Shimura’s reciprocity law and class invariants

Osmanbey Uzunkol

Fakultät für Mathematik
Technische Universität Berlin
Institut de Mathématiques de Luminy

10th December 2009
Outline

Problem

Class polynomials
  Preliminaries
  Class invariants

Class invariants via reciprocity law of Shimura
  'Thetanullwerte'
    Class invariants as quotients of 'Thetanullwerten'

Class units
  Motivation
  Unit group

Class invariants for genus 2 (in progress)
  Hyperelliptic Curves with CM
  Sasaki’s result
  Higher order reciprocity law of Shimura
Hilbert’s 12th Problem, Kronecker-Weber

- **Kronecker-Weber**: A finite field extension $L/\mathbb{Q}$ is abelian if and only if $L \subseteq \mathbb{Q}(\zeta_n)$, i.e. the abelian extensions of $\mathbb{Q}$ are classified completely using the special values of the transcendental function $z \mapsto e^{2\pi iz}$ at points $z$ of finite order on the circle $\mathbb{R}/\mathbb{Z}$. 
Hilbert’s 12th Problem, Kronecker-Weber

- **Kronecker-Weber:** A finite field extension $L/Q$ is abelian if and only if $L \subseteq Q(\zeta_n)$, i.e. the abelian extensions of $Q$ are classified completely using the special values of the transcendental function $z \mapsto e^{2\pi iz}$ at points $z$ of finite order on the circle $\mathbb{R}/\mathbb{Z}$.

- **12th Problem:** Can we classify completely the abelian extensions of an arbitrary number field using special values of suitable transcendental functions?
Hilbert’s 12th Problem, Kronecker-Weber

- **Kronecker-Weber**: A finite field extension $L/\mathbb{Q}$ is abelian if and only if $L \subseteq \mathbb{Q}(\zeta_n)$, i.e., the abelian extensions of $\mathbb{Q}$ are classified completely using the special values of the transcendental function $z \mapsto e^{2\pi iz}$ at points $z$ of finite order on the circle $\mathbb{R}/\mathbb{Z}$.

- **12th Problem**: Can we classify completely the abelian extensions of an arbitrary number field using special values of suitable transcendental functions?
An example of a class polynomial

\[
(\text{Minimal polynomial of } j(\tau)) : \quad H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432.
\]

\textbf{Problem:} Is it possible to construct alternative class polynomials having significantly smaller coefficients than the above one?
An example of a class polynomial

- **(Minimal polynomial of \( j(\tau) \))**: 
  \[
  H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 
  95864841637996112067555072 \cdot x^4 + 
  775121756231241041610849730560 \cdot x^3 + 
  534484930703209896960446929872814080 \cdot x^2 + 
  6020337293681148983229932704488367325184 \cdot x + 
  28508041377034538166862450172153093456658432.
  \]

- **Problem**: Is it possible to construct alternative class polynomials having significantly smaller coefficients than the above one with the possibility of retrieving \( j(\tau) \)?
An example of a class polynomial

*(Minimal polynomial of $j(\tau)) :
H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 +
95864841637996112067555072 \cdot x^4 +
775121756231241041610849730560 \cdot x^3 +
534484930703209896960446929872814080 \cdot x^2 +
6020337293681148983229932704488367325184 \cdot x +
28508041377034538166862450172153093456658432.*

**Problem:** Is it possible to construct alternative class polynomials having significantly smaller coefficients than the above one with the possibility of retrieving $j(\tau)$?
Algebraic number theory

- $K$: Imaginary quadratic number field with the discriminant $d < 0$.
- $\mathcal{O}_t$: The unique order of $K$ with the conductor $t$, i.e. $[\mathcal{O}_K : \mathcal{O}_t] = t$.
- A free $\mathbb{Z}$–module $a \neq 0$ of rank 2 in $K$ is called
  1. an ideal of $\mathcal{O}_t$, if $\mathcal{O}_t a \subseteq a$,
  2. an integral ideal of $\mathcal{O}_t$, if $\mathcal{O}_t a \subseteq a \subseteq \mathcal{O}_t$,
  3. a fractional ideal of $\mathcal{O}_t$, if $\mathcal{O}_t = \{ \xi \in K | \xi a \subseteq a \}$.
- Every free $\mathbb{Z}$–module of rank 2 is a fractional ideal of an order in $K$. 
Complex multiplication

- Fractional ideals of $O_t$ form a multiplicative group $I_t$, having the subgroup $H_t = \{\gamma O_t | \gamma \in K, \gamma \neq 0\}$.
- The factor group $Cl_t := I_t/H_t$ is called the ring ideal class group (mod $t$).
Complex multiplication

- Fractional ideals of $\mathcal{O}_t$ form a multiplicative group $\mathcal{I}_t$, having the subgroup $\mathcal{H}_t = \{ \gamma \mathcal{O}_t | \gamma \in K, \gamma \neq 0 \}$.
- The factor group $\text{Cl}_t := \mathcal{I}_t / \mathcal{H}_t$ is called the ring ideal class group (mod $t$), (class field theory $\Rightarrow$) with the class number $h_t := |\text{Cl}_t|$. 

Class field theory:
We have a Galois extension $\Omega_t$, the so-called ring class field (mod $t$), of $K$ with $\text{Cl}_t \cong \text{Gal}(\Omega_t/K)$.

Main theorem of complex multiplication:
$\Omega_t = K(j(\tau)), \tau \in \mathcal{H} \cap \mathcal{O}_t$, in particular $\Omega := \Omega_1$ is the Hilbert class field of $K$, i.e. the maximal totally unramified abelian extension of $K$.

$\mathcal{J}(\tau_i), 1 \leq i \leq h_t$, form a complete system of conjugate numbers over $K$.

Due to $\mathbb{Q}(\mathcal{J}(\tau)) = \mathbb{R} \cap \Omega_t$ also over $\mathbb{Q}$. 
Complex multiplication

- Fractional ideals of $\mathcal{O}_t$ form a multiplicative group $\mathcal{I}_t$, having the subgroup $\mathcal{H}_t = \{\gamma \mathcal{O}_t | \gamma \in K, \gamma \neq 0\}$.
- The factor group $\text{Cl}_t := \mathcal{I}_t / \mathcal{H}_t$ is called the ring ideal class group $\text{(mod } t\text{)}, \text{(class field theory } \Rightarrow \text{)}$ with the class number $h_t := |\text{Cl}_t|$.
- **Class field theory:** We have a Galois extension $\Omega_t$, the so-called ring class field (mod $t$), of $K$ with $\text{Cl}_t \cong \text{Gal}(\Omega_t/K)$. 
Complex multiplication

- Fractional ideals of $\mathcal{O}_t$ form a multiplicative group $\mathcal{I}_t$, having the subgroup $\mathcal{H}_t = \{ \gamma \mathcal{O}_t | \gamma \in K, \gamma \neq 0 \}$.
- The factor group $\text{Cl}_t := \mathcal{I}_t / \mathcal{H}_t$ is called the ring ideal class group (mod $t$), (class field theory $\Rightarrow$) with the class number $h_t := |\text{Cl}_t|$.
- **Class field theory:** We have a Galois extension $\Omega_t$, the so-called ring class field (mod $t$), of $K$ with $\text{Cl}_t \cong \text{Gal}(\Omega_t/K)$.
- **Main theorem of complex multiplication:** $\Omega_t = K(j(\tau))$, $\tau \in \mathbb{H} \cap \mathcal{O}_t$, 
Complex multiplication

- Fractional ideals of $\mathcal{O}_t$ form a multiplicative group $\mathcal{I}_t$, having the subgroup $\mathcal{H}_t = \{ \gamma \mathcal{O}_t | \gamma \in K, \gamma \neq 0 \}$.
- The factor group $\text{Cl}_t := \mathcal{I}_t / \mathcal{H}_t$ is called the ring ideal class group (mod $t$), (class field theory $\Rightarrow$) with the class number $h_t := |\text{Cl}_t|$.
- **Class field theory:** We have a Galois extension $\Omega_t$, the so-called ring class field (mod $t$), of $K$ with $\text{Cl}_t \cong \text{Gal}(\Omega_t/K)$.
- **Main theorem of complex multiplication:** $\Omega_t = K(j(\tau))$, $\tau \in \mathbb{H} \cap \mathcal{O}_t$, in particular $\Omega := \Omega_1$ is the Hilbert class field of $K$, i.e. the maximal totally unramified abelian extension of $K$. 
Complex multiplication

- Fractional ideals of $\mathcal{O}_t$ form a multiplicative group $\mathcal{I}_t$, having the subgroup $\mathcal{H}_t = \{\gamma \mathcal{O}_t | \gamma \in K, \gamma \neq 0\}$.
- The factor group $\text{Cl}_t := \mathcal{I}_t / \mathcal{H}_t$ is called the ring ideal class group $(\text{mod } t)$, (class field theory $\Rightarrow$) with the class number $h_t := |\text{Cl}_t|$.

Class field theory: We have a Galois extension $\Omega_t$, the so-called ring class field $(\text{mod } t)$, of $K$ with $\text{Cl}_t \cong \text{Gal}(\Omega_t / K)$.

Main theorem of complex multiplication: $\Omega_t = K(j(\tau))$, $\tau \in \mathbb{H} \cap \mathcal{O}_t$, in particular $\Omega := \Omega_1$ is the Hilbert class field of $K$, i.e. the maximal totally unramified abelian extension of $K$.

- $j(\tau_i), 1 \leq i \leq h_t$, form a complete system of conjugate numbers over $K$. 
Complex multiplication

- Fractional ideals of $O_t$ form a multiplicative group $I_t$, having the subgroup $H_t = \{ \gamma O_t | \gamma \in K, \gamma \neq 0 \}$.
- The factor group $Cl_t := I_t / H_t$ is called the ring ideal class group (mod $t$), (class field theory $\Rightarrow$) with the class number $h_t := |Cl_t|$.
- Class field theory: We have a Galois extension $\Omega_t$, the so-called ring class field (mod $t$), of $K$ with $Cl_t \cong Gal(\Omega_t / K)$.
- Main theorem of complex multiplication: $\Omega_t = K(j(\tau))$, $\tau \in \mathbb{H} \cap O_t$, in particular $\Omega := \Omega_1$ is the Hilbert class field of $K$, i.e. the maximal totally unramified abelian extension of $K$.
- $j(\tau_i), 1 \leq i \leq h_t$, form a complete system of conjugate numbers over $K$.
- $\Rightarrow$ Due to $\mathbb{Q}(j(\tau)) = \mathbb{R} \cap \Omega_t$ also over $\mathbb{Q}$. 
Complex multiplication

- Fractional ideals of $\mathcal{O}_t$ form a multiplicative group $\mathcal{I}_t$, having the subgroup $\mathcal{H}_t = \{ \gamma \mathcal{O}_t | \gamma \in K, \gamma \neq 0 \}$.
- The factor group $\text{Cl}_t := \mathcal{I}_t/\mathcal{H}_t$ is called the ring ideal class group (mod $t$), (class field theory $\Rightarrow$) with the class number $h_t := |\text{Cl}_t|$.
- Class field theory: We have a Galois extension $\Omega_t$, the so-called ring class field (mod $t$), of $K$ with $\text{Cl}_t \cong \text{Gal}(\Omega_t/K)$.
- Main theorem of complex multiplication: $\Omega_t = K(j(\tau))$, $\tau \in \mathbb{H} \cap \mathcal{O}_t$,
in particular $\Omega := \Omega_1$ is the Hilbert class field of $K$, i.e. the maximal totally unramified abelian extension of $K$.
- $j(\tau_i), 1 \leq i \leq h_t$, form a complete system of conjugate numbers over $K$.
  $\Rightarrow$ Due to $\mathbb{Q}(j(\tau)) = \mathbb{R} \cap \Omega_t$ also over $\mathbb{Q}$. 
Shimura’s reciprocity law and class invariants

Class polynomials

Preliminaries

\[
K(j(\tau)) = \Omega_t
\]

\[
Q(j(\tau)) = K(j(\tau)) \cap \mathbb{R}
\]

Class polynomial: “numerical computation”

\[
\tau_i \in \mathcal{O}_t \cap \mathbb{H} \text{ with } D = t^2 d
\]

\[
H_D(x) = \prod_{1 \leq i \leq h_t} (X - j(\tau_i)) \in \mathbb{Z}[X].
\]

Enge et. al: The required precision is

\[
\left\lfloor \log_2 \left( 2.48 h_t + \pi \sqrt{|D|} \sum_{(a,b,c) \in \mathcal{H}(D)} \frac{1}{a} \right) \right\rfloor + 2.
\]
Shimura’s reciprocity law and class invariants

K(j(τ)) = Ωₜ

Q(j(τ)) = K(j(τ)) ∩ ℜ

Q

▶ Class polynomial: “numerical computation”

τᵢ ∈ ℌ with D = t²d

H_D(x) = \prod_{1 \leq i \leq h_t} (X - j(τᵢ)) ∈ ℤ[X].

▶ Enge et al: The required precision is

\left\lfloor \log_2 \left( 2.48 h_t + \pi \sqrt{|D|} \sum_{(a,b,c) \in ℋ(D)} \frac{1}{a} \right) \right\rfloor + 2.

▶ Brauer-Siegel: The class number hₜ grows like |D|^{1/2+o(1)}.

⇒ appr. \sqrt{|D|} coefficients need to be computed.
Class polynomial: "numerical computation"

\[ \tau_i \in \mathcal{O}_t \cap \mathbb{H} \text{ with } D = t^2d \]

\[ H_D(x) = \prod_{1 \leq i \leq h_t} (X - j(\tau_i)) \in \mathbb{Z}[X]. \]

Enge et. al: The required precision is

\[ \left\lfloor \log_2 \left( 2.48h_t + \pi \sqrt{|D|} \sum_{(a,b,c) \in \mathcal{H}(D)} \frac{1}{a} \right) \right\rfloor + 2. \]

Brauer-Siegel: The class number \( h_t \) grows like \( |D|^{1/2 + o(1)} \).

\( \Rightarrow \) appr. \( \sqrt{|D|} \) coefficients need to be computed.
Coefficients

\[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432. \]

- Coefficients are 'huge'!
- Even worse: They grow exponentially in the size \(|D| \to \infty|\).
Shimura’s reciprocity law and class invariants

Class polynomials

Preliminaries

Coefficients

\[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432. \]

- Coefficients are ‘huge’!
- Even worse: They grow exponentially in the size \(|D| \to \infty\).
Weber class invariants

- Define $\gamma_2(\tau) = \sqrt[3]{j(\tau)}$ and $\gamma_3(\tau) = \sqrt{j(\tau) - 12^3}$.

- Schläfli functions

  $f(\tau) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)}$, $f_1(\tau) = \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)}$, $f_2(\tau) = \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)}$

  with $\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n)$, $q = e^{2\pi i \tau}$. 
Weber class invariants

- Define $\gamma_2(\tau) = 3\sqrt[3]{j(\tau)}$ and $\gamma_3(\tau) = \sqrt{j(\tau) - 12^3}$.

- **Schläfli functions**

  $f(\tau) = e^{-\pi i \frac{1}{24}} \frac{\eta\left(\frac{\tau + 1}{2}\right)}{\eta(\tau)}$, $f_1(\tau) = \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)}$, $f_2(\tau) = \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)}$

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

- **Weber:** $f(\tau)f_1(\tau)f_2(\tau) = \sqrt{2}$ for every $\tau \in \mathbb{H}$. 
Weber class invariants

- Define $\gamma_2(\tau) = 3\sqrt[3]{j(\tau)}$ and $\gamma_3(\tau) = \sqrt{j(\tau) - 12^3}$.

- Schlafli functions
  
  \[ f(\tau) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)}, \]
  \[ f_1(\tau) = \frac{\eta(\tau)}{\eta(\tau/2)}, \]
  \[ f_2(\tau) = \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)} \]

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

- Weber: $f(\tau)f_1(\tau)f_2(\tau) = \sqrt{2}$ for every $\tau \in \mathbb{H}$.

- We have: $\gamma_2 = \frac{f^{24} - 16}{f^8} = \frac{f_1^{24} + 16}{f_1^8} = \frac{f_2^{24} + 16}{f_2^8}$.
Weber class invariants

- Define $\gamma_2(\tau) = 3\sqrt{j(\tau)}$ and $\gamma_3(\tau) = \sqrt{j(\tau) - 12^3}$.

- **Schläfli functions**
  
  $f(\tau) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)}$, $f_1(\tau) = \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)}$, $f_2(\tau) = \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)}$

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

- **Weber**: $f(\tau)f_1(\tau)f_2(\tau) = \sqrt{2}$ for every $\tau \in \mathbb{H}$.

- We have: $\gamma_2 = \frac{f_2^{24} - 16}{f_8^4} = \frac{f_1^{24} + 16}{f_8^4} = \frac{f_2^{24} + 16}{f_2^8}$.

- We have $\mathbb{Q}(j(\tau)) \subseteq \mathbb{Q}(g(\tau))$, where $g$ is a power of one of the Schläfli functions.
Weber class invariants

- Define $\gamma_2(\tau) = 3\sqrt[3]{j(\tau)}$ and $\gamma_3(\tau) = \sqrt{j(\tau) - 12^3}$.

- Schläfli functions
  $$
  f(\tau) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)},
  f_1(\tau) = \frac{\eta(\tau)}{\eta(\tau)},
  f_2(\tau) = \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)}
  $$
  with $\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n), q = e^{2\pi i \tau}$.

- Weber: $f(\tau)f_1(\tau)f_2(\tau) = \sqrt{2}$ for every $\tau \in \mathbb{H}$.

- We have: $\gamma_2^2 = \frac{f_2^{24} - 16}{f_8^8} = \frac{f_1^{24} + 16}{f_8^8} = \frac{f_2^{24} + 16}{f_2^8}$.

- We have $\mathbb{Q}(j(\tau)) \subseteq \mathbb{Q}(g(\tau))$, where $g$ is a power of one of the Schläfli functions.
A theorem of Schertz

- \( g(\tau) \) is called a **class invariant**, if also \( \mathbb{Q}(j(\tau)) = \mathbb{Q}(g(\tau)) \).

- **Schertz, Gee:** Let \( \tau \in \mathbb{H} \cap K \) be a root of \( Ax^2 + Bx + C = 0 \) with \( D(\tau) = B^2 - 4AC = -4m = t^2d \). Then
  1. \( g(\tau) = f(\tau)^3 \), if \( m \equiv 3 \mod 8 \),
  2. \( g(\tau) = \left(\frac{1}{2}f(\tau)^4\right)^3 \), if \( m \equiv 5 \mod 8 \),

are class invariants and algebraic integers.
A theorem of Schertz

- \( g(\tau) \) is called a **class invariant**, if also \( \mathbb{Q}(j(\tau)) = \mathbb{Q}(g(\tau)) \).

- **Schertz, Gee:** Let \( \tau \in \mathbb{H} \cap K \) be a root of \( Ax^2 + Bx + C = 0 \) with \( D(\tau) = B^2 - 4AC = -4m = t^2d \). Then
  1. \( g(\tau) = f(\tau)^3 \), if \( m \equiv 3 \mod 8 \),
  2. \( g(\tau) = \left(\frac{1}{2}f(\tau)^4\right)^3 \), if \( m \equiv 5 \mod 8 \),

are class invariants and algebraic integers.

- Similarly, there exist class invariants for \( m \equiv 1, 2, 4, 6, 7 \mod 8 \).
A theorem of Schertz

- $g(\tau)$ is called a class invariant, if also $\mathbb{Q}(j(\tau)) = \mathbb{Q}(g(\tau))$.

- **Schertz, Gee:** Let $\tau \in \mathbb{H} \cap K$ be a root of $Ax^2 + Bx + C = 0$ with $D(\tau) = B^2 - 4AC = -4m = t^2d$. Then
  1. $g(\tau) = f(\tau)^3$, if $m \equiv 3 \mod 8$,
  2. $g(\tau) = \left(\frac{1}{2}f(\tau)^4\right)^3$, if $m \equiv 5 \mod 8$,

are class invariants and algebraic integers.

- Similarly, there exist class invariants for $m \equiv 1, 2, 4, 6, 7 \mod 8$. 
Shimura’s reciprocity law and class invariants

Class polynomials

Class invariants

The old polynomial,

\[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432. \]

\[ -204 = -4 \cdot 51 \Rightarrow 51 \equiv 3 \mod 8 \Rightarrow g(\tau) = f(\tau)^3 \text{ is a class invariant.} \]
The old polynomial,

\[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432. \]

\(-204 = -4 \cdot 51 \Rightarrow 51 \equiv 3 \mod 8 \Rightarrow g(\tau) = f(\tau)^3 \) is a class invariant.

The new class polynomial:

\[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \]
The old polynomial,
\[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + \\
95864841637996112067555072 \cdot x^4 + \\
775121756231241041610849730560 \cdot x^3 + \\
534484930703209896960446929872814080 \cdot x^2 + \\
6020337293681148983229932704488367325184 \cdot x + \\
28508041377034538166862450172153093456658432. \]

\[ -204 = -4 \cdot 51 \Rightarrow 51 \equiv 3 \text{ mod } 8 \Rightarrow g(\tau) = f(\tau)^3 \text{ is a class invariant.} \]

The new class polynomial:
\[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \]
Shimura’s reciprocity law and class invariants

Class polynomials

Class invariants

\[
\begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix} \in \Gamma = SL(2, \mathbb{Z}) \text{ acts on } \mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \text{ by }
\]

\[
z \mapsto \frac{az+b}{cz+d}
\]

\[\Gamma(N) := \ker(SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/N\mathbb{Z})), \text{ then } X(N) \to X(1) \text{ is a Galois cover with the group } SL(2, \mathbb{Z}/N\mathbb{Z})/\pm 1\]
\[
\begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix} \in \Gamma = \text{SL}(2, \mathbb{Z}) \text{ acts on } \mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \text{ by }
\]
\[
z \mapsto \frac{az+b}{cz+d}
\]
\[
\Gamma(N) := \ker(\text{SL}(2, \mathbb{Z}) \to \text{SL}(2, \mathbb{Z}/N\mathbb{Z})), \text{ then } X(N) \to X(1) \text{ is a Galois cover with the group } \text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\pm 1
\]
\[
\Rightarrow \text{ the function field } \mathcal{F}_{N,\mathbb{C}} \text{ of } X(N) \text{ is a Galois extension of } \mathcal{F}_{1,\mathbb{C}} = \mathbb{C}(j) \text{ with the Galois group } \text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}
Shimura’s reciprocity law and class invariants

Class polynomials

Class invariants

\[
\begin{pmatrix}
  a & b \\
  c & d
\end{pmatrix} \in \Gamma = \text{SL}(2, \mathbb{Z}) \text{ acts on } \mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \text{ by}
\]

\[
z \mapsto \frac{az+b}{cz+d}
\]

\[\Gamma(N) := \ker(\text{SL}(2, \mathbb{Z}) \to \text{SL}(2, \mathbb{Z}/N\mathbb{Z})), \text{ then } X(N) \to X(1) \text{ is a Galois cover with the group } \text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}
\]

\[\Rightarrow \text{ the function field } \mathcal{F}_N,\mathbb{C} \text{ of } X(N) \text{ is a Galois extension of } \mathcal{F}_1,\mathbb{C} = \mathbb{C}(j) \text{ with the Galois group } \text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}
\]

\[\Rightarrow \text{ Passing to arithmetical modular forms, the function field } \mathcal{F}_N \text{ of modular forms having coeffs in } \mathbb{Q}(\zeta_N) \text{ is a galois extension of } \mathcal{F}_1(\zeta_N) \text{ with the Galois group } \text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}, \text{ hence } \text{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) = \text{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}
\]
Shimura’s reciprocity law and class invariants

Class polynomials

Class invariants

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \text{SL}(2, \mathbb{Z})$ acts on $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ by

$z \mapsto \frac{az+b}{cz+d}$

$\Gamma(N) := \ker(\text{SL}(2, \mathbb{Z}) \to \text{SL}(2, \mathbb{Z}/N\mathbb{Z}))$, then $X(N) \to X(1)$ is a Galois cover with the group $\text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$

$\Rightarrow$ the function field $\mathcal{F}_{N,\mathbb{C}}$ of $X(N)$ is a Galois extension of $\mathcal{F}_{1,\mathbb{C}} = \mathbb{C}(j)$ with the Galois group $\text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$

Passing to arithmetical modular forms, the function field $\mathcal{F}_N$ of modular forms having coeffs in $\mathbb{Q}(\zeta_N)$ is a galois extension of $\mathcal{F}_1(\zeta_N)$ with the Galois group $\text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, hence $\text{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) = \text{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$

Let $\mathcal{F} = \bigcup_N \mathcal{F}_N$
Shimura's reciprocity law and class invariants

Class polynomials

Class invariants

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \text{SL}(2, \mathbb{Z}) \text{ acts on } \mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \text{ by }
\]
\[z \mapsto \frac{az+b}{cz+d}\]

\[\Gamma(N) := \ker(\text{SL}(2, \mathbb{Z}) \to \text{SL}(2, \mathbb{Z}/N\mathbb{Z}))\], then \(X(N) \to X(1)\) is a Galois cover with the group \(\text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}\)

⇒ the function field \(\mathcal{F}_{N,\mathbb{C}}\) of \(X(N)\) is a Galois extension of \(\mathcal{F}_{1,\mathbb{C}} = \mathbb{C}(j)\) with the Galois group \(\text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}\)

Passing to arithmetical modular forms, the function field \(\mathcal{F}_N\) of modular forms having coeffs in \(\mathbb{Q}(\zeta_N)\) is a galois extension of \(\mathcal{F}_1(\zeta_N)\) with the Galois group \(\text{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}\), hence \(\text{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) = \text{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{\pm 1\}\)

Let \(\mathcal{F} = \bigcup_N \mathcal{F}_N\)
Shimura’s reciprocity law and class invariants

Class invariants via reciprocity law of Shimura

Exact sequences

We have

\[
\begin{align*}
\{\pm 1\} & \longrightarrow \text{SL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \text{Gal}(\mathcal{F}_N/\mathcal{F}_1(\zeta_N)) \longrightarrow 1 \\
\{\pm 1\} & \longrightarrow \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \longrightarrow 1 \\
1 & \longrightarrow (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \text{Gal}(\mathcal{F}_1(\zeta_N)/\mathcal{F}_1) \longrightarrow 1
\end{align*}
\]

Taking projective limit we obtain

\[
1 \longrightarrow \{\pm 1\} \longrightarrow \text{GL}(2, \hat{\mathbb{Z}}) \longrightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1
\]
Exact sequences

We have

\[
\begin{array}{cccccc}
\{\pm 1\} & \longrightarrow & \text{SL}(2, \mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \text{Gal}(\mathcal{F}_N/\mathcal{F}_1(\zeta_N)) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \\
\{\pm 1\} & \longrightarrow & \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^* & \longrightarrow & \text{Gal}(\mathcal{F}_1(\zeta_N)/\mathcal{F}_1) & \longrightarrow & 1 \\
\end{array}
\]

- Taking projective limit we obtain

\[
\begin{array}{cccccc}
1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \text{GL}(2, \hat{\mathbb{Z}}) & \longrightarrow & \text{Gal}(\mathcal{F}/\mathcal{F}_1) & \longrightarrow & 1 \\
\end{array}
\]

- On the other side the main thm of CM implies

\[
\begin{array}{cccccc}
1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \hat{\mathcal{O}}^* = \prod_p \mathcal{O}_p^* & \overset{A}{\longrightarrow} & \text{Gal}(K^{ab}/H) & \longrightarrow & 1 \\
\end{array}
\]
Exact sequences

We have

\[
\{\pm 1\} \longrightarrow \text{SL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \text{Gal}(\mathcal{F}_N/\mathcal{F}_1(\zeta_N)) \longrightarrow 1
\]

\[
\{\pm 1\} \longrightarrow \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \longrightarrow 1
\]

\[
1 \longrightarrow (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \text{Gal}(\mathcal{F}_1(\zeta_N)/\mathcal{F}_1) \longrightarrow 1
\]

Taking projective limit we obtain

\[
1 \longrightarrow \{\pm 1\} \longrightarrow \text{GL}(2, \hat{\mathbb{Z}}) \longrightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1
\]

On the other side the main thm of CM implies

\[
1 \longrightarrow \mathcal{O}^* \longrightarrow \hat{\mathcal{O}}^* = \prod_p \mathcal{O}_p^* \overset{A}{\longrightarrow} \text{Gal}(K^{ab}/H) \longrightarrow 1
\]
The Shimura’s reciprocity law map connects these two sequences:

\[ 1 \rightarrow \mathcal{O}^* \rightarrow \prod_p \mathcal{O}_p^* \rightarrow \text{Gal}(K^{ab}/H) \rightarrow 1 \]

\[ 1 \rightarrow \{\pm 1\} \rightarrow \text{GL}(2, \hat{\mathbb{Z}}) \rightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \rightarrow 1 \]

with \( f(\tau)^x = (f(\tau)^{h_\tau(x^{-1})})(\tau) \) and \( (f(\tau))^x = f(\tau) \iff f^{h_\tau(x)} = f \).

Reducing the diagram by the second main thm of CM:

\[ \mathcal{O}^* \rightarrow (\mathcal{O}/N\mathcal{O})^* \rightarrow \text{Gal}(K(F_N(\tau))/H) \rightarrow 1 \]

\[ \{\pm 1\} \rightarrow \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \rightarrow \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \rightarrow 1 \]
The Shimura’s reciprocity law map connects these two sequences:

\[
1 \longrightarrow \mathcal{O}^* \longrightarrow \prod_p \mathcal{O}_p^* \longrightarrow \text{Gal}(K^{ab}/H) \longrightarrow 1
\]

\[
1 \longrightarrow \{\pm 1\} \longrightarrow \text{GL}(2, \widehat{\mathbb{Z}}) \longrightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1
\]

with \( f(\tau)^x = (f(\tau)^{h_\tau}(x^{-1}))(\tau) \) and \( (f(\tau))^x = f(\tau) \iff f^{h_\tau}(x) = f \).

Reducing the diagram by the second main thm of CM:

\[
\mathcal{O}^* \longrightarrow (\mathcal{O}/N\mathcal{O})^* \longrightarrow \text{Gal}(K(F_N(\tau))/H) \longrightarrow 1
\]

\[
\{\pm 1\} \longrightarrow \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \longrightarrow 1
\]

Let \( g \) be a function of some level \( N \). Then \( g \) is a class invariant iff

\[
h_{\tau,N}(((\mathcal{O}/N\mathcal{O})^*)) = \{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \} \text{ acts trivially on } g, \text{ where } X^2 + AX + B \text{ the min poly of } \tau
\]
The Shimura’s reciprocity law map connects these two sequences:

\[
1 \longrightarrow \mathcal{O}^* \longrightarrow \prod_p \mathcal{O}_p^* \longrightarrow \text{Gal}(K^{ab}/H) \longrightarrow 1
\]

\[
h_\tau
\]

\[
1 \longrightarrow \{\pm 1\} \longrightarrow \text{GL}(2, \hat{\mathbb{Z}}) \longrightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1
\]

with \( f(\tau)^x = (f(\tau)^{h_\tau(x^{-1})})(\tau) \) and \((f(\tau))^x = f(\tau) \iff f^{h_\tau(x)} = f\).

Reducing the diagram by the second main thm of CM:

\[
\mathcal{O}^* \longrightarrow (\mathcal{O}/N\mathcal{O})^* \longrightarrow \text{Gal}(K(F_N(\tau))/H) \longrightarrow 1
\]

\[
h_{\tau,N}
\]

\[
\{\pm 1\} \longrightarrow \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \longrightarrow 1
\]

Let \( g \) be a function of some level \( N \). Then \( g \) is a class invariant iff

\[
h_{\tau,N}((\mathcal{O}/N\mathcal{O})^*) = \left\{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \right\} \text{ acts trivially on } g, \text{ where } X^2 + AX + B \text{ the min poly of } \tau
\]
If we replace the base field with a field of discriminant having the same residue class modulo $4N$, the integers $B, C$ and the image of $h_{\tau,N}$ are the same modulo $N$.

$\Rightarrow$ For a positive proportion of imaginary quadratic fields, we have the class invariant $g$, if it is for one of them a class invariant.
If we replace the base field with a field of discriminant having the same residue class modulo $4N$, the integers $B$, $C$ and the image of $h_{\tau,N}$ are the same modulo $N$

$\Rightarrow$ For a positive proportion of imaginary quadratic fields, we have the class invariant $g$, if it is for one of them a class invariant

- **Complexity:** improvement by a constant factor (e.g. 48, 72) in the height of coeffs of descent generating polys enables the computation feasible, and yields efficient applications in ECPP, pairing based constructions etc.
If we replace the base field with a field of discriminant having the same residue class modulo $4N$, the integers $B, C$ and the image of $h_{\tau,N}$ are the same modulo $N$

⇒ For a **positive proportion** of imaginary quadratic fields, we have the class invariant $g$, if it is for one of them a class invariant

- **Complexity**: improvement by a constant factor (e.g. 48, 72) in the height of coeffs of descent generating polys enables the computation feasible, and yields efficient applications in ECPP, pairing based constructions etc.

- **Optimality, (Kim 03)**: lower bound on 'Selberg’s eigenvalue’ $\lambda_1$,

- **Stevenhagen et. at.** $r(g) = \frac{\deg_f \Phi(j,g)}{\deg_j \Phi(j,g)} \leq 1/(24\lambda_1)$. 
If we replace the base field with a field of discriminant having the same residue class modulo $4N$, the integers $B, C$ and the image of $h_{\tau, N}$ are the same modulo $N$

⇒ For a **positive proportion** of imaginary quadratic fields, we have the class invariant $g$, if it is for one of them a class invariant

- **Complexity:** improvement by a constant factor (e.g. 48, 72) in the height of coeffs of descent generating polys enables the computation **feasible**, and yields efficient applications in ECPP, pairing based constructions etc.
- **Optimality, (Kim 03):** lower bound on 'Selberg’s eigenvalue' $\lambda_1$,
- **Stevenhagen et. at.** $r(g) = \frac{\deg_f \Phi(j, g)}{\deg_j \Phi(j, g)} \leq \frac{1}{24\lambda_1}$.

⇒ A proven upper bound 100.82 and a conjectural upper bound 96 for $r(g)$

⇒ $r(f_2) = 72$. Hence for a positive proportion of fields we have 'fast' optimal class invariants.
If we replace the base field with a field of discriminant having the same residue class modulo $4N$, the integers $B$, $C$ and the image of $h_{\tau,N}$ are the same modulo $N$

$\Rightarrow$ For a positive proportion of imaginary quadratic fields, we have the class invariant $g$, if it is for one of them a class invariant

- **Complexity:** improvement by a constant factor (e.g. 48, 72) in the height of coeffs of descent generating polys enables the computation feasible, and yields efficient applications in ECPP, pairing based constructions etc.

- **Optimality, (Kim 03):** lower bound on 'Selberg’s eigenvalue’ $\lambda_1$,

- **Stevenhagen et. at.** $r(g) = \frac{\deg_f \Phi(j,g)}{\deg_j \Phi(j,g)} \leq 1/(24\lambda_1)$.

$\Rightarrow$ A proven upper bound 100.82 and a conjectural upper bound 96 for $r(g)$

$\Rightarrow r(f_2) = 72$. Hence for a positive proportion of fields we have 'fast' optimal class invariants.
Theta functions

For $\tau \in \mathbb{H}_2 := \{ \tau \in M(2, \mathbb{C}) : \tau \text{ symmetric, } \Im(\tau) \text{ positive definite} \}$ and $\delta, \epsilon \in (\mathbb{Z}/2\mathbb{Z})^g$ we have the Thetanullwerte

$$\theta_{\delta \epsilon}(z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp \left( \pi i \left[ (n + \frac{1}{2} \delta)^t \Omega (n + \frac{1}{2} \delta) + 2(n + \frac{1}{2} \delta)^t (z + \frac{1}{2} \epsilon) \right] \right),$$

odd Thetanullwerte $\delta^t \epsilon \equiv 1 \mod 2 \Rightarrow 2^{g-1}(2^g - 1)$ of them

even Thetanullwerte $\delta^t \epsilon \equiv 1 \mod 2 \Rightarrow 2^{g-1}(2^g + 1)$ of them

- The Jacobi theta functions $\theta_{00}(\tau), \theta_{10}(\tau), \theta_{01}(\tau), \theta_{11}(\tau)$ are the 'Thetanullwerte' for $g = 1$.

- Modified Schläfli functions:
  $$\mathfrak{F}(\tau) := \frac{2\theta_{00}(\tau)^2}{\theta_{01}(\tau)\theta_{10}(\tau)}, \quad \mathfrak{F}_1(\tau) := \frac{2\theta_{01}(\tau)^2}{\theta_{00}(\tau)\theta_{10}(\tau)}, \quad \mathfrak{F}_2(\tau) := \frac{2\theta_{10}(\tau)^2}{\theta_{00}(\tau)\theta_{01}(\tau)}.$$

- U.: We have $\mathfrak{F}(\tau) = f(\tau)^6$, $\mathfrak{F}_1(\tau) = f_1(\tau)^6$ and $\mathfrak{F}_2(\tau) = f_2(\tau)^6$
Shimura’s reciprocity law and class invariants

Class invariants as quotients of 'Thetanullwerten'

Complexity

▶ **U.:** \( g(\tau) = \frac{1}{8} \bar{\psi}^2 \) is a class invariant and algebraic integer, if \( m \equiv 5 \mod 8 \).

▶ **Dupont (2007):** Complexity \( O(M(N) \log N) \).
Complexity

- **U.:** \( g(\tau) = \frac{1}{8} \zeta^2 \) is a class invariant and algebraic integer, if \( m \equiv 5 \mod 8 \).

- **Dupont (2007):** Complexity \( O(\mathcal{M}(N) \log N) \).

- **Dupont (2007):** \( \eta^{12} \) has also \( O(\mathcal{M}(N) \log N) \).
Complexity

- **U.:** $g(\tau) = \frac{1}{8} \zeta^2$ is a class invariant and algebraic integer, if $m \equiv 5 \mod 8$.
- **Dupont (2007):** Complexity $O(\mathcal{M}(N) \log N)$.
- **Dupont (2007):** $\eta^{12}$ has also $O(\mathcal{M}(N) \log N)$.
- **Extra:** We need to find the 12th root of $\eta^{12}$, for example by Newton iteration.
Complexity

- **U.:** \( g(\tau) = \frac{1}{8} \bar{S}^2 \) is a class invariant and algebraic integer, if \( m \equiv 5 \mod 8 \).

- **Dupont (2007):** Complexity \( O(\mathcal{M}(N) \log N) \).

- **Dupont (2007):** \( \eta^{12} \) has also \( O(\mathcal{M}(N) \log N) \).

- **Extra:** We need to find the 12th root of \( \eta^{12} \), for example by Newton iteration.
Motivation

$W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64$.

Now considering the coefficients:

\[
\begin{array}{cccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 \\
\end{array}
\]

\[1 - 16 - 12 + 48 + 144 + 64 + 64 = 2^6\]
Motivation

- $W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64.$
- Now considering the coefficients:

$$
\begin{array}{ccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6
\end{array}
$$
Motivation

- $W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64$.
- Now considering the coefficients:

$$
\begin{array}{ccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6 \\
1 & -2 \cdot 8 & -2^2 \cdot 3 & \\
\end{array}
$$
Motivation

- \( W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \)
- Now considering the coefficients:

\[
\begin{array}{cccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 & = 2^6 \\
1 & -2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & & & &
\end{array}
\]
Motivation

\[ W_{-204}(x) = x^6 - 16x^5 - 12x^4 + 48x^3 + 144x^2 + 64x + 64. \]

Now considering the coefficients:

\[
\begin{array}{cccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6 \\
1 & -2^2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & +2^4 \cdot 9
\end{array}
\]
Motivation

\[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \]

Now considering the coefficients:

\[ \begin{array}{cccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6 \\
1 & -2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & +2^4 \cdot 9 & +2^5 \cdot 2 \\
\end{array} \]
Motivation

\[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \]

Now considering the coefficients:

\[
\begin{array}{cccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6 \\
1 & -2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & +2^4 \cdot 9 & +2^5 \cdot 2 & +2^6 \cdot 1
\end{array}
\]
Motivation

$W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64.$

Now considering the coefficients:

\[
\begin{array}{cccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6 \\
1 & -2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & +2^4 \cdot 9 & +2^5 \cdot 2 & +2^6 \cdot 1 \\
1 & -8 & -3 & +6 & +9 & +2 & +1
\end{array}
\]
Motivation

\[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \]

Now considering the coefficients:

\[
\begin{array}{cccccccc}
1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6 \\
1 & -2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & +2^4 \cdot 9 & +2^5 \cdot 2 & +2^6 \cdot 1 \\
1 & -8 & -3 & +6 & +9 & +2 & +1
\end{array}
\]

The new polynomial:

\[ W'_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1. \]
Motivation

- \( W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \)

- Now considering the coefficients:

  \[
  \begin{array}{cccccccc}
  1 & -16 & -12 & +48 & +144 & +64 & +64 = 2^6 \\
  1 & -2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & +2^4 \cdot 9 & +2^5 \cdot 2 & +2^6 \cdot 1 \\
  1 & -8 & -3 & +6 & +9 & +2 & +1 \\
  \end{array}
  \]

- The new polynomial:
  \( W'_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1. \)

- Is it possible to use \( \frac{g(\tau)}{2} \) as a class invariant instead of \( g(\tau) \) for \( m \equiv 3 \mod 8 \)?
Motivation

- \( W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64. \)

- Now considering the coefficients:

<table>
<thead>
<tr>
<th>1</th>
<th>-16</th>
<th>-12</th>
<th>+48</th>
<th>+144</th>
<th>+64</th>
<th>+64</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-2 \cdot 8</td>
<td>-2^2 \cdot 3</td>
<td>+2^3 \cdot 6</td>
<td>+2^4 \cdot 9</td>
<td>+2^5 \cdot 2</td>
<td>+2^6 \cdot 1</td>
</tr>
<tr>
<td>1</td>
<td>-8</td>
<td>-3</td>
<td>+6</td>
<td>+9</td>
<td>+2</td>
<td>+1</td>
</tr>
</tbody>
</table>

- The new polynomial:
  \( W'_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1. \)

- Is it possible to use \( \frac{g(\tau)}{2} \) as a class invariant instead of \( g(\tau) \) for \( m \equiv 3 \mod 8 \)? If yes, are they always units?
Motivation

- \( W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64 \).
- Now considering the coefficients:
  
  \[
  \begin{array}{cccccccc}
    1 & -16 & -12 & +48 & +144 & +64 & +64 &= 2^6 \\
    1 & -2 \cdot 8 & -2^2 \cdot 3 & +2^3 \cdot 6 & +2^4 \cdot 9 & +2^5 \cdot 2 & +2^6 \cdot 1 \\
    1 & -8 & -3 & +6 & +9 & +2 & +1
  \end{array}
  \]

- The new polynomial:
  \( W'_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1 \).
- Is it possible to use \( \frac{g(\tau)}{2} \) as a class invariant instead of \( g(\tau) \) for \( m \equiv 3 \mod 8 \)? If yes, are they always units?
Class units

**Theorem, U.:** Let \( g(\tau) \) be one of the class invariants introduced as above.

1. \( g(\tau) \) is a unit, hence we say **class unit**, if we have \( m \equiv 1, 5, 7 \mod 8 \) and \( m \equiv 2 \mod 4 \)
2. Splitting the case \( m \equiv 3 \mod 8 \) into three parts, we have:
   2.1 \( g(\tau)/2 \) is a class invariant and a unit, if \( m \equiv 3 \mod 24 \),
   2.2 \( g(\tau) \) has the norm \( 2^l \) with \( h_t = 3l \) if \( m \equiv 11, 19 \mod 24 \).
3. Similarly splitting the last case \( m \equiv 4 \mod 8 \) into two parts, we have
   3.1 \( g(\tau) \) is a unit, if \( m \equiv 4 \mod 16 \),
   3.2 In the last case \( m \equiv 12 \mod 16 \), we write \( m = 16k + 12 \).

Then have 6 more cases:

- \( g(\tau) \) has the norm \( 2^l \) with \( h = 2l \) if \( k \equiv 0, 1, 5 \mod 6 \),
- \( g(\tau) \) has the norm \( 2^l \) with \( h = 6l \) if \( k \equiv 2, 4 \mod 6 \),
- \( g(\tau)/2 \) is a class invariant with the norm \( 2^l \) with \( h = 2l \) if \( k \equiv 3 \mod 6 \).
Example once more

- **the oldest polynomial**
  \[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432, \]

- **class polynomial of Weber**
  \[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64, \]
Example once more

- **the oldest polynomial**
  \[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432, \]

- **class polynomial of Weber**
  \[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64, \]

- **new class polynomial**
  \[ W'_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1. \]
Example once more

- **the oldest polynomial**
  \[ H_{-204}(x) = x^6 - 30703802307926880672 \cdot x^5 + 95864841637996112067555072 \cdot x^4 + 775121756231241041610849730560 \cdot x^3 + 534484930703209896960446929872814080 \cdot x^2 + 6020337293681148983229932704488367325184 \cdot x + 28508041377034538166862450172153093456658432, \]

- **class polynomial of Weber**
  \[ W_{-204}(x) = x^6 - 16 \cdot x^5 - 12 \cdot x^4 + 48 \cdot x^3 + 144 \cdot x^2 + 64 \cdot x + 64, \]

- **new class polynomial**
  \[ W'_{-204}(x) = x^6 - 8 \cdot x^5 - 3 \cdot x^4 + 6 \cdot x^3 + 9 \cdot x^2 + 2 \cdot x + 1. \]
The field $K(j(\tau))$ has the unit rank $h_t - 1$.

$E$: unit group of $\mathcal{O}_{K(j(\tau))}$. 
The field $K(j(\tau))$ has the unit rank $h_t - 1$.

$E$ : unit group of $\mathcal{O}_{K(j(\tau))}$.

$h_t - 1$ class units as roots of the same class polynomial (with roots of unity) form a subgroup $H$. 
The field $K(j(\tau))$ has the unit rank $h_t - 1$.

$E$ : unit group of $\mathcal{O}_{K(j(\tau))}$.

$h_t - 1$ class units as roots of the same class polynomial (with roots of unity) form a subgroup $H$.

$[E : H] = \det(\mathcal{R})/R$

1. $\mathcal{R}$ regulator matrix with $ij$–th entry $\log |g_i(\tau)(j)|^2$. 

$\mathcal{R}$ the regulator of $K(j(\tau))$. 

$\Rightarrow$ upper bound $B$ for $[E : H]$.

Hajir: For $p^e_i \leq B$, determine the maximal $e_i^p$ of $p^e_i$ together with the new subgroup $U$ with the index $[E : H]/p^e_i = \Rightarrow$ Construct step by step fundamental units explicitly.
The field $K(j(\tau))$ has the unit rank $h_t - 1$.  
$E$: unit group of $\mathcal{O}_{K(j(\tau))}$.  
$h_t - 1$ class units as roots of the same class polynomial (with roots of unity) form a subgroup $H$.  
$[E : H] = \det(\mathcal{R})/R$

1. $\mathcal{R}$ regulator matrix with $ij$–th entry $\log |g_i(\tau)^{(j)}|^2$,  
2. $R$ the regulator of $K(j(\tau))$.  

lower regulator bound (Pohst, et al) $\Rightarrow$ upper bound $B$ for $[E : H]$.  
Hajir: For $p_i \leq B$, determine the maximal $e_i$ of $p_i$ together with the new subgroup $U$ with the index $[E : H]/p_i^{e_i} = \Rightarrow$ Construct step by step fundamental units explicitely.
The field $K(j(\tau))$ has the unit rank $h_t - 1$.

$E$: unit group of $\mathcal{O}_{K(j(\tau))}$.

$h_t - 1$ class units as roots of the same class polynomial (with roots of unity) form a subgroup $H$.

$[E : H] = \det(\mathcal{R})/R$

1. $\mathcal{R}$ regulator matrix with $ij$–th entry $\log |g_i(\tau)^{(j)}|^2$,
2. $R$ the regulator of $K(j(\tau))$.

lower regulator bound (Pohst, et al)

$\Rightarrow$ upper bound $B$ for $[E : H]$. 
The field $K(j(\tau))$ has the unit rank $h_t - 1$.

$E$ : unit group of $\mathcal{O}_{K(j(\tau))}$.

$h_t - 1$ class units as roots of the same class polynomial (with roots of unity) form a subgroup $H$.

$[E : H] = \det(\mathcal{R})/R$

1. $\mathcal{R}$ regulator matrix with $ij$–th entry $\log |g_i(\tau)^{(j)}|^2$,
2. $R$ the regulator of $K(j(\tau))$.

**lower regulator bound (Pohst, et al)**

$\Rightarrow$ upper bound $B$ for $[E : H]$.

**Hajir**: For $p_i \leq B$, determine the maximal $e_i$ of $p_i$ together with the new subgroup $U$ with the index $[E : H]/p_i^{e_i}$.

$\implies$ Construct step by step fundamental units explicitly.
The field $K(j(\tau))$ has the unit rank $h_t - 1$.

$E$ : unit group of $\mathcal{O}_{K(j(\tau))}$.

$h_t - 1$ class units as roots of the same class polynomial (with roots of unity) form a subgroup $H$.

$[E : H] = \det(\mathcal{R})/R$

1. $\mathcal{R}$ regulator matrix with $ij$–th entry $\log |g_i(\tau)^{(j)}|^2$,
2. $R$ the regulator of $K(j(\tau))$.

**lower regulator bound (Pohst, et al)**

⇒ upper bound $B$ for $[E : H]$.

**Hajir**: For $p_i \leq B$, determine the maximal $e_i$ of $p_i$ together with the new subgroup $U$ with the index $[E : H]/p_i^{e_i}$.

⇒⇒ Construct step by step fundamental units explicitely.
An example

\[ W'_{-204}(x) = x^6 - 8x^5 - 3x^4 + 6x^3 + 9x^2 + 2x + 1. \]

The lower regulator bound with KANT/KASH is 43.3706.
An example

- \( W'_{-204}(x) = x^6 - 8x^5 - 3x^4 + 6x^3 + 9x^2 + 2x + 1. \)
- The lower regulator bound with KANT/KASH is 43.3706.
- 74.6592 is the numerical value of \( \det(\mathcal{R}) \).
An example

- $W'_{-204}(x) = x^6 - 8x^5 - 3x^4 + 6x^3 + 9x^2 + 2x + 1$.
- The lower regulator bound with KANT/KASH is $43.3706$.
- $74.6592$ is the numerical value of $\det(R)$.
- $B = 1.7214 \Rightarrow$ class units together with roots of unity form the unit group of $\mathcal{O}_K(j(\tau))$. 
Shimura’s reciprocity law and class invariants

An example

▪ $W'_{-204}(x) = x^6 - 8x^5 - 3x^4 + 6x^3 + 9x^2 + 2x + 1$.
▪ The lower regulator bound with KANT/KASH is $43.3706$.
▪ $74.6592$ is the numerical value of $\det(\mathcal{R})$.
▪ $B = 1.7214 \Rightarrow$ class units together with roots of unity form the unit group of $\mathcal{O}_K(j(\tau))$. 
Preliminaries

- $K$: a **primitive** totally imaginary quadratic extension of a real quadratic field $K_0$
- $\Phi = (\phi_1, \phi_2)$ is the type of $K$ (or the corresponding abelian surface), and $K^r$ is the reflex field of $K$ with the type $\Psi = (\psi_1, \psi_2)$
- An abelian surface is **simple** if it is not isogenous to product of elliptic curves, and equivalently if $K$ is primitive, i.e. $K$ is cyclic are non-Galois over $\mathbb{Q}$.
- If $I$ is an $\mathcal{O}_K$ ideal, then the quotient $A = \mathbb{C}^2/\Phi(I)$ is an abelian surface of type $\Phi$
- The dual variety $A^* = \mathbb{C}^2/\Phi(\mathcal{O}_K^{-1}I)$
- If Steinitz class of $K$ is a principal ideal, then $A \cong A^*$ and $A$ is said to be principally polarizable.
Every principally polarized abelian surface, ppas, over $\mathbb{C}$ is of the form $A_\tau = \mathbb{C}^2/\mathbb{Z}^2 + \mathbb{Z}^2 \tau$.

The moduli space of ppas has dimension 3 with the coordinates $j_1, j_2, j_3$, which are quotients of polynomials of 10 even Thetanullwerte for genus 2 evaluated at $\tau$.

We have $s$ isomorphism classes of ppas with CM by $\mathcal{O}_K$ with $s = h_K$, if $K$ Galois and $s = 2h_K$, if dihedral.

As in $g = 1$ we can construct the class polynomials for $i = 1, 2, 3$

$$H_i(X) = \prod_{j=1}^{s}(X - j_i(\tau_j)) \in \mathbb{Q}[X]$$
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Hyperelliptic Curves with CM

- **Shimura, Taniyama:** The field $K^r(j_1, j_2, j_3)$ is a subfield of Hilbert class field $H^r$ of $K^r$, generically proper

- **Goren et. al:** There is a bound on the denominators of $H_i(X)$
Shimura’s reciprocity law and class invariants
Class invariants for genus 2 (in progress)
Hyperelliptic Curves with CM

Shimura, Taniyama: The field $K^r(j_1, j_2, j_3)$ is a subfield of Hilbert class field $H^r$ of $K^r$, generically proper

Goren et. al: There is a bound on the denominators of $H_i(X)$

Streng: $H_i$ can be computed in $\tilde{O}(\Delta^{7/2})$, $\Delta$ discriminant of $K$
Shimura, Taniyama: The field $K_r(j_1, j_2, j_3)$ is a subfield of Hilbert class field $H_r$ of $K_r$, generically proper

Goren et. al: There is a bound on the denominators of $H_i(X)$

Streng: $H_i$ can be computed in $\tilde{O}(\Delta^{7/2})$, $\Delta$ discriminant of $K$

Kohel et. al: Database for $H_i$ and 2–adic and 3–adic canonical lifting algorithms to compute $H_i$
Shimura’s reciprocity law and class invariants
Class invariants for genus 2 (in progress)
Hyperelliptic Curves with CM

- **Shimura, Taniyama:** The field $K^r(j_1, j_2, j_3)$ is a subfield of Hilbert class field $H^r$ of $K^r$, generically proper
- **Goren et. al:** There is a bound on the denominators of $H_i(X)$
- **Streng:** $H_i$ can be computed in $\tilde{O}(\Delta^{7/2})$, $\Delta$ discriminant of $K$
- **Kohel et. al:** Database for $H_i$ and 2–adic and 3–adic canonical lifting algorithms to compute $H_i$
- **Question 1:** Is it possible to find a system of modular functions $g_i$ of some level $N$ with $K^r(j_1, j_2, j_3) = K^r(g_1, g_2, g_3)$?
- **Question 2:** Is it possible to obtain a system of class invariants $g_i$ having class polynomials with rational coefficients?
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Hyperelliptic Curves with CM

- **Shimura, Taniyama:** The field $K^r(j_1, j_2, j_3)$ is a subfield of Hilbert class field $H^r$ of $K^r$, generically proper

- **Goren et. al:** There is a bound on the denominators of $H_i(X)$

- **Streng:** $H_i$ can be computed in $\widetilde{O}(\Delta^{7/2})$, $\Delta$ discriminant of $K$

- **Kohel et. al:** Database for $H_i$ and 2—adic and 3—adic canonical lifting algorithms to compute $H_i$

- **Question 1:** Is it possible to find a system of modular functions $g_i$ of some level $N$ with $K^r(j_1, j_2, j_3) = K^r(g_1, g_2, g_3)$?

- **Question 2:** Is it possible to obtain a system of class invariants $g_i$ having class polynomials with rational coefficients?
Kronecker: $\mathbb{Q}(j) = \mathbb{Q}(\theta_{10}(2\tau)/\theta_{00}(2\tau), \tau \in \mathbb{H})$ and $\mathcal{F}_N$ is gen’d by the functions

$$
\theta_{11}(2\tau, 2(\tau \cdot h' + h))/\theta_{01}(2\tau, 2(\tau \cdot h' + h))
$$

with $(h', h) \in \frac{1}{N}\mathbb{Z}^2$

$\Gamma(2, 4)$ is the subgroup of the full Siegel modular group $\Gamma = \text{Sp}(4, \mathbb{Z})$ whose elements $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ have the properties

$$
M \equiv 1_4 \mod 2 \text{ and } \{a^tb\} = \{c^td\} \equiv 0 \mod 4
$$
Kronecker: \( \mathbb{Q}(j) = \mathbb{Q}(\theta_{10}(2\tau)/\theta_{00}(2\tau), \tau \in \mathbb{H}) \) and \( \mathcal{F}_N \) is gen’d by the functions

\[
\theta_{11}(2\tau, 2(\tau \cdot h' + h))/\theta_{01}(2\tau, 2(\tau \cdot h' + h))
\]

with \((h', h) \in \frac{1}{N}\mathbb{Z}^2\)

\(\Gamma(2, 4)\) is the subgroup of the full Siegel modular group \( \Gamma = \text{Sp}(4, \mathbb{Z}) \) whose elements \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) have the properties

\( M \equiv 1_4 \mod 2 \) and \( \{a^t b\} = \{c^t d\} \equiv 0 \mod 4 \)
Three quotients $k_a(\tau) = \theta_{a0}(2\tau)/\theta_{00}(2\tau)$ for $a(\neq 0) \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$, say $a = (1, 0), (0, 1), (1, 1)$, form a set of generators for the field of modular functions relative to $\Gamma(2, 4)$, say in analogy $\mathcal{F}_1$.

$\mathcal{F}_N$ is the field

$$\mathbb{Q}\left(k_a(\tau, (\tau, 12h)) : a \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2, h \in \frac{1}{N}\mathbb{Z}^4/\mathbb{Z}^4 \right)$$

with

$$k_a(\tau, (\tau, 12h)) = \theta_{a0}(2\tau, 2(\tau, 12))/{\theta_{00}(2\tau, 2(\tau h_1 + h_2))}$$
Three quotients \( k_a(\tau) = \theta_{a0}(2\tau)/\theta_{00}(2\tau) \) for \( a(\neq 0) \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2 \), say \( a = (1,0), (0,1), (1,1) \), form a set of generators for the field of modular functions relative to \( \Gamma(2,4) \), say in analogy \( \mathcal{F}_1 \)

\( \mathcal{F}_N \) is the field

\[
\mathbb{Q} \left( k_a(\tau, (\tau, 1_2 h)) : a \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2, h \in \frac{1}{N}\mathbb{Z}^4/\mathbb{Z}^4 \right)
\]

with

\[
k_a(\tau, (\tau, 1_2 h)) = \theta_{a0}(2\tau, 2(\tau, 1_2))/\theta_{00}(2\tau, 2(\tau h_1 + h_2))
\]
Sasaki's result: 

\( \zeta_N \in \mathcal{F}_N \), \( \mathbb{Q}(\zeta_N) \) is algebraically closed in \( \mathbb{F}_N \)

\( \text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong U := (\text{Sp}(4, \mathbb{Z}/N\mathbb{Z})) / \{\pm 1\} \rtimes (\mathbb{Z}/N\mathbb{Z})^* \)

Hence for \( \mathcal{F} = \bigcup_N \mathcal{F}_N \), we have

\[
1 \longrightarrow \{\pm 1\} \longrightarrow \hat{U} \longrightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1
\]

with \( \hat{U} < \text{Gl}(4, \hat{\mathbb{Z}}) \)
Shimura's reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Sasaki's result

- **Sasaki:** $\zeta_N \in \mathcal{F}_N$, $\mathbb{Q}(\zeta_N)$ is algebraically closed in $\mathbb{F}_N$
- $\text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong U := (\text{Sp}(4, \mathbb{Z}/N\mathbb{Z})) / \{\pm 1\} \rtimes (\mathbb{Z}/N\mathbb{Z})^*$
- **Hence for** $\mathcal{F} = \bigcup_N \mathcal{F}_N$, we have

  $1 \longrightarrow \{\pm 1\} \longrightarrow \hat{U} \longrightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1$

  with $\hat{U} < \text{Gl}(4, \hat{\mathbb{Z}})$

- **Sasaki:** By Riemann addition formula $\mathcal{F}_1$ is

  $\mathbb{Q}(\theta_{ab}(\tau)^2 / \theta_{cd}(\tau)^2 : ab, bd \text{ even})$ and every ppas is isomorphic to an another defined over $\mathcal{F}_1$. 
Sasaki: $\zeta_N \in \mathcal{F}_N$, $\mathbb{Q}(\zeta_N)$ is algebraically closed in $\mathbb{F}_N$

$\text{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong U := (\text{Sp}(4, \mathbb{Z}/N\mathbb{Z})) / \{\pm 1\} \rtimes (\mathbb{Z}/N\mathbb{Z})^*$

Hence for $\mathcal{F} = \bigcup_N \mathcal{F}_N$, we have

$$1 \longrightarrow \{\pm 1\} \longrightarrow \hat{U} \longrightarrow \text{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1$$

with $\hat{U} < \text{Gl}(4, \hat{\mathbb{Z}})$

Sasaki: By Riemann addition formula $\mathcal{F}_1$ is $\mathbb{Q}(\theta_{ab}(\tau)^2 / \theta_{cd}(\tau)^2 : ab, bd$ even) and every ppas is isomorphic to another defined over $\mathcal{F}_1$. 
For a number field $K$, we have by class field theory

$$1 \rightarrow \mathcal{O}_K^* \rightarrow \hat{\mathcal{O}}_K^* \times \prod_{p \text{ real}} < -1 >^A \rightarrow \text{Gal}(K^{ab}/K) \rightarrow \text{Cl}_K \rightarrow 1$$

The image under the Artin map $A$ is $\text{Gal}(H/K)$. Since $K'$ is totally imaginary the Artin map is trivial on the infinite part.
For a number field $K$, we have by class field theory

$$1 \rightarrow \mathcal{O}_K^* \rightarrow \hat{\mathcal{O}}_K^* \times \prod_{p \text{ real}} < -1 > \xrightarrow{A} \text{Gal}(K^{ab}/K) \rightarrow \text{Cl}_K \rightarrow 1$$

The image under the Artin map $A$ is $\text{Gal}(H/K)$. Since $K^r$ is totally imaginary the Artin map is trivial on the infinite part.

For simplicity write $F = K^r$,

$\mathbb{A}$, ring of rational adeles, $\mathbb{A}_f$ its finite part, $F_\mathbb{A}^*$, idele group of $F$, and we consider $F^*$ as embedded in $F_\mathbb{A}^*$. Further, we write the Artin map $A = [s, K]$ for $s \in F_\mathbb{A}^*$. 
For a number field $K$, we have by class field theory

$$1 \to \mathcal{O}_K^* \to \hat{\mathcal{O}}_K^* \times \prod_{p \text{ real}} < -1 >^A \to \text{Gal}(K^{ab}/K) \to \text{Cl}_K \to 1$$

The image under the Artin map $A$ is $\text{Gal}(H/K)$. Since $K^r$ is totally imaginary the Artin map is trivial on the infinite part.

For simplicity write $F = K^r$.

$\mathbb{A}$, ring of rational adeles, $\mathbb{A}_f$ its finite part, $F^*_\mathbb{A}$, idele group of $F$, and we consider $F^*$ as embedded in $F^*_\mathbb{A}$. Further, we write the Artin map $A = [s, K]$ for $s \in F^*_\mathbb{A}$. 
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Higher order reciprocity law of Shimura

\[ G_{A^+} := \{ \gamma \in \text{Gl}(4, \mathbb{A}) : \gamma^t J \gamma = v(\gamma)J, v(\gamma) \in \mathbb{A}^*, v(\gamma)_\infty > 0 \} \]

and \( G_{\mathbb{Q}^+} := G_{A^+} \cap \text{Gl}(4, \mathbb{Q}) \) with \( J = \begin{pmatrix} 0 & -1_2 \\ 1_2 & 0 \end{pmatrix} \)

There is an associative right action of \( G_{A^+} \) on the arithmetical modular forms of weight \( k \), \( f \rightarrow f^u \) with \( u \in G_{A^+} \) with the properties:

\[ f^\gamma = \text{det}(c \tau + d)^{-k} f(\gamma(\tau)) \text{ for } \gamma \in G_{\mathbb{Q}^+}, \]

\[ f^{i(t)} = f[t, \mathbb{Q}] \text{ with } i(t) = \begin{pmatrix} 1_2 & 0 \\ 0 & t^{-1}1_2 \end{pmatrix}, t \in \hat{\mathbb{Z}}^*, \]

The subgroup of \( G_{A^+} \) fixing \( f \) is open
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Higher order reciprocity law of Shimura

\[ G_{\mathbb{A}+} := \{ \gamma \in \text{Gl}(4, \mathbb{A}) : \gamma^t J \gamma = v(\gamma) J, v(\gamma) \in \mathbb{A}^*, v(\gamma)_\infty > 0 \} \]

and \[ G_{\mathbb{Q}+} := G_{\mathbb{A}+} \cap \text{Gl}(4, \mathbb{Q}) \]

with \[ J = \begin{pmatrix} 0 & -12 \\ 12 & 0 \end{pmatrix} \]

There is an associative right action of \( G_{\mathbb{A}+} \) on the arithmetical modular forms of weight \( k \), \( f \rightarrow f^u \) with \( u \in G_{\mathbb{A}+} \) with the properties:

\[ f^\gamma = \det(c\tau + d)^{-k} f(\gamma(\tau)) \] for \( \gamma \in G_{\mathbb{Q}+} \),

\[ f^i(t) = f[t, \mathbb{Q}] \] with \( i(t) = \begin{pmatrix} 12 & 0 \\ 0 & t^{-1} 12 \end{pmatrix} \), \( t \in \mathbb{\hat{Z}}^* \),

The subgroup of \( G_{\mathbb{A}+} \) fixing \( f \) is open

These modular forms are essentially rational powers of 'Thetanullwerte'
\( G_{\mathbb{A}^+} := \{ \gamma \in \text{Gl}(4, \mathbb{A}) : \gamma^t J \gamma = v(\gamma) J, v(\gamma) \in \mathbb{A}^*, v(\gamma)_\infty > 0 \} \)

and \( G_{\mathbb{Q}^+} := G_{\mathbb{A}^+} \cap \text{Gl}(4, \mathbb{Q}) \) with \( J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \)

There is an associative right action of \( G_{\mathbb{A}^+} \) on the arithmetical modular forms of weight \( k \), \( f \to f^u \) with \( u \in G_{\mathbb{A}^+} \) with the properties:

\[ f^\gamma = \det(c\tau + d)^{-k} f(\gamma(\tau)) \text{ for } \gamma \in G_{\mathbb{Q}^+}, \]

\[ f^{i(t)} = f^{[t, \mathbb{Q}]} \text{ with } i(t) = \begin{pmatrix} 1 & 0 \\ 0 & t^{-1} \end{pmatrix}, \quad t \in \hat{\mathbb{Z}}^*, \]

The subgroup of \( G_{\mathbb{A}^+} \) fixing \( f \) is open

These modular forms are essentially rational powers of 'Thetanullwerte'
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Higher order reciprocity law of Shimura

- $\xi : F \to M(4, \mathbb{Q})$ the representation derived from the corresponding Riemann form
- $h : F^* \to K^*$ the type norm map
- **Shimura**: The higher order reciprocity map $\xi \circ h$ takes $F^*$ to $G_{\mathbb{Q}^+}$, and $F^*_\mathbb{A}$ to $G_{\mathbb{A}^+}$, and we have

$$f(\tau)[x,F] = f^{\xi \circ h(x^{-1})}(\tau)$$

- **U.**: As in genus 1 case we have a restricted map $\xi \circ h$ from $\hat{O}^*$ to $\hat{U}$,
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Higher order reciprocity law of Shimura

- $\xi : F \rightarrow M(4, \mathbb{Q})$ the representation derived from the corresponding Riemann form
- $h : F^* \rightarrow K^*$ the type norm map
- **Shimura**: The higher order reciprocity map $\xi \circ h$ takes $F^*$ to $G_{\mathbb{Q}^+}$, and $F_{\mathbb{A}}^*$ to $G_{\mathbb{A}^+}$, and we have

$$f(\tau)[x,F] = f^{\xi \circ h(x^{-1})}(\tau)$$

- **U.**: As in genus 1 case we have a restricted map $\xi \circ h$ from $\hat{O}^*$ to $\hat{U}$, which we can reduce using the second main theorem of CM to a map from $(O_F/N_O_F)^*$ to a subgroup $V$ of $Gl(4, \mathbb{Z}/N\mathbb{Z})$. 
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Higher order reciprocity law of Shimura

- \( \xi : F \rightarrow M(4, \mathbb{Q}) \) the representation derived from the corresponding Riemann form

- \( h : F^* \rightarrow K^* \) the type norm map

- **Shimura**: The higher order reciprocity map \( \xi \circ h \) takes \( F^* \) to \( G_{\mathbb{Q}^+} \), and \( F_A^* \) to \( G_{A^+} \), and we have

  \[
  f(\tau)[x,F] = f^{\xi \circ h(x^{-1})}(\tau)
  \]

- **U.**: As in genus 1 case we have a restricted map \( \xi \circ h \) from \( \hat{O}^* \) to \( \hat{U} \), which we can reduce using the second main theorem of CM to a map from \( (\mathcal{O}_F/\mathcal{N}\mathcal{O}_F)^* \) to a subgroup \( V \) of \( \text{Gl}(4, \mathbb{Z}/N\mathbb{Z}) \).

  If three modular functions \( g_i \) of some level \((2N, 4N)\) is in \( F(j_1, j_2, j_3) \), then \( V \) acts trivially on \( g_i \).
Shimura’s reciprocity law and class invariants

Class invariants for genus 2 (in progress)

Higher order reciprocity law of Shimura

- $\xi : F \rightarrow M(4, \mathbb{Q})$ the representation derived from the corresponding Riemann form

- $h : F^* \rightarrow K^*$ the type norm map

- **Shimura:** The higher order reciprocity map $\xi \circ h$ takes $F^*$ to $G_{\mathbb{Q}^+}$, and $F_{\mathbb{A}}^*$ to $G_{\mathbb{A}^+}$, and we have

\[
  f(\tau)[x,F] = f^{\xi \circ h(x^{-1})}(\tau)
\]

- **U.:** As in genus 1 case we have a restricted map $\xi \circ h$ from $\hat{\mathbb{O}}^*$ to $\hat{U}$,

  which we can reduce using the second main theorem of CM to a map from $(\mathcal{O}_F/N\mathcal{O}_F)^*$ to a subgroup $V$ of $\text{Gl}(4, \mathbb{Z}/N\mathbb{Z})$. If three modular functions $g_i$ of some level $(2N, 4N)$ is in $F(j_1, j_2, j_3)$, then $V$ acts trivially on $g_i$. 
Shimura’s reciprocity law and class invariants

MERCI BEAUCOUP!
uzunkol@math.tu-berlin.de
Lattices, elliptic curves

- $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$: a lattice, i.e. discrete submodule of $\mathbb{C}$ of rank 2 over $\mathbb{Z}$,

- Two lattices $L$ and $L'$ are said to be homothetic if there exists a nonzero $\mu$ with $L = \mu L'$,
Lattices, elliptic curves

- \( L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \): a lattice, i. e. discrete submodule of \( \mathbb{C} \) of rank 2 over \( \mathbb{Z} \),

- Two lattices \( L \) and \( L' \) are said to be homothetic if there exists a nonzero \( \mu \) with \( L = \mu L' \),

- For \( L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \), define \emph{j-invariant} of \( L \) as
  \[
  j(\tau) = \frac{g_2(\omega_1, \omega_2)^3}{g_2(\omega_1, \omega_2)^3 - 27g_3(\omega_1, \omega_2)^2}
  \]

  with \( g_2(\omega_1, \omega_2) = 60 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^4} \) and
  \( g_3(\omega_1, \omega_2) = 140 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^6} \) (\( \tau = \omega_1/\omega_2 \)).
Lattices, elliptic curves

- $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$: a lattice, i.e. discrete submodule of $\mathbb{C}$ of rank 2 over $\mathbb{Z}$,
- Two lattices $L$ and $L'$ are said to be homothetic if there exists a nonzero $\mu$ with $L = \mu L'$,
- For $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, define $j$-invariant of $L$ as
  
  $j(\tau) = \frac{g_2(\omega_1, \omega_2)^3}{(g_2(\omega_1, \omega_2)^3 - 27g_3(\omega_1, \omega_2)^2)}$ with
  
  $g_2(\omega_1, \omega_2) = 60 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^4}$ and
  
  $g_3(\omega_1, \omega_2) = 140 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^6}$ ($\tau = \omega_1/\omega_2$).
- ⇒ Two homothetic lattices have the same $j$-invariant.
Lattices, elliptic curves

- $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$: a lattice, i.e. discrete submodule of $\mathbb{C}$ of rank 2 over $\mathbb{Z}$,

- Two lattices $L$ and $L'$ are said to be homothetic if there exists a nonzero $\mu$ with $L = \mu L'$,

- For $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, define $j$-invariant of $L$ as
  \[ j(\tau) = \frac{g_2(\omega_1, \omega_2)^3}{(g_2(\omega_1, \omega_2)^3 - 27g_3(\omega_1, \omega_2)^2)} \]
  with
  \[ g_2(\omega_1, \omega_2) = 60 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^4} \quad \text{and} \]
  \[ g_3(\omega_1, \omega_2) = 140 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^6} \quad (\tau = \omega_1/\omega_2). \]

- Two homothetic lattices have the same $j$-invariant.

- Every elliptic curve $E/\mathbb{C}: y^2 = 4x^3 - ax - b$ is isomorphic to a complex torus $\mathbb{C}/L$. 
Lattices, elliptic curves

- \( L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \) : a lattice, i. e. discrete submodule of \( \mathbb{C} \) of rank 2 over \( \mathbb{Z} \),
- Two lattices \( L \) and \( L' \) are said to be homothetic if there exists a nonzero \( \mu \) with \( L = \mu L' \),
- For \( L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \), define \( j \)-invariant of \( L \) as
  \[
  j(\tau) = \frac{g_2(\omega_1, \omega_2)^3}{(g_2(\omega_1, \omega_2)^3 - 27g_3(\omega_1, \omega_2)^2)} \]
  with
  \[
  g_2(\omega_1, \omega_2) = 60 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^4} \]
  and
  \[
  g_3(\omega_1, \omega_2) = 140 \sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^6} \quad (\tau = \omega_1/\omega_2).
  \]
  \( \Rightarrow \) Two homothetic lattices have the same \( j \)-invariant.
- Every elliptic curve \( E/\mathbb{C} : y^2 = 4x^3 - ax - b \) is isomorphic to a complex torus \( \mathbb{C}/L \).
Shimura’s reciprocity law and class invariants

Ring of endomorphisms

- Isomorphy classes of elliptic curves correspond to homothety classes of lattices,
- two elliptic curves $E_1$ and $E_2$ are isomorphic over $\mathbb{C}$ iff $j(E_1) = j(E_2)$. Furthermore, $j(\tau)$ is an algebraic integer for all $\tau \in \mathbb{H} := \{z \in \mathbb{C} : \text{Im}(z) > 0\}$. 
Ring of endomorphisms

- Isomorphism classes of elliptic curves correspond to homothety classes of lattices,
- Two elliptic curves $E_1$ and $E_2$ are isomorphic over $\mathbb{C}$ iff $j(E_1) = j(E_2)$. Furthermore, $j(\tau)$ is an algebraic integer for all $\tau \in \mathbb{H} := \{z \in \mathbb{C} : \text{Im}(z) > 0\}$.
- $\text{End}(E) \cong \text{End}(\mathbb{C}/L) = \{\mu \in \mathbb{C} : \mu L \subseteq L\}$,
Ring of endomorphisms

- Isomorphy classes of elliptic curves correspond to homothety classes of lattices,
- two elliptic curves $E_1$ and $E_2$ are isomorphic over $\mathbb{C}$ iff $j(E_1) = j(E_2)$. Furthermore, $j(\tau)$ is an algebraic integer for all $\tau \in \mathbb{H} := \{z \in \mathbb{C} : \text{Im}(z) > 0\}$.
- $\text{End}(E) \cong \text{End}(\mathbb{C}/L) = \{\mu \in \mathbb{C} : \mu L \subseteq L\}$,
- if there exists an endomorphism $\mu \in \mathbb{C} - \mathbb{Z}$, then $E$ is said to have complex multiplication,
- $\implies$ Deuring: $\text{End}(E)$ is isomorphic to an order of an imaginary quadratic number field.
Ring of endomorphisms

- Isomorphism classes of elliptic curves correspond to homothety classes of lattices,
- Two elliptic curves $E_1$ and $E_2$ are isomorphic over $\mathbb{C}$ iff $j(E_1) = j(E_2)$. Furthermore, $j(\tau)$ is an algebraic integer for all $\tau \in \mathbb{H} := \{z \in \mathbb{C} : \text{Im}(z) > 0\}$.
- $\text{End}(E) \cong \text{End}(\mathbb{C}/L) = \{\mu \in \mathbb{C} : \mu L \subseteq L\}$,
- If there exists an endomorphism $\mu \in \mathbb{C} - \mathbb{Z}$, then $E$ is said to have complex multiplication,
- $\implies$ **Deuring**: $\text{End}(E)$ is isomorphic to an order of an imaginary quadratic number field.
Construction with 'Thetanullwerte'

- **Thm. 1:** We have following equalities for $\tau \in \mathbb{H} \cap K$:
  \[
  \mathcal{F}(\tau) = f(\tau)^6, \\
  \mathcal{F}_1(\tau) = f_1(\tau)^6, \\
  \mathcal{F}_2(\tau) = f_2(\tau)^6, \\
  \eta(\tau)^3 = \frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2}. 
  \]

- **Proof:**
  \[
  \frac{\theta_{00} \cdot \theta_{01} \cdot \theta_{10}}{\eta^3} = \eta^3 \cdot \left( \frac{f \cdot f_1 \cdot f_2}{\eta^3} \right)^2 = 2\eta^3 
  \]
  by Weber $\theta_{00}=\eta^2$ etc.

  \[
  \Rightarrow \eta(\tau)^3 = \frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2}. 
  \]

  On the other side, we have

  \[
  \frac{\theta_{00}^3}{\eta^3} = \eta^3 f^6 
  \]

  as by above $\theta_{00}=\eta^2$

  Similarly, we obtain the equalities for $\mathcal{F}_1$ and $\mathcal{F}_2$. $\square$
Construction with ’Thetanullwerte’

- **Thm. 1:** We have following equalities for $\tau \in \H \cap K$:
  \[
  \mathcal{F}(\tau) = f(\tau)^6, \\
  \mathcal{F}_1(\tau) = f_1(\tau)^6, \\
  \mathcal{F}_2(\tau) = f_2(\tau)^6, \\
  \eta(\tau)^3 = \frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2}.
  \]

- **Proof:**
  \[
  \theta_{00} \cdot \theta_{01} \cdot \theta_{10} = \eta^3 \cdot \left( f \cdot f_1 \cdot f_2 \right)^2 = 2\eta^3 \text{ by Weber } \theta_{00} = \eta f^2 \text{ etc.} = \sqrt{2} \text{ (Weber)}
  \]
  \[
  \Rightarrow \eta(\tau)^3 = \frac{\theta_{00}(\tau)\theta_{01}(\tau)\theta_{10}(\tau)}{2}. \text{On the other side, we have}
  \]
  \[
  \theta_{00}^3 = \eta^3 f^6 \text{ as by above } \theta_{00} = \eta f^2
  \]
  
  Similarly, we obtain the equalities for $\mathcal{F}_1$ and $\mathcal{F}_2$. □
Shimura’s reciprocity law and class invariants

\[ \Delta \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right) : \text{the discriminant of the lattice, spanned by } \omega_1 \text{ and } \omega_2, \text{ with } \tau = \frac{\omega_1}{\omega_2}. \]

\[ \Delta(\tau) := (2\pi)^{12} \eta(\tau)^{24}, \text{ with } \Delta \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right) = \omega_2^{-12} \Delta(\tau). \]

Let \( p \) be a prime with \( p^l | t \) but \( p^{l+1} \nmid t, l \in \mathbb{Z}^{\geq 0}, t \in \mathbb{N} \). Let further \( P := \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathbb{Z}^{2 \times 2} \) be a primitive matrix (i. e. \( P \) has coprime nonzero entries) of determinant \( p \). We define now

\[ \varphi_P(\tau) := p^{12} \frac{\Delta \left( P \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right) \right)}{\Delta \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right)} \]

with \([\omega_1, \omega_2]\) as a basis of a fractional ideal \( I \subseteq \mathcal{O}_t \).
\[\Delta \left( \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \right) : \text{the discriminant of the lattice, spanned by } \omega_1 \text{ and } \omega_2, \text{ with } \tau = \frac{\omega_1}{\omega_2}.\]

\[\Delta(\tau) := (2\pi)^{12} \eta(\tau)^{24}, \text{ with } \Delta \left( \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \right) = \omega_2^{-12} \Delta(\tau).\]

Let \( p \) be a prime with \( p^l \mid t \) but \( p^{l+1} \nmid t, \) \( l \in \mathbb{Z}_{\geq 0}, \) \( t \in \mathbb{N}. \) Let further \( P := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times2} \) be a primitive matrix (i.e. \( P \) has coprime nonzero entries) of determinant \( p. \) We define now

\[\varphi_P(\tau) := p^{12} \frac{\Delta \left( P \left( \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \right) \right)}{\Delta \left( \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \right)}\]

with \([\omega_1, \omega_2] \) as a basis of a fractional ideal \( I \subseteq \mathcal{O}_t.\)
Class units

- **Deuring:** Let the prerequisites be as above:

1. *p* ramified in *K*: Then \( \varphi_p(\tau) \) is a unit, if \( P \left( \frac{\omega_1}{\omega_2} \right) \) is a basis of a fractional ideal \( p\mathcal{O}_t \).
Class units

- **Deuring**: Let the prerequisites be as above:

1. *p* ramified in *K*: Then \( \frac{\varphi_p(\tau)}{p^6} \) is a unit, if \( P \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right) \) is a basis of a fractional ideal \( p\mathcal{O}_t \).

2. *p* inert in *K*: Then \( \frac{\varphi_p(\alpha)}{p^{\frac{12}{1} - \frac{1}{p^{t-1}(p+1)}}} \) is a unit, if \( P \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right) \) is a basis of a fractional \( \mathcal{O}_{tp^{-1}} \)–ideal.
Class units

> **Deuring:** Let the prerequisites be as above:

1. *p* ramified in *K*: Then \( \frac{\varphi_p(\tau)}{p^6} \) is a unit, if \( P \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right) \) is a basis of a fractional ideal \( p\mathcal{O}_t \).

2. *p* inert in *K*: Then \( \frac{\varphi_p(\alpha)}{p^{12\left[1 - \frac{1}{p^l - 1/(p+1)}\right]}} \) is a unit, if \( P \left( \begin{array}{c} \omega_1 \\ \omega_2 \end{array} \right) \) is a basis of a fractional \( \mathcal{O}_{tp^{-1}} \)–ideal.

> **Thm. 3:** Let \( g(\tau) \) be one of the class invariants of Weber. Then \( g(\tau) \) is a unit, hence we say class units, if we have \( m \equiv 1, 5, 7 \mod 8 \) and \( m \equiv 2 \mod 4 \).

(Some cases stated by Birch without a proof!)
Class units

▶ **Deuring:** Let the prerequisites be as above:

1. **$p$ ramified in $K$:** Then $\frac{\varphi_P(\tau)}{p^6}$ is a unit, if $P \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ is a basis of a fractional ideal $p\mathcal{O}_t$.

2. **$p$ inert in $K$:** Then $\frac{\varphi_P(\alpha)}{p^{12} \left[ \frac{1}{1 - \frac{1}{p^{1/(p+1)}}} \right]}$ is a unit, if $P \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ is a basis of a fractional $\mathcal{O}_{tp^{-1}}$–ideal.

▶ **Thm. 3:** Let $g(\tau)$ be one of the class invariants of Weber. Then $g(\tau)$ is a unit, hence we say **class units**, if we have $m \equiv 1, 5, 7 \mod 8$ and $m \equiv 2 \mod 4$.

(Some cases stated by **Birch** without a proof!)
Proof for the case $m \equiv 5 \mod 8$:

$\Rightarrow \tau \in \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'}) = K$ with $d' \equiv -1 \mod 4$ and $t \equiv 1 \mod 4$

$\Rightarrow$ we obtain $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $(2) = p^2$, as 2 is ramified in $\mathcal{O}_K$.

Considering the basis $[\tau, 1]$ of $\mathcal{O}_t$ together with $P := \begin{pmatrix} 1 & t \\ 0 & 2 \end{pmatrix}$, we have $P \begin{pmatrix} \tau \\ 1 \end{pmatrix} = [\tau + t, 2]$ as a basis of the ideal $p\mathcal{O}_t$.

$\implies 2^{-6} \frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)}$ is a unit, Deuring
Proof for the case $m \equiv 5 \mod 8$:

$\Rightarrow \tau \in \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'}) = K$ with $d' \equiv -1 \mod 4$ and $t \equiv 1 \mod 4$

$\Rightarrow$ we obtain $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $(2) = p^2$, as 2 is ramified in $\mathcal{O}_K$.

Considering the basis $[\tau, 1]$ of $\mathcal{O}_t$ together with

$P := \begin{pmatrix} 1 & t \\ 0 & 2 \end{pmatrix}$, we have $P \begin{pmatrix} \tau \\ 1 \end{pmatrix} = [\tau + t, 2]$ as a basis of the ideal $p\mathcal{O}_t$.

$\implies 2^{-6} \frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)}$ is a unit, hence Deuring

$2^{-6} \frac{\Delta(\frac{\tau+1}{2})}{\Delta(\tau)} = g(\tau)^2 = \left( \left( \frac{f(\tau)^4}{2} \right)^3 \right)^2$

is a unit, which implies the property of being unit for $g(\tau)$. $\square$
Proof for the case $m \equiv 5 \pmod{8}$:

$\Rightarrow \tau \in \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'}) = K$ with $d' \equiv -1 \pmod{4}$ and $t \equiv 1 \pmod{4}$

$\Rightarrow$ we obtain $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $(2) = p^2$, as 2 is ramified in $\mathcal{O}_K$.

Considering the basis $[\tau, 1]$ of $\mathcal{O}_t$ together with

$P := \begin{pmatrix} 1 & t \\ 0 & 2 \end{pmatrix}$, we have $P \begin{pmatrix} \tau \\ 1 \end{pmatrix} = [\tau + t, 2]$ as a basis of the ideal $p\mathcal{O}_t$.

$\implies 2^{-6} \frac{\Delta(\frac{\tau + 1}{2})}{\Delta(\tau)}$ is a unit, hence

Deuring

$2^{-6} \frac{\Delta(\frac{\tau + 1}{2})}{\Delta(\tau)} = g(\tau)^2 = \left( \left( \frac{f(\tau)^4}{2} \right)^3 \right)^2$

is a unit, which implies the property of being unit for $g(\tau)$. □