Smaller class invariants for constructing curves of genus 2

Marco Streng

THE UNIVERSITY OF WARWICK

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

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

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

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

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

$$\begin{aligned} & X^7 + 313645809715X^6 - 3091990138604570X^5 \\ & + 98394038810047812049302X^4 \\ & - 8235342634397307799680913 89X^3 \\ & + 513880036645397678032372632 9446X^2 \\ & - 425319473946139603274605151187659X \\ & + 737707086760731113357714241006081263. \end{aligned}$$

- Weber (around 1900) replaces this by

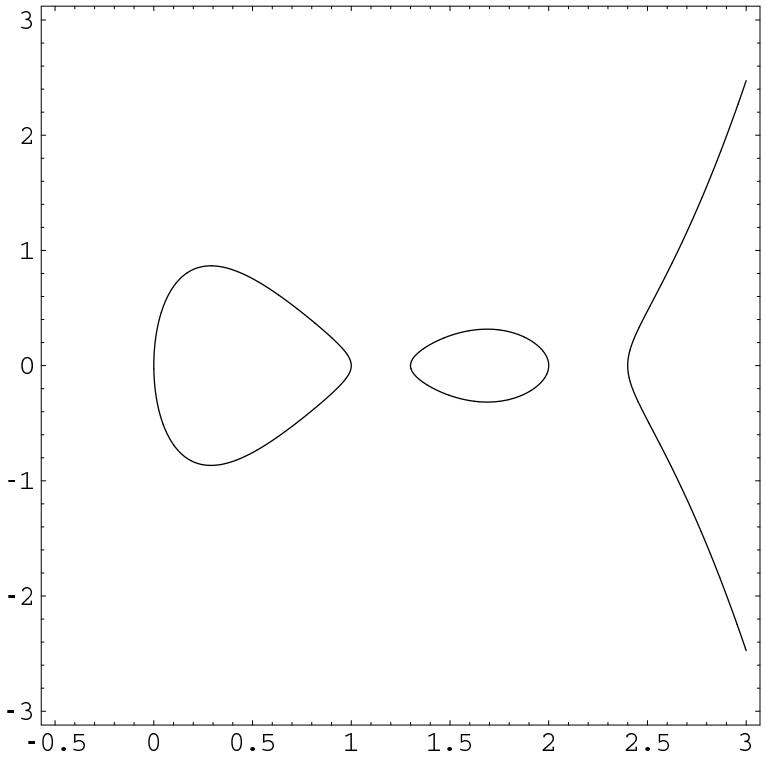
$$X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X - 1.$$

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:

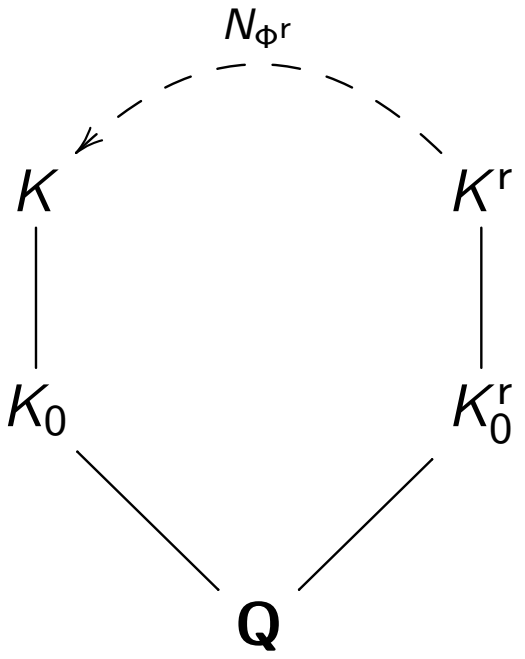
- A *CM-field* is a field $K = K_0(\sqrt{r})$ with K_0 a totally real number field and $r \in K_0$ totally negative.
- Let $A/\mathbf{C}$ be a g-dim. ab. var. We say that *A has CM* if $\mathcal{O} = \mathrm{End}(A)$ is an order in a CM-field K of degree $2g$.

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

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

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

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.

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

Igusa class polynomials

Definition:

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

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

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

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

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

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

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

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

$$\begin{aligned}
H_{i_1} &= y^4 - 16906968y^3 + 54245326531032y^2 \\
&\quad + 6990615303516000y - 494251688841750000 \\
7^4 H_{i_1,i_2} &= 1181176456752y^3 - 6134558308934655456y^2 \\
&\quad - 1236449605135697928000y \\
&\quad + 7908422422819073400000 \\
7^4 H_{i_1,i_3} &= 1782128620567774368y^3 \\
&\quad - 923275242804122377609363 2y^2 \\
&\quad - 1189728258050864079984816000y \\
&\quad + 8411851188017391200914800000 0
\end{aligned}$$

Example

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

$$\begin{aligned}
H_{i_1} &= y^2 + (1250964\omega - 8453484)y \\
&\quad + 374134464\omega - 1022492484 \\
7^4 H_{i_1,i_2} &= (-139899783096\omega + 590588228376)y \\
&\quad - 45253281038112\omega \\
&\quad + 143469827584272 \\
7^4 H_{i_1,i_3} &= (-21191535855807 5664\omega \\
&\quad + 89106431028388 7184)y \\
&\quad - 44591718318414329664\omega \\
&\quad + 138345299573665361184
\end{aligned}$$

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 $(\pi) = N_{\Phi^r}(\mathfrak{P})$ 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

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

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: $\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$ 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 $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)\left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & v \end{smallmatrix}\right)^{-1} A\right]$.

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*.
- $\mathrm{Gal}(\mathcal{H}_N/\mathcal{H}_1) = (\mathcal{O}_K/N\mathcal{O}_K)^*/\mathcal{O}_K^*$.

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

Galois groups of values of modular functions

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

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*.

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

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

- $\mathrm{Sp}_{2g}(\mathbf{Z}/N\mathbf{Z})$ acts on $\mathcal{F}_N$ via $f^A(\tau) := f(A\tau)$.

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

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

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

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

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

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

where

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

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

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 $\mathcal{F}_N$.

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.

New: also a version for non-maximal orders!

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

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

- 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 $(\mu) = N_{\Phi^{\mathrm{r}}}(\mathfrak{a})$ and $\mu\overline{\mu} \in \mathbf{Q}$.
- Again, the full version also gives the action of $\mathrm{Gal}(\mathcal{H}_1/K^{\mathrm{r}})$.

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)

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

$$\begin{aligned}
H_{i_1} = {} & 2\cdot 101^2 y^7 + (-3104103242327172955 10\sqrt{13} \\
& + 1119200340441877742 20) y^6 \\
& + (-3048153753949203903518415010711883051 00\sqrt{13} \\
& + 1099027465536189912517941272236385718800) y^5 \\
& + (-2201909580030523730272623848434538048317834513875\sqrt{13} \\
& + 7939097894735431844153019089320973153011210882125) y^4 \\
& + (-2094350525854786365698329174961782735189420898791141250\sqrt{13} \\
& + 7551288209764401665731458692859504138760400195691473750) y^3 \\
& + (-9073929148004948551367529911060413111164047132473806072343 75\sqrt{13} \\
& + 3271651681305911192688931423723753094763461200379169938284375) y^2 \\
& + (-3002833209931303972009176044594248822678130105181013997490 8125000\sqrt{13} \\
& + 1082686911007343815712119688911738797861670637028107319568221 25000) y \\
& + (-3208541702911513221287770105217518905131207705054905377767632 8984375\sqrt{13} \\
& + 1156856162931200670387093211443242850125709667683265459917987 279296875)
\end{aligned}$$

Example 1 (the first field that I tried)

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

$$\begin{aligned}
H_f = 3^8 101^2 y^7 &+ (21911488848\sqrt{13} \\
&\quad - 76603728240) y^6 \\
&+ (-203318356742784\sqrt{13} \\
&\quad + 733099844294784) y^5 \\
&+ (-280722122877358080\sqrt{13} \\
&\quad + 1012158088965439488) y^4 \\
&+ (-2349120383562514432\sqrt{13} \\
&\quad + 8469874588158623744) y^3 \\
&+ (-7859120312174877081 6\sqrt{13} \\
&\quad + 28336461342113110425 6) y^2 \\
&+ (250917334141632512\sqrt{13} \\
&\quad - 904696010264018944) y \\
&+ (-364471595827200\sqrt{13} \\
&\quad + 1312782658043904)
\end{aligned}$$

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

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

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

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

Example 1 (continued)

Terminal — vim

```
20402*y^7 + (-3104103242327172955l0*w + 1119200340441877774220)*y^6 + (-304815375394920390351841501071188305100*w + 109902746553618991251794127223638571880l)*y^
5 + (-22019095800305237302726238484345380483178345138l5*w + 7939097894735431844153019089320973153011210882125)*y^4 + (-209435052585478636569832917496178273518942
20898791141250*w + 7551288209764401665731458692859504138760400195691473750)*y^3 + (-907392914800494855136752991106041311116404713247380607234375*w + 32716516813
059111926889314237237530947634612003791699382843l5)*y^2 + (-300283320993130397200917604459424882267813010518101399749081250l0*w + 108268691100734381571211968891
173879786167063702810731956822125000)*y - 320854170291151322128777010521751890513120770505490537777676328984375*w + 115685616293120067038709321144324285012570967
676832654599179872792968l5
(104060401, (155942160719197448511497600*w - 562257456480820026589520000)*y^6 + (109154602499979112810510487699824623408880000*w - 393562516266564444521976453468
30542588488000)*y^5 + (168373146277549827762748743327083206237502305644120000*w - 607078012314904622487588715272472722561309748288920000)*y^4 + (238652435808138
594034697534364809573290025398381044081800000*w - 860473594320621938090309645042531340247319597576659017800000)*y^3 + (104322262281490071026402121264030948196570
701298335683621237000000*w - 376139265828315347221671304362880264396213048032027706818473000000)*y^2 + (342297875798482409043538177650756761387477655302872178825498344500000*w - 123417254267383244241994945690006410420648371654142139253170029450000000)*y + 254448518301571719798504716559584579677190202948541991757945905
09050000000*w - 917427179702154136965420921800929165552409449453935704933267030479000000000)
(104060401, (-401293743582723568931726496349830593280000*w + 144688516901040803235248236964164104960000000)*y^6 + (-150691322565598360614324071092234553362077543575085646400000*w + 5433252902777486004872984777262721832123795770308636080000000)*y^5 + (-108855621965595195085933595655105530639258039862586528260017139200000*w + 392484526619477604863831300493747027977626813308670528357285462400000000)*y^4 + (-10353823389206156431412892798015311801020716070867604781938124565025200000000*w + 373312411268811417545692299808079200809053049201941228989188938172172000000000)*y^3 + (-448587085518736503138084995501765262898207210034111826722643631810811467600000000000*w + 161740373834875403999081406584053087025063464444949761701818434060112989480000000000)*y^2 + (-148450817277784374908896669100295472510110826966451685368788333734587930637950000000000*w + 53524703357958707189954024543113780056778974142637863570602637613048936719283000000000000)*y - 1586204110477319767185402578315040039982207174583408730603126895573612283837343100000000000*w + 57191402536777228691212061834613761513813820681312886606435353486027577666420399000000000000)

[]

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, (41905393771416834893855*w - 151092045959653499519700)*y^6 + (11592484582019984410924800l0*w - 417972975704981422669661760)*y^5 + (12951880098256415522883
1040640*w - 466986678079250707086400110720)*y^4 + (10885102500054726041031863193600*w - 392467952026285742183742821376l0)*y^3 + (362081585411863852521942156902400*
w - 13055037221037690918286676803584l0)*y^2 + (-11560148682168304991951388672l0*w + 41680708825545261657391890432l0)*y + 167832146481204715187077120*w - 6051274098
09396328300544000)
(227580096987, (34104550549288481989464525120l0*w - 122965705732355339815128024000l0)*y^6 + (-12123395860163496956645924413440l0*w + 43711525406558650285722584263680
800)*y^5 + (-60174769227220740723276443630837760l0*w + 21696321593795687059360471106310144l00)*y^4 + (-49693242047739485540706106502086656l00*w + 17917153224716783
917797429054269030400)*y^3 + (-16921148470858140572334540684986941440l0*w + 61010068451418100963346141935860449280l0)*y^2 + (5402394998617578964856171214667776l00*
w - 19478612177825875571967161435947008l00)*y - 784327759750570090436933294489600*w + 28279339545494453334975440748544l00)
(936543609, (-36116436922445121203855384671484753395200000*w + 13021966521093672291172341326774769446400000l0)*y^6 + (-15039984821726678711276688055484464063457280000l0*w + 5422743645693566605491580789612255198119936000l0)*y^5 + (-12662166564429494977088155622330531073028915200000l0*w + 4565409080651624497583377524074531773623828480000l0)*y^4 + (-10719709209308014748074483997967330898862407680000000*w + 3865046121222358474110919166281402602155959910400000l0)*y^3 + (-353105366252496267117522365249085297127493468160000l00*w + 1273139503664866997122422810601488454443734138880000l00)*y^2 + (11273572588158291045880821416491999356172369920000l0*w - 4064744402426999315840447433688615968187613184000l0)*y - 16367166736347542146477303996238276098785280000l0*w + 5901265890196965955371033765785353595125760000l0
)
```

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