Constructing Class invariants

Aristides Kontogeorgis

Department of Mathematics
University of Athens.

Workshop Thales 1-3 July 2015

: Algebraic modeling of topological and computational structures and applications
Contents

Elliptic Curves

Number Fields

Modular functions

Galois cohomology

Examples
An elliptic curve defined over a field $K$ of characteristic $p > 3$ is a curve given by the equation

$$E : y^2 = x^3 + ax + b$$

such that $4a^3 + 27b^2 \neq 0$.

The set of points $E(K)$ together with a point at infinity is an abelian group.
An elliptic curve defined over a field $K$ of characteristic $p > 3$ is a curve given by the equation

$$E : y^2 = x^3 + ax + b$$

such that $4a^3 + 27b^2 \neq 0$.

The set of points $E(K)$ together with a point at infinity is an abelian group.
Elliptic curves defined over finite fields

The set of points $E(\mathbb{F}_p)$ form a finite abelian group. The following bound holds

$$\#E(\mathbb{F}_p) \leq q + 1 - \alpha r \leq q + 1 + 2\sqrt{q}.$$  

Discrete logarithm problem

Given elements $P, Q$ on an abelian group so that $nP = Q$. Find $n$.

This is a difficult problem, we have to try all possible $n$, until we find the correct one.

Abelian groups are usually: $\mathbb{F}_p^*, E$.

Even if the abelian group has a big order then is can be a product of small factors like $(\mathbb{Z}/2\mathbb{Z})^n$ and the discrete logarithm problem is easy. For the elliptic curve cases, the discrete logarithm problem is difficult if the order of the group has order a prime number, therefore it a cyclic group.
Elliptic curves defined over finite fields

The set of points \( E(\mathbb{F}_p) \) form a finite abelian group. The following bound holds

\[
\#E(\mathbb{F}_p) \leq q + 1 - \alpha_r \leq q + 1 + 2\sqrt{q}.
\]

**Discrete logarithm problem**

Given elements \( P, Q \) on an abelian group so that \( nP = Q \). Find \( n \).

This is a difficult problem, we have to try all possible \( n \), until we find the correct one.

**Abelian groups are usually:** \( \mathbb{F}_p^*, E \).

Even if the abelian group has a big order then it can be a product of small factors like \( (\mathbb{Z}/2\mathbb{Z})^n \) and the discrete logarithm problem is easy. For the elliptic curve cases, the discrete logarithm problem is difficult if the order of the group has order a prime number, therefore it is a cyclic group.
Elliptic curves defined over finite fields

The set of points \( E(\mathbb{F}_p) \) form a finite abelian group. The following bound holds

\[
\#E(\mathbb{F}_p) \leq q + 1 - \sigma_r \leq q + 1 + 2\sqrt{q}.
\]

**Discrete logarithm problem**

Given elements \( P, Q \) on an abelian group so that \( nP = Q \). Find \( n \).

This is a difficult problem, we have to try all possible \( n \), until we find the correct one.

**Abelian groups are usually**: \( \mathbb{F}_p^*, E \).

Even if the abelian group has a big order then is can be a product of small factors like \( (\mathbb{Z}/2\mathbb{Z})^n \) and the discrete logarithm problem is easy. For the elliptic curve cases, the discrete logarithm problem is difficult if the order of the group has order a prime number, therefore it a cyclic group.
The set of points $E(\mathbb{F}_p)$ form a finite abelian group. The following bound holds:

$$\#E(\mathbb{F}_p) \leq q + 1 - \alpha r \leq q + 1 + 2\sqrt{q}.$$ 

**Discrete logarithm problem**

Given elements $P, Q$ on an abelian group so that $nP = Q$. Find $n$.

This is a difficult problem, we have to try all possible $n$, until we find the correct one.

**Abelian groups are usually**: $\mathbb{F}_p^*, E$.

Even if the abelian group has a big order then it can be a product of small factors like $(\mathbb{Z}/2\mathbb{Z})^n$ and the discrete logarithm problem is easy.

For the elliptic curve cases, the discrete logarithm problem is difficult if the order of the group has order a prime number, therefore it a cyclic group.
Elliptic curves defined over finite fields

The set of points $E(\mathbb{F}_p)$ form a finite abelian group. The following bound holds

$$\#E(\mathbb{F}_p) \leq q + 1 - \alpha_r \leq q + 1 + 2\sqrt{q}.$$ 

**Discrete logarithm problem**

Given elements $P, Q$ on an abelian group so that $nP = Q$. Find $n$.

This is a difficult problem, we have to try all possible $n$, until we find the correct one.

**Abelian groups are usually**: $\mathbb{F}_p^*$, $E$.

Even if the abelian group has a big order then it can be a product of small factors like $(\mathbb{Z}/2\mathbb{Z})^n$ and the discrete logarithm problem is easy.

For the elliptic curve cases, the discrete logarithm problem is difficult if the order of the group has order a prime number, therefore it a cyclic group.
Construct prime order elliptic curves

1. Randomly: Select random elliptic curves until we hit one with the correct order.

2. Complex multiplication method.

We will focus on the second method.
Every elliptic curve over \( \mathbb{C} \) is a quotient of the universal covering space \( \mathbb{C} \) modulo a discrete subgroup - lattice \( L = \mathbb{Z} + \tau \mathbb{Z}, \Im(\tau) > 0 \). Lattices \( L, L' \) give the same elliptic curves if and only if

\[
\tau' = \frac{a\tau + b}{c\tau + d}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}).
\]

The quotient map

\[
\mathbb{H} \to \text{SL}(2, \mathbb{Z})\backslash \mathbb{H} \cong \mathbb{C}
\]

is called the \( j \)-invariant. It is a \( \text{SL}(2, \mathbb{Z}) \)-invariant function hence periodic. It admits a Fourier expansion at \( q = e^{2\pi i \tau} \),

\[
j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 +
\]
Elliptic curves as quotients of the complex numbers

Every elliptic curve over $\mathbb{C}$ is a quotient of the universal covering space $\mathbb{C}$ modulo a discrete subgroup - lattice $L = \mathbb{Z} + \tau \mathbb{Z}$, $\Im(\tau) > 0$. Lattices $L, L'$ give the same elliptic curves if and only if

$$\tau' = \frac{a\tau + b}{c\tau + b}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}).$$

The quotient map

$$\mathbb{H} \rightarrow \text{SL}(2, \mathbb{Z}) \backslash \mathbb{H} \cong \mathbb{C}$$

is called the $j$-invariant. It is a $\text{SL}(2, \mathbb{Z})$-invariant function hence periodic. It admits a Fourier expansion at $q = e^{2\pi i \tau}$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \ldots$$
Elliptic curves as quotients of the complex numbers

Every elliptic curve over $\mathbb{C}$ is a quotient of the universal covering space $\mathbb{C}$ modulo a discrete subgroup - lattice $L = \mathbb{Z} + \tau \mathbb{Z}$, $\Im(\tau) > 0$. Lattices $L, L'$ give the same elliptic curves if and only if

$$\tau' = \frac{a\tau + b}{c\tau + d}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}).$$

The quotient map

$$\mathbb{H} \to \text{SL}(2, \mathbb{Z}) \backslash \mathbb{H} \cong \mathbb{C}$$

is called the $j$-invariant. It is a $\text{SL}(2, \mathbb{Z})$- invariant function hence periodic. It admits a Fourier expansion at $q = e^{2\pi i \tau}$,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \ldots$$
**Remarks**: The coefficients of the Fourier expansion are integers. They are related to the dimensions of the irreducible representations of the Monster, the biggest sporadic simple group with order

\[ 8080174247945128758864599049617107570057543680000000000. \]
A number field is a finite extension of the field \( \mathbb{Q} \), i.e. a field

\[
K = \mathbb{Q}[x]/f(x),
\]

where \( f(x) \) is an irreducible polynomial of \( \mathbb{Q}[x] \). The ring of algebraic integers \( \mathcal{O} \) is the ring consisted of elements

\[
\mathcal{O} = \{ x \in K : \text{such that } x \text{ is a root of a monic polynomial } f(x) \in \mathbb{Z}[x] \}.
\]

The ring \( \mathcal{O} \) is not a unique factorization domain but it is a Dedekind ring: every ideal is decomposed uniquely as a product of prime ideals.

\[
l = p_1^{e_1} \cdots p_r^{e_r}.
\]
A number field is a finite extension of the field $\mathbb{Q}$, i.e. a field

$$K = \mathbb{Q}[x]/f(x),$$

where $f(x)$ is an irreducible polynomial of $\mathbb{Q}[x]$. The ring of algebraic integers $\mathcal{O}$ is the ring consisted of elements

$$\mathcal{O} = \{x \in K : \text{such that } x \text{ is a root of a monic polynomial } f(x) \in \mathbb{Z}[x]\}.$$

The ring $\mathcal{O}$ is not a unique factorization domain but it is a Dedekind ring: every ideal is decomposed uniquely as a product of prime ideals.

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$
Number fields

A number field is a finite extension of the field $\mathbb{Q}$, i.e. a field

$$K = \mathbb{Q}[x]/f(x),$$

where $f(x)$ is an irreducible polynomial of $\mathbb{Q}[x]$. The ring of algebraic integers $\mathcal{O}$ is the ring consisted of elements

$$\mathcal{O} = \{x \in K : \text{such that } x \text{ is a root of a monic polynomial } f(x) \in \mathbb{Z}[x]\}.$$

The ring $\mathcal{O}$ in not a unique factorization domain but it is a Dedekind ring: every ideal is decomposed uniquely as a product of prime ideals.

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$
We consider the semigroup of ideals of \( \mathcal{O} \), which is enlarged to a group adding fractional ideals. These are abelian additive subgroups \( I \) of the number field \( K \), such that for some \( x \in \mathcal{O} \) the set \( xI \) is an ideal of the ring \( \mathcal{O} \). In this way we construct the group of fractional ideals \( \mathcal{I}(\mathcal{O}) \).

**Example:** The fractional ideals of \( \mathbb{Z} \) are the elements \( \frac{m}{n} \mathbb{Z}, \ m, n \in \mathbb{Z} \).

We also consider the subgroup \( \mathcal{P}(\mathcal{O}) \) of principal fractional ideals \( a\mathcal{O} \), where \( a \in K \).

The quotient is the class group

\[
\text{Cl}(\mathcal{O}) = \frac{\mathcal{I}(\mathcal{O})}{\mathcal{P}(\mathcal{O})}.
\]

One can show that the class group is a finite group.
We consider the semigroup of ideals of $\mathcal{O}$, which is enlarged to a group adding fractional ideals. These are abelian additive subgroups $I$ of the number field $K$, such that for some $x \in \mathcal{O}$ the set $xI$ is an ideal of the ring $\mathcal{O}$. In this way we construct the group of fractional ideals $I(\mathcal{O})$.

**Example:** The fractional ideals of $\mathbb{Z}$ are the elements $\frac{m}{n}\mathbb{Z}$, $m, n \in \mathbb{Z}$.

We also consider the subgroup $Pl(\mathcal{O})$ of principal fractional ideals $a\mathcal{O}$, where $a \in K$.

The quotient is the class group

$$\text{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{Pl(\mathcal{O})}.$$  

One can show that the class group is a finite group.
We consider the semigroup of ideals of \( \mathcal{O} \), which is enlarged to a group adding fractional ideals. These are abelian additive subgroups \( I \) of the number field \( K \), such that for some \( x \in \mathcal{O} \) the set \( xI \) is an ideal of the ring \( \mathcal{O} \). In this way we construct the group of fractional ideals \( \mathcal{I}(\mathcal{O}) \).

**Example:** The fractional ideals of \( \mathbb{Z} \) are the elements \( \frac{m}{n} \mathbb{Z} \), \( m, n \in \mathbb{Z} \).

We also consider the subgroup \( \mathcal{PI}(\mathcal{O}) \) of principal fractional ideals \( a\mathcal{O} \), where \( a \in K \).

The quotient is the class group

\[
\text{Cl}(\mathcal{O}) = \frac{\mathcal{I}(\mathcal{O})}{\mathcal{PI}(\mathcal{O})}.
\]

One can show that the class group is a finite group.
We consider the semigroup of ideals of $\mathcal{O}$, which is enlarged to a group adding fractional ideals. These are abelian additive subgroups $I$ of the number field $K$, such that for some $x \in \mathcal{O}$ the set $xI$ is an ideal of the ring $\mathcal{O}$. In this way we construct the group of fractional ideals $I(\mathcal{O})$.

**Example:** The fractional ideals of $\mathbb{Z}$ are the elements $\frac{m}{n}\mathbb{Z}$, $m, n \in \mathbb{Z}$.

We also consider the subgroup $\text{Pl}(\mathcal{O})$ of principal fractional ideals $a\mathcal{O}$, where $a \in K$.

The quotient is the class group

$$\text{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{\text{Pl}(\mathcal{O})}.$$  

One can show that the class group is a finite group.
Consider an extension of number fields $L/K$. A prime ideal $P$ of $\mathcal{O}_K$ can be seen as an ideal of $\mathcal{O}_L$ by scalar extension $P\mathcal{O}_L$. It does not remain prime so it can be written as

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r},$$

where $Q_i$ are prime ideals of $\mathcal{O}_L$. If all $e_i = 1$ then we will say that $P$ is not ramified in the extension $L/K$. If no ideal is ramified then the extension is called unramified.
Consider an extension of number fields $L/K$. A prime ideal $P$ of $\mathcal{O}_K$ can be seen as an ideal of $\mathcal{O}_L$ by scalar extension $P\mathcal{O}_L$. It does not remain prime so it can be written as

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r},$$

where $Q_i$ are prime ideals of $\mathcal{O}_L$.

If all $e_i = 1$ then we will say that $P$ is not ramified in the extension $L/K$. If no ideal is ramified then the extension is called unramified.
Consider an extension of number fields $L/K$. A prime ideal $P$ of $\mathcal{O}_K$ can be seen as an ideal of $\mathcal{O}_L$ by scalar extension $P\mathcal{O}_L$. It does not remain prime so it can be written as

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r},$$

where $Q_i$ are prime ideals of $\mathcal{O}_L$. If all $e_i = 1$ then we will say that $P$ is not ramified in the extension $L/K$. If no ideal is ramified then the extension is called unramified.
Theorem
For every number field there is a Galois extension $H_K$ defined to be the maximal unramified abelian extension of $K$. For the Galois group is the class group of $K$.

$\text{Gal}(H_K/K) = \text{Cl}(\mathcal{O}_K)$.

The field $H_K$ is called the Hilbert’s class field.

Remarks: Unramified extensions in Riemann surface theory correspond to topological coverings. Fields with class group $\text{Cl}(\mathcal{O}_K) = \{1\}$ cannot have unramified covers therefore are in some sense “simply connected”. For example $\mathbb{Q}$ simply connected. In this direction: The fact that every ideal of $\mathbb{Z}$ is principal is the number theoretical analogon to the topological theorem: “every vector bundle over simply connected manifold is globally trivial”. The group

$$\text{Cl}(\mathcal{O}_K) = \pi^1(\text{Spec}\mathcal{O}_K)^\text{ab} = H_1(\text{Spec}\mathcal{O}_K).$$
Theorem

For every number field there is a Galois extension $H_K$ defined to be the maximal unramified abelian extension of $K$. For the Galois group is the class group of $K$ \( \text{Gal}(H_K/K) = \text{Cl}(\mathcal{O}_K) \).

The field $H_K$ is called the Hilbert’s class field.

Remarks: Unramified extensions in Riemann surface theory correspond to topological coverings. Fields with class group $\text{Cl}(\mathcal{O}_K) = \{1\}$ cannot have unramified covers therefore are in some sense “simply connected”. For example $\mathbb{Q}$ is simply connected. In this direction: The fact that every ideal of $\mathbb{Z}$ is principal is the number theoretical analogon to the topological theorem: “every vector bundle over simply connected manifold is globally trivial”. The group

\[
\text{Cl}(\mathcal{O}_K) = \pi^1(\text{Spec}\mathcal{O}_K)^{ab} = H_1(\text{Spec}\mathcal{O}_K).
\]
D. Hilbert
Construction of the Hilbert class field

Suppose that $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$ with $d$ square free. We compute that

$$\mathcal{O}_K = \begin{cases} 
\mathbb{Z}[\sqrt{-d}] & \text{if } -d \equiv 2, 3 \mod 4 \\
\mathbb{Z}[\frac{1+\sqrt{-d}}{2}] & \text{if } -d \equiv 1 \mod 4
\end{cases}$$

We will show soon that these are the endomorphisms of an elliptic curve with complex multiplication.
The class group of an imaginary quadratic field

**Quadratic forms of discriminant D**

\[ ax^2 + bxy + cy^2; \ b^2 - 4ac = -D, \ a, b, c \in \mathbb{Z} \ (a, b, c) = 1 \]

K.F. Gauss Disquisitiones Arithmeticae.

We will say that two quadratic forms are equivalent if there is an element in \( SL(2, \mathbb{Z}) \) sending one to the other. The equivalence classes are in one to one correspondence to the class group and they can be computed easily since a full set of representatives is given by elements \((a, b, c)\) such that

\[ |b| \leq a \leq \sqrt{\frac{D}{3}}, \ a \leq c, \ (a, b, c) = 1, \ b^2 - 4ac = -D \]

if \( |b| = a \) or \( a = c \) then \( b \geq 0 \).
The class group of an imaginary quadratic field

Quadratic forms of discriminant $D$

$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, \ a, b, c \in \mathbb{Z} \ (a, b, c) = 1$$

K.F. Gauss Disquisitiones Arithmeticae.

We will say that two quadratic forms are equivalent if there is an element in $SL(2, \mathbb{Z})$ sending one to the other. The equivalence classes are in one to one correspondence to the class group and they can be computed easily since a full set of representatives is given by elements $(a, b, c)$ such that

$$|b| \leq a \leq \sqrt{\frac{D}{3}}, \ a \leq c, \ (a, b, c) = 1, \ b^2 - 4ac = -D$$

if $|b| = a$ or $a = c$ then $b \geq 0$. 


The class group of an imaginary quadratic field

**Quadratic forms of discriminant D**

\[ ax^2 + bxy + cy^2; \quad b^2 - 4ac = -D, \quad a, b, c \in \mathbb{Z} \quad (a, b, c) = 1 \]

K.F. Gauss *Disquisitiones Arithmeticae*.

We will say that two quadratic forms are equivalent if there is an element in \( SL(2, \mathbb{Z}) \) sending one to the other. The equivalence classes are in one to one correspondence to the class group and they can be computed easily since a full set of representatives is given by elements \((a, b, c)\) such that

\[ |b| \leq a \leq \sqrt{\frac{D}{3}}, \quad a \leq c, \quad (a, b, c) = 1, \quad b^2 - 4ac = -D \]

if \(|b| = a\) or \(a = c\) then \(b \geq 0\).
K.F. Gauss
Complex multiplication

We consider the ring of endomorphisms of an elliptic curve. In most of the cases $\text{End}(E) \cong \mathbb{Z}$.

$$[n] : E \rightarrow E \quad P \mapsto nP$$

There are cases where $\text{End}(E)$ is an order in an imaginary quadratic field. For example

$$\text{End}(\mathbb{C}/\mathbb{Z}[i]) = \mathbb{Z}[i].$$

Finite fields

Frobenious endomorphism Frobenious $F : x \mapsto x^p$ is an element in $\text{End}(E)$. It satisfies a characteristic polynomial

$$x^2 - \text{tr}(F)x + q = 0.$$

$$N_p = p + 1 \pm \text{tr}(F)$$
Complex multiplication

We consider the ring of endomorphisms of an elliptic curve. In most of the cases $\text{End}(E) \cong \mathbb{Z}$.

$$[n] : E \to E \quad P \mapsto nP$$

There are cases where $\text{End}(E)$ is an order in an imaginary quadratic field. For example

$$\text{End}(\mathbb{C}/\mathbb{Z}[i]) = \mathbb{Z}[i].$$

Finite fields

Frobenious endomorphism Frobenious $F : x \mapsto x^p$ is an element in $\text{End}(E)$. It satisfies a characteristic polynomial

$$x^2 - \text{tr}(F)x + q = 0.$$ 

$$N_p = p + 1 \pm \text{tr}(F)$$
Complex multiplication

We consider the ring of endomorphisms of an elliptic curve. In most of the cases $\text{End}(E) \cong \mathbb{Z}$.

$$[n] : E \rightarrow E \quad P \mapsto nP$$

There are cases where $\text{End}(E)$ is an order in an imaginary quadratic field. For example

$$\text{End}(\mathbb{C}/\mathbb{Z}[i]) = \mathbb{Z}[i].$$

Finite fields

Frobenious endomorphism Frobenious $F : x \mapsto x^p$ is an element in $\text{End}(E)$. It satisfies a characteristic polynomial

$$x^2 - \text{tr}(F)x + q = 0.$$ 

$$N_p = p + 1 \pm \text{tr}(F)$$
Consider $\tau \in \mathbb{H}$, which is a root of a monic polynomial in $\mathbb{Z}[x]$ of degree 2. We set $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau \mathbb{Z})$. Then

1. $\text{End}(E_\tau) = E_\tau$.

2. $j(\tau) = j(E_\tau)$ is an algebraic integer. Its irreducible polynomial is given by the equation

$$H_D(x) = \prod_{[a,b,c] \in CL(K)} \left( x - j \left( \frac{-b + \sqrt{-D}}{2a} \right) \right) \in \mathbb{Z}[x].$$

3. The element $j(\tau)$ generates the Hilber class field.
Kronecker’s Jugendtraum or Hilbert’s twelfth problem

**Kronecker-Weber theorem**
Every abelian extension is a subfield of a cyclotomic \( \mathbb{Q} \left( \exp \left( \frac{2\pi i}{n} \right) \right) \).

**Kronecker’s Jugendtraum**
Produce Hilbert’s class fields as special values of complex functions.

**What is known?**
Complex multiplication for elliptic curves.
Generalization of imaginary quadratic extensions CM-fields and abelian varieties with complex multiplication (Shimura).
**Kronecker’s Jugendtraum or Hilbert’s twelfth problem**

*Kronecker-Weber theorem*

Every abelian extension is a subfield of a cyclotomic \( \mathbb{Q} \left( \exp \left( \frac{2\pi i}{n} \right) \right) \).

*Kronecker’s Jugendtraum*

Produce Hilbert’s class fields as special values of complex functions.

**What is known?**

Complex multiplication for elliptic curves.

Generalization of imaginary quadratic extensions CM-fields and abelian varieties with complex multiplication (Shimura).
Kronecker’s Jugendtraum or Hilbert’s twelfth problem

**Kronecker-Weber theorem**
Every abelian extension is a subfield of a cyclotomic $\mathbb{Q} \left( \exp \left( \frac{2\pi i}{n} \right) \right)$.

**Kronecker’s Jugendtraum**
Produce Hilbert’s class fields as special values of complex functions.

**What is known?**
Complex multiplication for elliptic curves.
Generalization of imaginary quadratic extensions CM-fields and abelian varieties with complex multiplication (Shimura).
1. We have to construct the $j$-invariant.

2. By Hasse bound we have that

$$Z := 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2.$$ 

3. The equation

$$4p = u^2 + Dv^2$$

for some $u$ satisfies $m = p + 1 \pm u$. The negative number $-D$ is called CM-discriminant for the prime $p$.

4. 

$$x^2 - \text{tr}(F)x + p \mapsto \Delta = \text{tr}(F)^2 - 4p = -Dv^2.$$
1. We have to construct the $j$-invariant.

2. By Hasse bound we have that
   \[ Z := 4p - (p + 1 - m)^2 \geq 0 \implies Z = Dv^2. \]

3. The equation
   \[ 4p = u^2 + Dv^2 \]
   for some $u$ satisfies $m = p + 1 \pm u$. The negative number $-D$ is called CM-discriminatnt for the prime $p$.

4. \[ x^2 - \text{tr}(F)x + p \mapsto \Delta = \text{tr}(F)^2 - 4p = -Dv^2. \]
Elliptic curve construction

1. We have to construct the $j$-invariant.

2. By Hasse bound we have that
   \[ Z := 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2. \]

3. The equation
   \[ 4p = u^2 + Dv^2 \]
   for some $u$ satisfies $m = p + 1 \pm u$. The negative number $-D$ is called CM-discriminant for the prime $p$.

4. \[ x^2 - \text{tr}(F)x + p \mapsto \Delta = \text{tr}(F)^2 - 4p = -Dv^2. \]
1. We have to construct the $j$-invariant.

2. By Hasse bound we have that
   $$Z := 4p - (p + 1 - m)^2 \geq 0 \Rightarrow Z = Dv^2.$$

3. The equation
   $$4p = u^2 + Dv^2$$
   for some $u$ satisfies $m = p + 1 \pm u$. The negative number $-D$ is called CM-discriminant for the prime $p$

4. $$x^2 - \text{tr}(F)x + p \mapsto \Delta = \text{tr}(F)^2 - 4p = -Dv^2.$$
Reduction of elliptic curve modulo $\bmod p$

\[
\begin{align*}
(C) & \quad \tau \in \text{End}(E(C)) \\
(F_p) & \quad F \in \text{End}(E(F_p)) \\
\end{align*}
\]

\[
\begin{align*}
& j \text{ is a root of } H_D(x) \in \mathbb{Z}[x] \\
& j \text{ is a root of } H_D(x) \bmod p \in F_p[x]
\end{align*}
\]
Elliptic curve construction

1. Select a prime $p$. Select the smallest $D$ together with $u, v \in \mathbb{Z}$ such that $4p = u^2 + Dv^2$.

2. If one of $p + 1 - u, p + 1 + u$ has order a prime number we proceed to elliptic curve construction. If not we try a different $p$.

3. Compute the Hilbert polynomial $H_D(x) \in \mathbb{Z}[x]$ using the values of the $j$-invariant. Next compute the polynomial $H_D(x) \mod p$. One root if the $j$ invariant we are looking for which can be given by (for $j \neq 0, 1728$)

$$y^2 = x^3 + 3kc^2x + 2kc^3, \ k = j/(1728 - j), \ c \in \mathbb{F}_p$$
There is a problem!

The coefficients of the Hilbert polynomial grow very fast. The Hilbert polynomial for \( \mathbb{Q}(\sqrt{-299}) \) is:

\[
x^8 + 391086320728105978429440x^7
\]
\[-28635280874816126174326167699456x^6
\]+2094055410006322146651491130721133658112x^5
\]+186547260770756829961971675685151791296544768x^4
\]+6417141278133218665289808655954275181523718111232x^3
\]-19207839443594488822936988943836177115227877227364352x^2
\]+45797528808215150136248975363201860724351225694802411520x
\]-18273883965326272223717626628647422907813731016193733558272.
Alternative method for computing the Hilbert class field.

Dedekind’s $\eta$-function

$$\eta(\tau) = \exp \left( \frac{2\pi i \tau}{24} \right) \prod_{n=1}^{\infty} (1 - q^n), \quad q = \exp(2\pi i \tau), \quad \tau \in \mathbb{H}.$$ 

which leads to the Weber functions:

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

Which can also producte the Hilbert class field (D. Zagier–N. Yui).

What is special about them?

They are modular functions
Alternative method for computing the Hilbert class field.

Dedekind's $\eta$-function

$$\eta(\tau) = \exp\left(\frac{2\pi i \tau}{24}\right) \prod_{n=1}^{\infty} (1 - q^n), \quad q = \exp(2\pi i \tau), \quad \tau \in \mathbb{H}. $$

which leads to the Weber functions:

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

Which can also produce the Hilbert class field (D. Zagier- N. Yui).

What is special about them?

They are modular functions
Dedekind's $\eta$-function

$$\eta(\tau) = \exp\left(\frac{2\pi i \tau}{24}\right) \prod_{n=1}^{\infty} (1 - q^n), \quad q = \exp(2\pi i \tau), \quad \tau \in \mathbb{H}. $$

which leads to the Weber functions:

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

Which can also producte the Hilbert class field (D. Zagier- N. Yui).

What is special about them?

They are modular functions.
Modular functions of level $N$

We consider the group

$$
\Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \text{ with } A \equiv I_2 \text{ mod} N \right\}.
$$

The quotient space $\Gamma(N) \backslash \mathbb{H}$ is a Riemann surface $Y(N)$ which can be compactified to a compact Riemann surface $X(N)$ adding some points on the line $\text{Im}(s) = 0$. The meromorphic functions on $X(N)$ are called modular functions of level $N$.

The Riemann surfaces $X(N)$ correspond to algebraic curves defined over the field $\mathbb{Q}(\zeta_N)$. The Fourier expansions of modular functions of level $N$ have coefficients in $\mathbb{Q}(\zeta_N)$.
We consider the group

\[ \Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \text{ with } A \equiv I_2 \mod N \right\}. \]

The quotient space \( \Gamma(N) \backslash \mathbb{H} \) is a Riemann surface \( Y(N) \) which can be compactified to a compact Riemann surface \( X(N) \) adding some points on the line \( \text{Im}(s) = 0 \). The meromorphic functions on \( X(N) \) are called modular functions of level \( N \).

The Riemann surfaces \( X(N) \) correspond to algebraic curves defined over the field \( \mathbb{Q}(\zeta_N) \). The Fourier expansions of modular functions of level \( N \) have coefficients in \( \mathbb{Q}(\zeta_N) \).
Modular functions of level $N$

We consider the group

$$\Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \text{ with } A \equiv l_2 \mod N \right\}.$$

The quotient space $\Gamma(N) \backslash \mathbb{H}$ is a Riemann surface $Y(N)$ which can be compactified to a compact Riemann surface $X(N)$ adding some points on the line $\text{Im}(s) = 0$. The meromorphic functions on $X(N)$ are called modular functions of level $N$.

The Riemann surfaces $X(N)$ correspond to algebraic curves defined over the field $\mathbb{Q}(\zeta_N)$. The Fourier expansions of modular functions of level $N$ have coefficients in $\mathbb{Q}(\zeta_N)$. 
Modular functions of level $N$

We consider the group 

$$\Gamma(N) = \left\{ A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \text{ with } A \equiv I_2 \mod N \right\}.$$ 

The quotient space $\Gamma(N) \backslash \mathbb{H}$ is a Riemann surface $Y(N)$ which can be compactified to a compact Riemann surface $X(N)$ adding some points on the line $\text{Im}(s) = 0$. The meromorphic functions on $X(N)$ are called modular functions of level $N$.

The Riemann surfaces $X(N)$ correspond to algebraic curves defined over the field $\mathbb{Q}(\zeta_N)$. The Fourier expansions of modular functions of level $N$ have coefficients in $\mathbb{Q}(\zeta_N)$. 
Modular functions of level $N$
M. Eichler

“There are five elementary arithmetical operations: addition, subtraction, multiplication, division, and modular forms.”
Theorem

Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of algebraic integers of the imaginary quadratic field $K$, and $x^2 + Bx + C$ the minimal polynomial of $\theta$. We consider a natural number $N > 1$ and $x_1, \ldots, x_n$ the generators of the group $(\mathcal{O}/N\mathcal{O})^*$, $x_i = a_i + b_i\theta \in \mathbb{Z}[\theta]$. We also consider the matrix

$$A_i = \begin{pmatrix} a_i - Bb_i & -Cb_i \\ b_i & a_i \end{pmatrix}.$$ 

If $f$ is a modular function of level $N$ and for all matrices $A_i$ we have

$$f(\theta) = f^{A_i}(\theta), \mathbb{Q}(j) \subset \mathbb{Q}(\theta),$$

then $f(\theta)$ generates the Hilbert class field.
\[ t_n = \sqrt{3} \frac{\eta(3\tau_n)\eta\left(\frac{1}{3}\tau_n + \frac{2}{3}\right)}{\eta^2(\tau_n)}, \]
\[ \tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \mod 24 \]

<table>
<thead>
<tr>
<th>( n )</th>
<th>( p_n(t) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>( t - 1 )</td>
</tr>
<tr>
<td>35</td>
<td>( t^2 + 1 - 1 )</td>
</tr>
<tr>
<td>59</td>
<td>( t^3 + 2t - 1 )</td>
</tr>
<tr>
<td>83</td>
<td>( t^3 + 2t^2 + 2t - 1 )</td>
</tr>
<tr>
<td>107</td>
<td>( t^3 - 2t^2 + 4t - 1 )</td>
</tr>
</tbody>
</table>

Claim \( p_n \) generate the Hilbert class field.
$$t_n = \sqrt{3} \frac{\eta(3\tau_n)\eta(\frac{1}{3}\tau_n+\frac{2}{3})}{\eta^2(\tau_n)},$$
\[
\tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \text{ mod } 24
\]

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p_n(t)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>$t - 1$</td>
</tr>
<tr>
<td>35</td>
<td>$t^2 + 1 - 1$</td>
</tr>
<tr>
<td>59</td>
<td>$t^3 + 2t - 1$</td>
</tr>
<tr>
<td>83</td>
<td>$t^3 + 2t^2 + 2t - 1$</td>
</tr>
<tr>
<td>107</td>
<td>$t^3 - 2t^2 + 4t - 1$</td>
</tr>
</tbody>
</table>

Claim: $p_n$ generate the Hilbert class field.
S. Ramanujan

\[ t_n = \sqrt{3} \frac{\eta(3\tau_n)\eta(\frac{1}{3}\tau_n+\frac{2}{3})}{\eta^2(\tau_n)}, \]

\[ \tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \mod 24 \]

<table>
<thead>
<tr>
<th>(n)</th>
<th>(p_n(t))</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>(t - 1)</td>
</tr>
<tr>
<td>35</td>
<td>(t^2 + 1 - 1)</td>
</tr>
<tr>
<td>59</td>
<td>(t^3 + 2t - 1)</td>
</tr>
<tr>
<td>83</td>
<td>(t^3 + 2t^2 + 2t - 1)</td>
</tr>
<tr>
<td>107</td>
<td>(t^3 - 2t^2 + 4t - 1)</td>
</tr>
</tbody>
</table>

**Claim** \(p_n\) generate the Hilbert class field.
"I learnt different areas of mathematics by trying to understand Ramanujan's work."
They proved that Ramanujan was right and they asked how polynomials for other values of $n$ can be constructed. E. Konstantinou and A.K. answered this question.

$$p_{299}(x) = x^8 + x^7 - x^6 - 12x^5 + 16x^4 - 12x^3 + 15x^2 - 13x + 1.$$
Can we find new invariants?

Shimura’s reciprocity law allows us to verify that a modular function generates the Hilbert’s class field. Can we construct such modular functions?

All known such invariants came out from extremely talented Mathematicians.
Can we find new invariants?

Shimura’s reciprocity law allows us to verify that a modular function generates the Hilbert’s class field. Can we construct such modular functions?

All known such invariants came out from extremely talented Mathematicians.
Invariants for common people

We can construct finitely dimensional vector spaces $V$ consisted of modular functions of level $N$ such that $GL(2, \mathbb{Z}/N\mathbb{Z})$ is acting on $V$. We write $a \in GL(2, \mathbb{Z}/N\mathbb{Z})$ as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in SL(2, \mathbb{Z}/N\mathbb{Z})$.

The group $SL(2, \mathbb{Z}/N\mathbb{Z})$ is generated by the elements $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

The action of $S$ on functions $g \in V$ is defined by $g \circ S = g(-1/z) \in V$ and the action of $T$ by $g \circ T = g(z + 1) \in V$. 
Invariants for common people

We can construct finitely dimensional vector spaces $V$ consisted of modular functions of level $N$ such that $GL(2, \mathbb{Z}/N\mathbb{Z})$ is acting on $V$. We write $a \in GL(2, \mathbb{Z}/N\mathbb{Z})$ as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in SL(2, \mathbb{Z}/N\mathbb{Z})$.

The group $SL(2, \mathbb{Z}/N\mathbb{Z})$ is generated by the elements $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

The action of $S$ on functions $g \in V$ is defined by $g \circ S = g(-1/z) \in V$ and the action of $T$ by $g \circ T = g(z + 1) \in V$. 
Invariants for common people

We can construct finitely dimensional vector spaces $V$ consisted of modular functions of level $N$ such that $GL(2, \mathbb{Z}/N\mathbb{Z})$ is acting on $V$. We write $a \in GL(2, \mathbb{Z}/N\mathbb{Z})$ as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in SL(2, \mathbb{Z}/N\mathbb{Z})$.

The group $SL(2, \mathbb{Z}/N\mathbb{Z})$ is generated by the elements $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

The action of $S$ on functions $g \in V$ is defined by $g \circ S = g(-1/z) \in V$ and the action of $T$ by $g \circ T = g(z + 1) \in V$. 
We can construct finitely dimensional vector spaces $V$ consisted of modular functions of level $N$ such that $GL(2, \mathbb{Z}/N\mathbb{Z})$ is acting on $V$. We write $a \in GL(2, \mathbb{Z}/N\mathbb{Z})$ as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in SL(2, \mathbb{Z}/N\mathbb{Z})$.

The group $SL(2, \mathbb{Z}/N\mathbb{Z})$ is generated by the elements $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

The action of $S$ on functions $g \in V$ is defined by $g \circ S = g(-1/z) \in V$ and the action of $T$ by $g \circ T = g(z + 1) \in V$. 
Finally the action \( \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \) is given by the action of elements \( \sigma_d \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \) on Fourier coefficients.

Since every element in \( \text{SL}(2, \mathbb{Z}/N\mathbb{Z}) \) is a word in \( S, T \) we have a function \( \rho \)

\[
\frac{\mathcal{O}}{N\mathcal{O}}^* \xrightarrow{\phi} \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \rightarrow \text{GL}(V), \tag{1}
\]

where \( \phi \) is the natural homomorphisms.
Finally the action \( \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \) is given by the action of elements \( \sigma_d \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \) on Fourier coefficients. Since every element in \( \text{SL}(2, \mathbb{Z}/N\mathbb{Z}) \) is a word in \( S, T \) we have a function \( \rho \)

\[
\begin{array}{ccc}
\frac{O}{N\mathcal{O}} \ast & \xrightarrow{\phi} & \text{GL}(2, \mathbb{Z}/N\mathbb{Z}) \\
\downarrow{\rho} & & \downarrow{\rightarrow} \\
& \text{GL}(V), & 
\end{array}
\]

(1)

where \( \phi \) is the natural homomorphisms.
The function $\rho$ as it is defined is not a homomorphism, but it satisfies the cocycle condition

$$\rho(\sigma \tau) = \rho(\tau) \rho(\sigma)^\tau$$

and gives rise to a class in $H^1(G, \text{GL}(V))$, where $G = (\mathcal{O}/N\mathcal{O})^*$. The restriction of $\rho$ on the subgroup $H = \ker \phi \subset G$ defined as

$$H := \{x \in G : \det(\phi(x)) = 1\}$$

is a homomorphism.
The function $\rho$ as it is defined is not a homomorphism, but it satisfies the cocycle condition

$$\rho(\sigma \tau) = \rho(\tau) \rho(\sigma)^\tau$$

and gives rise to a class in $H^1(G, \text{GL}(V))$, where $G = (\mathcal{O}/N\mathcal{O})^\ast$. The restriction of $\rho$ on the subgroup $H = \ker \phi \subset G$ defined as

$$H := \{ x \in G : \det(\phi(x)) = 1 \}$$

is a homomorphism.
Select a basis \( e_1, \ldots, e_m \) of \( V \)

Invariant theory gives us effective methods (Reynolds operator, diagonalization) for computing the ring of invariants \( \mathbb{Q}(\zeta_N)[e_1, \ldots, e_m]^H \).

We select the vector space \( V_n \) of invariant polynomials of degree \( n \).

The action of \( G/H \) on \( V_n \) gives a cocycle

\[
\rho' \in H^1(\text{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), \text{GL}(V_n)).
\]

Multidimensional Hilbert’s 90 theorem gives us the existence of \( P \in \text{GL}(V_n) \) so that

\[
\rho'(\sigma) = P^{-1}P^\sigma. \tag{3}
\]
Select a basis $e_1, \ldots, e_m$ of $V$

Invariant theory gives us effective methods (Reynolds operator, diagonalization) for computing the ring of invariants $\mathbb{Q}(\zeta_N)[e_1, \ldots, e_m]^H$.

We select the vector space $V_n$ of invariant polynomials of degree $n$.

The action of $G/H$ on $V_n$ gives a cocycle

$$\rho' \in H^1(\text{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}, \text{GL}(V_n)).$$

Multidimensional Hilbert’s 90 theorem gives us the existence of $P \in \text{GL}(V_n)$ so that

$$\rho'(\sigma) = P^{-1}P^\sigma. \quad (3)$$
Invariant Theory

Select a basis $e_1, \ldots, e_m$ of $V$

Invariant theory gives us effective methods (Reynolds operator, diagonalization) for computing the ring of invariants $\mathbb{Q}(\zeta_N)[e_1, \ldots, e_m]^H$.

We select the vector space $V_n$ of invariant polynomials of degree $n$.

The action of $G/H$ on $V_n$ gives a cocycle

$$\rho' \in H^1(\text{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), \text{GL}(V_n)).$$

Multidimensional Hilbert’s 90 theorem gives us the existence of $P \in \text{GL}(V_n)$ so that

$$\rho'(\sigma) = P^{-1}P^\sigma. \quad (3)$$
Computing $P$

Modified version of Glasby-Howlett probabilistic algorithm

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^\sigma.$$  \hspace{1cm} (4)

If we find a $2 \times 2$ matrix in $\text{GL}(2, \mathbb{Q}(\zeta_N))$ so that $B_Q$ is invertible, then $P := B_Q^{-1}$.

Since non invertible matrices are rare (they form a Zariski closed set in the space of matrices) finding such an invertible matrix is easy. The first random choice for $Q$ always worked!
Modified version of Glasby-Howlett probabilistic algorithm

\[ B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^\sigma. \]  \hspace{1cm} (4)

If we find a 2 × 2 matrix in \( \text{GL}(2, \mathbb{Q}(\zeta_N)) \) so that \( B_Q \) is invertible, then
\[ P := B_Q^{-1}. \]
Since non invertible matrices are rare (they form a Zariski closed set in the space of matrices) finding such an invertible matrix is easy. The first random choice for \( Q \) always worked!
Computing $P$

Modified version of Glasby-Howlett probabilistic algorithm

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^\sigma. \quad (4)$$

If we find a $2 \times 2$ matrix in $GL(2, \mathbb{Q}(\zeta_N))$ so that $B_Q$ is invertible, then

$$P := B_Q^{-1}. \quad (5)$$

Since non invertible matrices are rare (they form a Zariski closed set in the space of matrices) finding such an invertible matrix is easy. The first random choice for $Q$ always worked!
Examples

Generalized Weber functions $g_0$, $g_1$, $g_2$, $g_3$

$$g_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)}, \quad g_1(\tau) = \zeta_{24}^{-1} \frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},$$

$$g_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)}, \quad g_3(\tau) = \sqrt{3} \frac{\eta(3\tau)}{\eta(\tau)},$$

They are modular functions of level $72$. 
Examples

Generalized Weber functions $g_0, g_1, g_2, g_3$

\[ g_0(\tau) = \frac{\eta\left(\frac{\tau}{3}\right)}{\eta(\tau)}, \quad g_1(\tau) = \zeta_{24}^{-1} \frac{\eta\left(\frac{\tau+1}{3}\right)}{\eta(\tau)}, \]

\[ g_2(\tau) = \frac{\eta\left(\frac{\tau+2}{3}\right)}{\eta(\tau)}, \quad g_3(\tau) = \sqrt{3} \frac{\eta(3\tau)}{\eta(\tau)}, \]

They are modular functions of level 72.
Example

For $n = -571$ the group $H$ has order 144 and $G$ has order 3456. We compute that the polynomials

$$l_1 := g_0g_2 + \zeta_{72}^6 g_1g_3, \quad l_2 := g_0g_3 + (-\zeta_{72}^{18} + \zeta_{72}^6)g_1g_2$$

are invariant under the action of $H$.

Final invariants

$$e_1 := (-12\zeta_{72}^{18} + 12\zeta_{72}^6)g_0g_3 + 12\zeta_{72}^6 g_0g_3 + 12g_1g_2 + 12g_1g_3,$$

$$e_2 := 12\zeta_{72}^6 g_1g_2 + (-12\zeta_{72}^{18} + 12\zeta_{72}^6)g_0g_3 + (-12\zeta_{72}^{12} + 12)g_1g_3 + 12\zeta_{72}^{12} g_1g_3$$

Every $\mathbb{Z}$-linear combination of $e_1, e_2$ is also an invariant.
Example

For $n = -571$ the group $H$ has order 144 and $G$ has order 3456. We compute that the polynomials

$$l_1 := g_0 g_2 + \zeta_7^6 g_1 g_3,$$

$$l_2 := g_0 g_3 + (-\zeta_7^{18} + \zeta_7^6) g_1 g_2$$

are invariant under the action of $H$.

Final invariants

$$e_1 := (-12\zeta_7^{18} + 12\zeta_7^6) g_0 g_3 + 12\zeta_7^6 g_0 g_3 + 12 g_1 g_2 + 12 g_1 g_3,$$

$$e_2 := 12\zeta_7^6 g_1 g_2 + (-12\zeta_7^{18} + 12\zeta_7^6) g_0 g_3 + (-12\zeta_7^{12} + 12) g_1 g_3 + 12\zeta_7^{12} g_1 g_3$$

Every $\mathbb{Z}$-linear combination of $e_1, e_2$ is also an invariant.
### Examples

<table>
<thead>
<tr>
<th>Invariant</th>
<th>Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hilbert</td>
<td>$t^5 + 400497845154831586723701480652800t^4 + 818520809154613065770038265334290448384t^3 + 4398250752422094811238689419574422303726895104t^2 - 16319730975176203906274913715913862844512542392320t + 15283054453672803818066421650036653646232315192410112$</td>
</tr>
<tr>
<td>$g_0^{12} g_1^{12} + g_2^{12} g_3^{12}$</td>
<td>$t^5 - 5433338830617345268674t^4 + 90705913519542658324778088t^3 - 3049357177530030535811751619728t^2 - 39007182691221442431043741686448t - 1250992052647780072147837007511456$</td>
</tr>
<tr>
<td>$e_1$</td>
<td>$t^5 - 936t^4 - 60912t^3 - 2426112t^2 - 40310784t - 3386105856$</td>
</tr>
<tr>
<td>$e_2$</td>
<td>$t^5 - 1512t^4 - 29808t^3 + 979776t^2 + 3359232t - 423263232$</td>
</tr>
</tbody>
</table>
Generalized Weber Functions

\[ \nu_{N,0} := \sqrt{N} \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \nu_{k,N} := \eta \begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}, \quad 0 \leq k \leq N - 1. \]

These are known to be modular functions of level \( 24N \). Notice that \( \sqrt{N} \in \mathbb{Q}(\zeta_N) \subset \mathbb{Q}(\zeta_{24N}) \) and an explicit expression of \( \sqrt{N} \) in terms of \( \zeta_N \) can be given by using Gauss sums.
Generalized Weber Functions

\[ \nu_{N,0} := \sqrt{N} \frac{\eta \circ \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}}{\eta} \quad \text{and} \quad \nu_{k,N} := \frac{\eta \circ \begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}}{\eta}, \quad 0 \leq k \leq N - 1. \]

These are known to be modular functions of level \(24N\). Notice that \(\sqrt{N} \in \mathbb{Q}(\zeta_N) \subset \mathbb{Q}(\zeta_{24N})\) and an explicit expression of \(\sqrt{N}\) in terms of \(\zeta_N\) can be given by using Gauss sums.
Action of $\text{SL}(2, \mathbb{Z})$

In order to describe the $\text{SL}(2, \mathbb{Z})$-action we have to describe the action of the two generators $S, T$ of $\text{SL}(2, \mathbb{Z})$ given by $S : z \mapsto -\frac{1}{z}$ and $T : z \mapsto z + 1$. Keep in mind that

$$\eta \circ T(z) = \zeta_{24}\eta(z) \quad \text{and} \quad \eta \circ S(z) = \zeta_{8}^{-1}\sqrt{iz}\eta(z).$$

We compute that

$$\nu_{N,0} \circ S = \nu_{0,N} \quad \text{and} \quad \nu_{N,0} \circ T = \zeta_{24}^{-N-1}\nu_{N,0},$$

$$\nu_{0,N} \circ S = \nu_{N,0} \quad \text{and} \quad \nu_{0,N} \circ T = \zeta_{24}^{-1}\nu_{1,N},$$

for $1 \leq k < N - 1$ and $N$ is prime

$$\nu_{k,N} \circ S = \left(\frac{-c}{n}\right)^{\frac{1-n}{2}}\zeta_{24}^{N(k-c)}\nu_{k,N} \quad \text{and} \quad \nu_{k,N} \circ T = \zeta_{24}^{-1}\nu_{k+1,N},$$

where $c = -k^{-1} \mod N$. 
Example = 5

Assume that $N = 5$ and $D = -91$. We compute that the group $H$ of determinant 1 has invariants

$$\nu_{5,0} + (\zeta^{25} - \zeta^5)\nu_{3,5} \text{ and } \nu_{0,5} + (\zeta^{31} - \zeta^{23} - \zeta^{19} - \zeta^{15} + \zeta^7 + \zeta^3)\nu_{1,5}. $$

Using our method we arrive at the final invariants:

$$I_1 = (-1224\zeta^{28} + 612\zeta^{20} + 2740\zeta^{16} + 1516\zeta^{14} - 612)\nu_{5,0} + (4256\zeta^{28} - 2128\zeta^{20} - 1516\zeta^{16} + 2740\zeta^{14} + 2128)\nu_{0,5} + (-1224\zeta^{31} - 2740\zeta^{27} + 612\zeta^{15} + 1224\zeta^{11} + 1516\zeta^{3})\nu_{1,5} + (1516\zeta^{29} - 612\zeta^{25} + 1224\zeta^{13} - 1516\zeta^{9} - 2740\zeta)\nu_{3,5},$$

$$I_2 = (-1952\zeta^{28} + 976\zeta^{20} + 2128\zeta^{16} + 176\zeta^{4} - 976)\nu_{5,0} + (2304\zeta^{28} - 1152\zeta^{20} - 176\zeta^{16} + 2128\zeta^{4} + 1152)\nu_{0,5} + (-1952\zeta^{31} - 2128\zeta^{27} + 976\zeta^{15} + 1952\zeta^{11} + 176\zeta^{3})\nu_{1,5} + (176\zeta^{29} - 976\zeta^{25} + 1952\zeta^{13} - 176\zeta^{9} - 2128\zeta)\nu_{3,5}. $$

The $\mathbb{Q}$-vector space generated by these two functions consists of class functions.
We can now compute the corresponding polynomials:

\[ t^2 - 3060t - 28090800 \text{ and } t^2 - 4880t - 71443200. \]

Just for comparison the Hilbert polynomial corresponding to the \( j \) invariant is:

\[ t^2 + 10359073013760t - 3845689020776448. \]
Questions - further research

1. **Select the best invariants**

   Minimizing height in a lattice

2. By examples we see that the best invariants are in the case of monomials

3. There are cases $n \mod 24$ where no monomial invariants exist. In these cases our method gives us the best known results.
1. Select the best invariants: Minimizing height in a lattice

2. By examples we see that the best invariants are in the case of monomials

3. There are cases $n \mod 24$ where no monomial invariants exist. In these cases our method gives us the best known results.
1. Select the best invariants: Minimizing height in a lattice
2. By examples we see that the best invariants are in the case of monomials
3. There are cases $n \mod 24$ where no monomial invariants exist. In these cases our method gives us the best known results.
1. Select the best invariants: Minimizing height in a lattice
2. By examples we see that the best invariants are in the case of monomials
3. There are cases $n \mod 24$ where no monomial invariants exist. In these cases our method gives us the best known results.
Thank you!
E. Konstantinou, A. Kontogeorgis Computing polynomials of the Ramanujan $t_n$ class invariants

E. Konstantinou, A. Kontogeorgis
Ramanujan invariants for discriminants congruent to $5 \pmod{2^4}$

A. Kontogeorgis
Constructing class invariants