30028332099313039720091760445942488226781301051810139974908125000\sqrt{13} \\
&\quad + 108268691100734381571211968891173879786167063702810731956822125000)y \\
&+(-32085417029115132212877701052175189051312077050549053777676328984375\sqrt{13} \\
&\quad + 1156856162931200670387093211443242850125709667683265459917987279296875)
\end{aligned}$$

Example 1 (the first field that I tried)

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

$$\begin{aligned}H_f = 3^8 101^2 y^7 &+ (21911488848\sqrt{13}\\ &\quad - 76603728240)y^6\\ &+(-203318356742784\sqrt{13}\\ &\quad + 733099844294784)y^5\\ &+(-280722122877358080\sqrt{13}\\ &\quad + 1012158088965439488)y^4\\ &+(-234912038356251443 2\sqrt{13}\\ &\quad + 846987458815862374 4)y^3\\ &+(-785912031217487708 16\sqrt{13}\\ &\quad + 283364613421131104256)y^2\\ &+(250917334141632512\sqrt{13}\\ &\quad - 904696010264018944)y\\ &+(-364471595827200\sqrt{13}\\ &\quad + 1312782658043904)\end{aligned}$$

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

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

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

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

Example 1 (continued)

Terminal — vim

```
20402*y^7 + (-310410324232717295510*w + 1119200340441877774220)*y^6 + (-304815375394920390351841501071188305100*w + 1099027465536189912517941272236385718800)*y^
5 + (-2201909580030523730272623848434538048317834513875*w + 7939097894735431844153019089320973153011210882125)*y^4 + (-20943505258547863656983291749617827351894
20898791141250*w + 7551288209764401665731458692859504138760400195691473750)*y^3 + (-907392914800494855136752991106041311116404713247380607234375*w + 32716516813
05911192688931423723753094763461200379169938284375)*y^2 + (-30028332099313039720091760445942488226781301051810139974908125000*w + 108268691100734381571211968891
173879786167063702810731956822125000)*y - 320854170291151322128777010521751890513120770505490537777676328984375*w + 11568561629312006703870932114432428501257096
67683265459917987279296875
(104060401, (155942160719197448511497600*w - 562257456480820026589520000)*y^6 + (10915460249997911281051048769982462340888000*w - 393562516266564444521976453468
30542588488000)*y^5 + (168373146277549827762748743327083206237502305644120000*w - 607078012314904622487588715272472722561309748288920000)*y^4 + (238652435808138
594034697534364809573290025398381044081800000*w - 860473594320621938090309645042531340247319597576659017800000)*y^3 + (10432226228149007102640212126403094819657
0701298335683621237000000*w - 376139265828315347221671304362880264396213048032027706818473000000)*y^2 + (3422978757984824090435381776507567613874776553028721788
254983445000000*w - 12341725426738324424199494569900641042064837165414213925317002945000000)*y + 254448518301571719798504716559584579677190202948541991757945905
09050000000*w - 91742717970215413696542092180092916555240944945393570493326703047900000000)
(104060401, (-4012937435827235689317264963498305932800000*w + 14468851690104080323524823696416410496000000)*y^6 + (-15069132256559836061432407109223455336207754
35750856464000000*w + 54332529027774860048729847772627218321237957703086360800000000)*y^5 + (-1088556219655951950859335956551055306392580398625865282600171392000
0000*w + 39248452661947760486383130049374702797762681330867052835728546240000000)*y^4 + (-1035382338920615643141289279801531180102071607086760478193812456502520
0000000*w + 3733124112688114175456922998080792008090530492019412289891889381721720000000)*y^3 + (-4485870855187365031380849955017652628982072100341118267226436
318108114676000000000*w + 16174037383487540399908140658405308702506346444494976170181843406011298948000000000)*y^2 + (-14845081727778437490889666910029547251011
0826966451685368788333734587930637950000000000*w + 535247033579587071899540245431137800567789741426378635706026376130489367192830000000000)*y - 1586204110477319
767185402578315040039982207174583408730603126895573612283837343100000000000*w + 57191402536777228691212061834613761513813820681312886606435353486027577666420399
00000000000)

▯


66928761*y^7 + (21911488848*w - 76603728240)*y^6 + (-203318356742784*w + 733099844294784)*y^5 + (-280722122877358080*w + 1012158088965439488)*y^4 + (-2349120383
562514432*w + 8469874588158623744)*y^3 + (-78591203121748770816*w + 283364613421131104256)*y^2 + (250917334141632512*w - 904696010264018944)*y - 364471595827200
*w + 1312782658043904
(275427, (4190539377141683489385*w - 15109204595965349951970)*y^6 + (115924845820199844109248000*w - 417972975704981422669661760)*y^5 + (12951880098256415522883
1040640*w - 466986678079250707086400110720)*y^4 + (1088510250005472604103186319360*w - 3924679520262857421837428213760)*y^3 + (36208158541186385252194215690240*
w - 130550372210376909182866768035840)*y^2 + (-115601486821683049919513886720*w + 416807088255452616573918904320)*y + 167832146481204715187077120*w - 6051274098
09396328300544000)
(227580096987, (341045505492884819894645251200*w - 1229657057323553398151280240000)*y^6 + (-121233958601634969566459244134400*w + 437115254065586502857225842636
800)*y^5 + (-601747692272207407232764436308377600*w + 2169632159379568705936047110631014400)*y^4 + (-4969324204773948554070610650208665600*w + 17917153224716783
917797429054269030400)*y^3 + (-169211484708581405723345406849869414400*w + 610100684514181009633461419358604492800)*y^2 + (540239499861757896485617121466777600*
w - 1947861217782587557196716143594700800)*y - 784327759750570090436933294489600*w + 2827933954549445333497544074854400)
(936543609, (-36116436922445121203855384671484753395200000*w + 130219665210936722911723413267747694464000000)*y^6 + (-1503998482172667871127668805544844634572
800000*w + 542274364569356660549158078961225519811993600000)*y^5 + (-126621665644294949770881556223305310730289152000000*w + 45654090806516244975833775240745317
7362382848000000)*y^4 + (-1071970920930801474807448399796733089886240768000000*w + 3865046121222358474110919166281402602155959910400000)*y^3 + (-353105366252496
26711752236524908529712749346816000000*w + 127313950366486699712242281060148845444373413888000000)*y^2 + (112735725881582910458808214164919993561723699200000*w
- 406474440242699931584044743368861596818761318400000)*y - 163671667363475421464773039962382760987852800000*w + 590126589019696595537103376578535359512576000000
)
```

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 $K = Q[X]/(X^4 + 310X^2 + 17644)$. Moreover,

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

  has CM by $\mathcal{O}_K$.

Next

- 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