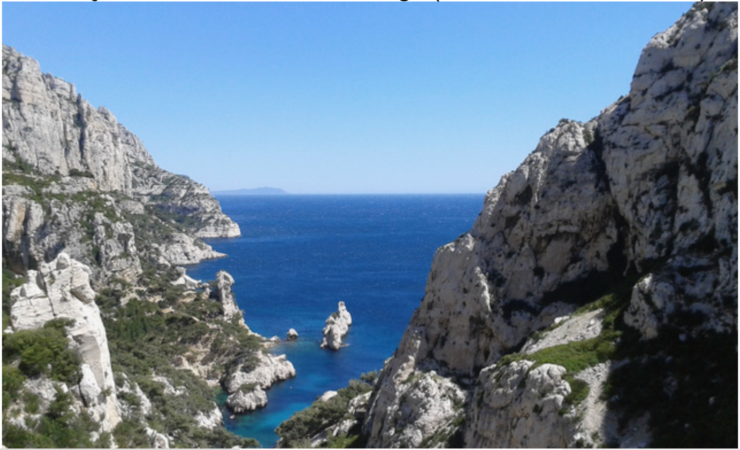
Schertz style class invariants for quartic CM fields

Marco Streng (Universiteit Leiden)
joint work with Andreas Enge (Université de Bordeaux)



AGC^2T
CIRM

3 June 2021

Schertz style class invariants for quartic CM fields

Marco Streng (Universiteit Leiden)
joint work with Andreas Enge (Université de Bordeaux)

AGC^2*T*
CIRM
(*online*)
3 June
2021

Goal

Our results are about $2 = 2$ (or more generally $g = g$).

Class invariants only give an improvement by a constant factor.

This talk is mostly about $1 = 1$.

Goal

Our results are about $2 = 2$ (or more generally $g = g$).

- Constructing varieties that are simple, so we can't use the a $1 + 1 = 2$ approach (as Jeroen Sijsling called it on Monday).

Class invariants only give an improvement by a constant factor.

- But such a constant factor was essential for the computation of modular polynomials for $g = 1$, as in the discussion after Jean Kieffer's talk on Monday.

This talk is mostly about $1 = 1$.

Elliptic curves with complex multiplication (CM)

Let k be a field of characteristic not 2 or 3.

An elliptic curve is a smooth projective curve of the form
$E : y^2 = x^3 + Ax + B$ with $A, B \in k$.

An endomorphism of E is an algebraic group homomorphism
$E \to E$ with $O \mapsto O$.

If $\mathrm{char}(k) = 0$, then "usually" $\mathrm{End}(E) = \mathbb{Z}$.
If $\mathrm{End}(E) \supsetneq \mathbb{Z}$, then we say that E has CM.

Example

- if $E : y^2 = x^3 + x$ and $i = \sqrt{-1} \in k$, then
  $f : (x, y) \mapsto (-x, iy)$.
- $\mathrm{End}(E) = \mathbb{Z}[f] \cong \mathbb{Z}[\sqrt{-1}]$

The Hilbert class polynomial

Definition: The *j-invariant* of the elliptic curve $y^2 = x^3 + Ax + B$ is

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

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

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

(e.g., $H_{\mathbb{Q}(\sqrt{-1})} = X - 1728$)

Application 1: roots generate the *Hilbert class field* of K
Application 2: elliptic curves of prescribed order

Application 2: elliptic curves of prescribed order

Algorithm:

1. If $p = \pi\overline{\pi}$ with $\pi \in \mathcal{O}_K$,
   (e.g., $p = a^2 + b^2$ for $K = \mathbb{Q}(\sqrt{-1})$)
2. then $(H_K \bmod p) \in \mathbb{F}_p[X]$ splits into linear factors.
3. Let $j_0 \in \mathbb{F}_p$ be a root and take $E/\mathbb{F}_p$ with $j(E) = j_0$.
4. Then (possibly after taking a twist), we have "Frob $= \pi$" and

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

   (e.g., $p + 1 - 2a$).

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

Computing the Hilbert class polynomial

- $\{\text{elliptic curves } E/\mathbb{C}\}/\cong \quad \longleftrightarrow \quad \{\text{lattices } \Lambda \subset \mathbb{C}\}/\cong$
- $\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$

Then
$$H_K = \prod_{[\mathfrak{a}] \in \mathcal{CL}(K)} (X - j(\mathfrak{a})) \in \mathbb{Z}[X].$$

Write $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ such that
$\tau = \omega_1/\omega_2 \in \mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

Then $j(E) = j(\Lambda) = j(\tau)$.

The size

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

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

using *class invariants*.

Replace j by a more general modular function.

Let $\mathcal{F}_N = \mathbb{Q}(\zeta_N)(X(N))$

$$= \left\{ \begin{array}{l} \text{meromorphic } f : \mathcal{H} \dashrightarrow \mathbb{C} \text{ such that} \\ (1)\ f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau) \text{ for all} \\ \qquad A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \text{ with } A \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod N \\ (2)\ f \in \mathbb{Q}(\zeta_N)[[q^{1/N}]] \text{ for } q = \exp(2\pi i\tau) \\ (3)\ f \text{ is meromorphic at the cusps} \end{array} \right\}$$

Examples:

- Example: $\mathcal{F}_1 = \mathbb{Q}(j)$.
- Weber used $\mathfrak{f}(\tau) = \zeta_{48}^{-1} \dfrac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} \in \mathcal{F}_{48}$, where

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n),$$

$$\zeta_{48} = e^{2\pi i/48}.$$

Replace j by a more general modular function.

$$\text{Let } \mathcal{F}_N = \mathbb{Q}(\zeta_N)(X(N)) \qquad \text{and} \qquad q = \exp(2\pi i \tau)$$

Examples:

- Example: $\mathcal{F}_1 = \mathbb{Q}(j)$.
- Weber used $\mathfrak{f}(\tau) = \zeta_{48}^{-1} \dfrac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} \in \mathcal{F}_{48}$, where

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n),$$
$$\zeta_{48} = e^{2\pi i/48}.$$

- Then $(\mathfrak{f}^{24} - 16)^3 - j\, \mathfrak{f}^{24} = 0$, which explains a factor $3 \cdot 24 = 72$ reduction in number of digits.
- Even better reduction for modular polynomials (assuming $\gcd(\ell, 48) = 1$).

Galois groups of modular functions

- Let $\mathcal{H}_N = K(f(\tau) : f \in \mathcal{F}_N)$, where $\tau\mathbb{Z} + \mathbb{Z}$ has CM by $\mathcal{O}_K$.
- $\mathcal{H}_1 = K(j(\tau))$ is the *Hilbert class field* of K.
- Call $f(\tau)$ a *class invariant* if $f(\tau) \in \mathcal{H}_1$.
- Weber's $\mathfrak{f}(\tau)$ is a class invariant for $\mathbb{Z}[\sqrt{-71}]$.

Galois groups:

$$\begin{tikzcd}
f \arrow[r] & f(\tau) \\
\mathcal{F}_N \arrow[r, dashed] \arrow[d, dash, "\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1"'] & \mathcal{H}_N \arrow[d, dash, "(\mathcal{O}_K/N\mathcal{O}_K)^*/\mathcal{O}_K^*"] \\
\mathbb{Q}(j) \arrow[r] & \mathcal{H}_1
\end{tikzcd}$$

Galois groups of modular functions

$$\begin{tikzcd}
f \arrow[r] & f(\tau) \\
\mathcal{F}_N \arrow[r, dashed] \arrow[d, dash, "\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1"'] & \mathcal{H}_N \arrow[d, dash, "(\mathcal{O}_K/N\mathcal{O}_K)^*/\mathcal{O}_K^*"] \\
\mathbb{Q}(j) \arrow[r] & \mathcal{H}_1
\end{tikzcd}$$

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

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

Explicitly: $g_\tau(x)$ is the transpose of the matrix of multiplication by x w.r.t. the $\mathbb{Q}$-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 gives the action of $G = \mathrm{Gal}(\mathcal{H}_N/K)$ on $f(\tau)$.

This allows us to

- check if $f(\tau)$ is a class invariant, i.e., $K(f(\tau)) \subseteq \mathcal{H}_1$
- compute the minimal polynomial of $f(\tau)$ over K:

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

Schertz style class invariants

Idea of Schertz: apply Shimura reciprocity once and for all to get one easily-usable theorem for many different f and K.

Theorem (Schertz) Let N be a positive integer.
Let f be a modular function such that $f(\tau)$ and $f(-1/\tau)$ have rational q-expansion and such that f is invariant under

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \mid b \right\}.$$

Let K be an imaginary quadratic number field such that all primes $p \mid N$ are split in K or have $\mathrm{ord}_p(N) = 1$ and are ramified in K.

Then there is a $\tau \in K$ with $f(\tau) \in \mathcal{H}_1$.

Moreover, Schertz gives a method for finding $\tau_1, \tau_2, \cdots, \tau_h$ with

$$\prod_{i=1}^{h} (X - f(\tau_i)) \in \mathbb{Q}[X].$$

Beyond elliptic curves

Higher genus curves and higher-dimensional abelian varieties.

Replace j in a suitable way.

Get: *class polynomials* with similar applications.

Examples:

- $y^2 = f(x)$ degree 5 or 6 (genus 2)
- $y^2 = f(x)$ degree 7 or 8 (genus 3)
- $y^3 = f(x)$ degree 4 (Picard curve of genus 3)
- smooth plane quartic curves (genus 3)
- $y^5 = f(x)$ degree 5 (cyclic curve of genus 6)

Class invariants for $g > 1$

An explicit version of Shimura's reciprocity law for Siegel modular functions [arxiv]
Rephrase Shimura's reciprocity law for $g \geq 1$ in a form that is explicit enough for doing calculations.

recip `https://bitbucket.org/mstreng/recip`
Implementation of reciprocity law and many other CM-related formulas and algorithms.

Schertz style class invariants in dimension 2 [arxiv]
With *Andreas Enge*: found a generalisation of Schertz' once-and-for-all method (for arbitrary g, but works best for $g \leq 2$).

Example

Consider thet *double Igusa quotient* $f = \frac{\Theta(\tau/2)\Theta(\tau/3)}{\Theta(\tau)\Theta(\tau/6)}$, where Θ is the product of the 10 "even theta constants".

If K is a primitive quartic CM field with real quadratic subfield K_0 and all primes of K_0 dividing 6 are split in K, then there exists a τ such that $f(\tau)$ (or maybe only $f(\tau)^2$) is a class invariant.

This changes

$$
\begin{aligned}
&2^{40} \cdot 13^4 \cdot X^5 \\
&+ (-614058542222020444579430 4\omega - 3229049049216954473077800 96)X^4 \\
&+ (-9663288403227640327417574195 2\omega - 4131427744203466842763320885248)X^3 \\
&+ (-961856435411091691207536138780672\omega - 19922426752533168631849612073238528)X^2 \\
&+ (-2810878875032206947279703590350876416\omega - 32507451628887950858017880191429021184)X \\
&+ (-39499917289929495153587578550801525308 01\omega - 591879683087731591574848056616335060746 74),
\end{aligned}
$$

where $\omega = \frac{1}{2}(1 + \sqrt{601})$, into ...

Example

Consider thet *double Igusa quotient* $f = \frac{\Theta(\tau/2)\Theta(\tau/3)}{\Theta(\tau)\Theta(\tau/6)}$, where Θ is the product of the 10 "even theta constants".

If K is a primitive quartic CM field with real quadratic subfield K_0 and all primes of K_0 dividing 6 are split in K, then there exists a τ such that $f(\tau)$ (or maybe only $f(\tau)^2$) is a class invariant.

This changes ... into

$$
\begin{aligned}
&2^2 \cdot 13^2 \cdot X^5 \\
&+ (1326\omega + 23894) \cdot X^4 \\
&+ (8833\omega + 1025477) \cdot X^3 \\
&+ (-14003\omega - 1482307) \cdot X^2 \\
&+ (-2040\omega - 6080) \cdot X \\
&- 2^2 \cdot 13^2,
\end{aligned}
$$

where $\omega = \frac{1}{2}(1 + \sqrt{601})$.

Open:

- Consequences for modular polynomials (decreasing size while still keeping the same applications).
- Statements about the quality of the class invariants.
- Finding more good functions.
- Polynomials relating the class invariants with the usual invariant (e.g., Igusa invariants).