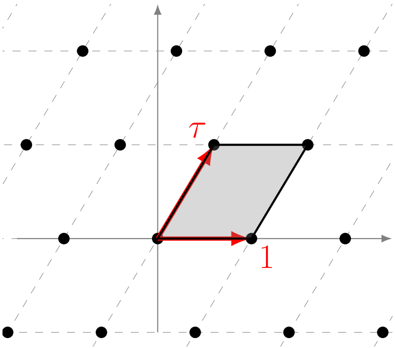
Generalized class polynomials

Marc Houben

Joint with Marco Streng

09/08/2022

Elliptic curves over $\mathbb{C}$



Elliptic curve $E = \mathbb{C}/(\mathbb{Z}[\tau]) = \mathbb{C}/\Lambda$

$\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\}$

Typically, $\mathrm{End}(\mathbb{Z}[\tau]) = \mathrm{End}(E) = \mathbb{Z}$.

If $a\tau^2 + b\tau + c = 0$ for coprime $a, b, c \in \mathbb{Z}$, then $\mathrm{End}(E) \cong \mathbb{Z}[a\tau] = \mathcal{O} \subseteq K = \mathbb{Q}(\tau)$.

The *Hilbert class polynomial* is:

$$H_\tau(X) = \prod_{\sigma \in \mathrm{Gal}(K(j(\tau))/K)} (X - \sigma(j(\tau))) = \prod_{\substack{E \text{ ell. curve} \\ \mathrm{End}(E) \cong \mathcal{O}}} (X - j(E)) \in \mathbb{Z}[X].$$

$K(j(\tau)) = K_{\mathcal{O}}$; the *ring class field* of $\mathcal{O}$.

The CM method

Goal

Construct an ordinary elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = N$.

What does $\#E(\mathbb{F}_q)$ say about $\mathrm{End}(E) = \mathcal{O}$?

$N = q + 1 - t$, where $\pi^2 - t\pi + q = 0$ ($\pi = \mathrm{Frob}_q$).

So $\mathbb{Z}[\pi] \subseteq \mathcal{O} \implies t^2 - 4q = \mathrm{Disc}(\mathbb{Z}[\pi]) = v^2 \,\mathrm{Disc}(\mathcal{O})$ for some $v \in \mathbb{Z}$.

Algorithm (CM method)

Given q, t, find $E/\mathbb{F}_q$ with trace t.

1. Find $v \in \mathbb{Z}$ and $D < 0$ such that $v^2 D = t^2 - 4q$.
2. Compute the Hilbert class polynomial $H_D(X) \in \mathbb{Z}[X]$.
3. Extract a root $j \in \mathbb{F}_q$ of $H_D \pmod{p}$.
4. Output E_j with $j(E_j) = j$ (or twist).

Class invariants

Example

For $\tau \in \mathbb{H}$ imaginary quadratic of discriminant $D = -103$,

$$\begin{aligned} H_\tau(X) &= X^5 + 70292286280125X^4 + 85475283659296875X^3 \\ &\quad + 4941005649165514137656250000X^2 \\ &\quad + 13355527720114165506172119140625X \\ &\quad + 28826612937014029067466156005859375. \end{aligned}$$

Definition

Let f be a modular function and $\tau \in \mathbb{H}$ imaginary quadratic. If $f(\tau) \in K_{\mathcal{O}}$ then we call (f, τ) a *class invariant*, and we define

$$H_\tau[f](X) = \prod_{\sigma \in \mathrm{Gal}(K(f(\tau))/K)} (X - \sigma(f(\tau))).$$

Example

Let $\mathfrak{f}(z) = \zeta_{48}^{-1}\eta(\frac{z+1}{2})/\eta(z)$. Then $(\mathfrak{f}^{24}-1)^3 - j\mathfrak{f}^{24} = 0$, and

$$H_\tau[\mathfrak{f}](X) = X^5 + 2X^4 + 3X^3 + 3X^2 + X - 1,$$

for (any) τ of discriminant $D = -103$.

Definition

The *reduction factor* of a modular function f of level N is

$$r(f) = \frac{\deg(j : X(N) \to \mathbb{P}^1)}{\deg(f : X(N) \to \mathbb{P}^1)}.$$

If $K(f(\tau)) = K_{\mathcal{O}}$ and $h(j(\tau)) \to \infty$, then $\frac{\log|H_\tau[j](X)|_\infty}{\log|H_\tau[f](X)|_\infty} \to r(f)$.

Theorem (Bröker–Stevenhagen, 2008)

$r(f) \leq 32768/325 \approx 100.82$.

Generalized class polynomials

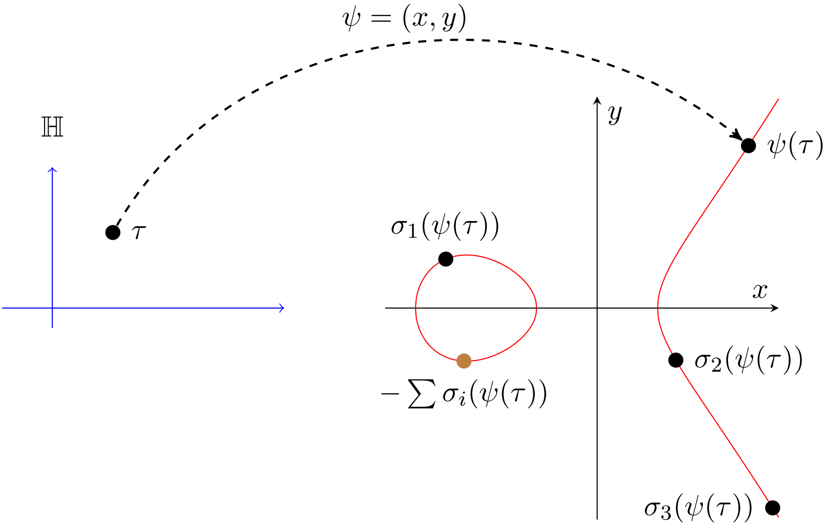
Let $C/\mathbb{Q}$ be a modular Weierstrass curve

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $\tau \in \mathbb{H}$ such that $(x, \tau), (y, \tau)$ are class invariants. Let $P = (x(\tau), y(\tau)) \in C(K_{\mathcal{O}})$. Let $G = \mathrm{Gal}(K(x(\tau), y(\tau))/K)$. The *generalized class function* $F_\tau[C] \in K(C)$ is defined by its divisor (hence only up to multiplication by an element of $K^\times$)

$$\mathrm{div} F_\tau[C] = \left[\sum_{\sigma \in G} (\sigma(P))\right] + \left(-\sum_{\sigma \in G} \sigma(P)\right) - (\#G + 1)(\infty).$$

The *generalized class polynomial* is then the unique polynomial $H_\tau[C] \in K[X, Y]$ with $\deg Y \leq 1$ such that $H_\tau[C](x, y) = F_\tau[C]$.


$\psi = (x, y)$
$\mathbb{H}$
τ
y
$\psi(\tau)$
$\sigma_1(\psi(\tau))$
x
$\sigma_2(\psi(\tau))$
$-\sum \sigma_i(\psi(\tau))$
$\sigma_3(\psi(\tau))$

Example

Let $C = X_+^0(119) : y^2 + 3xy - y = x^3 - 3x^2 + x$, where $(q = \exp(2\pi i/119))$

$$\begin{aligned} x &= q^{-2} + q^{-1} + 1 + q + 2q^2 + 2q^3 + 3q^4 + 3q^5 + 4q^6 + 5q^7 + \ldots \\ y &= q^{-3} + 1 + 2q + 2q^2 + 4q^3 + 4q^4 + 7q^5 + 9q^6 + 12q^7 + \ldots \end{aligned}$$

For τ of discriminant -103, we have

$$H_\tau[C] = X^3 + 2X^2 + XY + 2X + Y.$$

Definition

The *reduction factor* of a modular curve C is

$$r(C) = \frac{\deg(j : X(N) \to \mathbb{P}^1)}{\deg(\psi : X(N) \to C)}.$$

Theorem (H.–Streng, 2022)

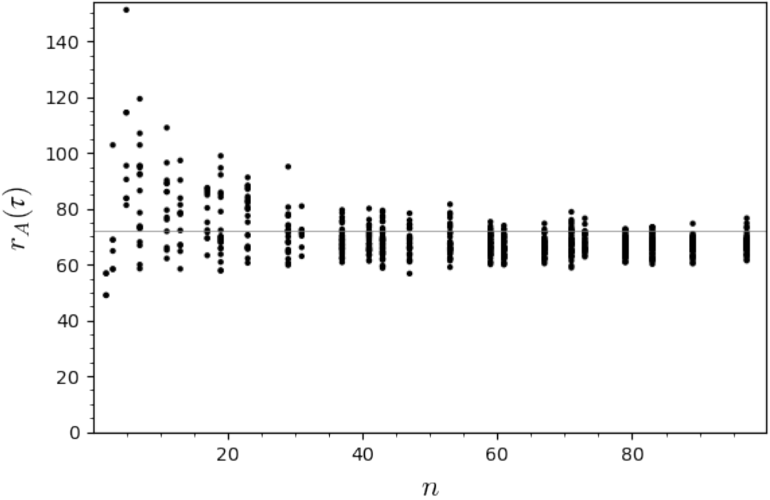
If C is an elliptic curve of rank 0, and $\tau \in \mathbb{H}$ ranges over a sequence of imaginary quadratic points for which

$$\frac{h(j(\tau))}{\log\log(\#\operatorname{Pic}(\mathcal{O}))} \to \infty,$$

then

$$\frac{\log |H_\tau[j]|_\infty}{\log |H_\tau[C]|_\infty} \to r(C) \cdot [K_{\mathcal{O}} : K(\psi(\tau))].$$

Computational results for $X_+^0(119)$



Open problems

1. Implement efficient computation of generalized class polynomials (e.g. using CRT).
2. Prove height reductions for arbitrary curves (e.g. $X_+^0(239)$).