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

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION & RELIGIOUS AFFAIRS
MANAGING AUTHORITY
Co-financed by Greece and the European Union

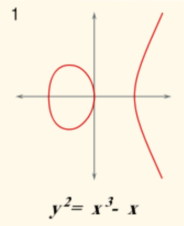
NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND

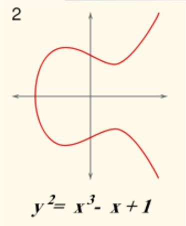
Contents

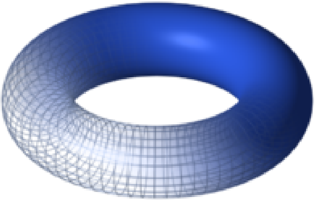
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013

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

$$E : y^2 = x^3 + ax + b \text{ such that } 4a^3 + 27b^2 \neq 0.$$



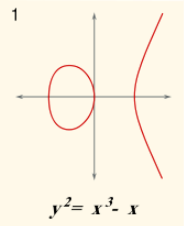


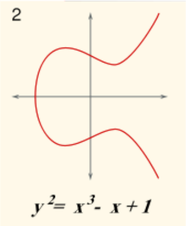


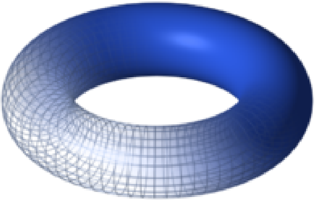
The set of points $E(K)$ together with a point at infinity is an abelian group.

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

$$E : y^2 = x^3 + ax + b \text{ such that } 4a^3 + 27b^2 \neq 0.$$







The set of points $E(K)$ together with a point at infinity is an abelian group.

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

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

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 usualy: $\mathbb{F}_{p^r}^*$, 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.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

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

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

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 usualy: $\mathbb{F}_{p^r}^*$, 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

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

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 usualy: $\mathbb{F}_{p^r}^*$, 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.

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

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

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

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 usualy: $\mathbb{F}_{p^r}^*$, 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.

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

Elliptic curves defined over finite fields

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

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

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 usualy: $\mathbb{F}_{p^r}^*, E$.

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.

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

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 $L = \mathbb{Z} + \tau\mathbb{Z}$, $\Im(\tau) > 0$. Lettices L, L' give the same elliptic curves if and only if

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

The quotient map

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

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

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 +$$

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

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

The quotient map

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

is called the j-invariant. It is a $\mathrm{SL}(2, \mathbb{Z})$- 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 $L = \mathbb{Z} + \tau\mathbb{Z}$, $\Im(\tau) > 0$. Lettices L, L' give the same elliptic curves if and only if

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

The quotient map

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

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

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 +$$

Επιχειρησιακό Πρόγραμμα Εκπαίδευση και Δια Βίου Μάθηση · ΕΣΠΑ 2007-2013 · Ευρωπαϊκή Ένωση

Remarks: The coefficients of the Fourier expansion are integers. They are related to the dimensions of the irreducible representations of the Monster, the bigest sporadic simple group with order

$$808017424794512875886459904961710757005754368000000000.$$

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.

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

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.

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

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.

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

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013 ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Class 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 $PI(\mathcal{O})$ of principal fractional ideals $a\mathcal{O}$, where $a \in K$.

The quotient is the class group

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

One can show that the class group is a finite group.

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013

Class 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 $PI(\mathcal{O})$ of principal fractional ideals $a\mathcal{O}$, where $a \in K$.

The quotient is the class group

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

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 $PI(\mathcal{O})$ of principal fractional ideals $a\mathcal{O}$, where $a \in K$.

The quotient is the class group

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

One can show that the class group is a finite group.

Class 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 $PI(\mathcal{O})$ of principal fractional ideals $a\mathcal{O}$, where $a \in K$.

The quotient is the class group

$$\mathrm{Cl}(\mathcal{O}) = \frac{I(\mathcal{O})}{PI(\mathcal{O})}.$$

One can show that the class group is a finite group.

Ramification)

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 exension 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 exension 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 exension 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 . For the Galois group is the class group of K $\mathrm{Gal}(H_K/K) = \mathrm{Cl}(\mathcal{O}_K)$.
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 $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ canot have unramified covers therefore are in some sence ``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 globaly trivial''. The group

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

Theorem

For every number field there is a Galois extension H_K defined to be the maximal unramified abelian extension of . For the Galois group is the class group of K $\mathrm{Gal}(H_K/K) = \mathrm{Cl}(\mathcal{O}_K)$.
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 $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$ canot have unramified covers therefore are in some sence ``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 globaly trivial''. The group

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

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

D. Hilbert

Construction of the Hilbert class field

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

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

We will show soon that these are the endomorphisms of an elliptic curve with complex multiplication.

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 $\mathrm{SL}(2, \mathbb{Z})$ sending one to the other. The equivalence classes are in one to one corespondence to the class group and they can computed easily since a full set of representatives is given by elements (a, b, c) such that

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

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

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 $\mathrm{SL}(2, \mathbb{Z})$ sending one to the other. The equivalence classes are in one to one corespondence to the class group and they can computed easily since a full set of representatives is given by elements (a, b, c) such that

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

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

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 $\mathrm{SL}(2, \mathbb{Z})$ sending one to the other. The equivalence classes are in one to one corespondence to the class group and they can computed easily since a full set of representatives is given by elements (a, b, c) such that

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

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

K.F. Gauss

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

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

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

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

Finite fields

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

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

$$N_p = p + 1 \pm \mathrm{tr}(\mathrm{F})$$

Complex multiplication

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

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

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

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

Finite fields

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

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

$$N_p = p + 1 \pm \mathrm{tr}(\mathrm{F})$$

Complex multiplication

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

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

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

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

Finite fields

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

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

$$N_p = p + 1 \pm \mathrm{tr}(\mathrm{F})$$

theorem

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. $\mathrm{End}(E_\tau) = E_\tau$.
2. $j(\tau) = j(E_\tau)$ is an algebraic integer. Its irreducible polynomial is given by the equation
$$H_D(x) = \prod_{[a,b,c]\in \mathrm{CL}(\mathrm{K})} \left(x - j\left(\frac{-b+\sqrt{-D}}{2a} \right) \right) \in \mathbb{Z}[x].$$
3. The element $j(\tau)$ generates the Hilber class field.

Kronecker-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-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).

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

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).

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-discriminatnt for the prime p

4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$

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-discriminatnt for the prime p
4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$

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-discriminatnt for the prime p
4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

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-discriminatnt for the prime p
4. $$x^2 - \mathrm{tr}(F)x + p \mapsto \Delta = \mathrm{tr}(F)^2 - 4p = -Dv^2.$$

Reduction of elliptic curve modulo $\bmod p$

$$\begin{array}{ccc}
(\mathbb{C}) & \tau \in \mathrm{End}(E(\mathbb{C})) & j \text{ is a root of } H_D(x) \in \mathbb{Z}[x] \\
\Big\downarrow & \Big\downarrow & \Big\downarrow \\
(\mathbb{F}_p) & F \in \mathrm{End}(E(\mathbb{F}_p)) & j \text{ is a root of } H_D(x) \bmod p \in \mathbb{F}_p[x]
\end{array}$$

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 $H_D(x) \bmod p$. One root if the j invariant we are looking for which can be given by (for $j \neq 0, 1728$)

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

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

There is a problem!

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

$$x^8 + 391086320728105978429440x^7$$

$$-28635280874816126174326167699456x^6$$

$$+20940554100063221466514911307211336581 12x^5 -$$

$$1865472607707568299619716756851517912965447 68x^4$$

$$+641714127813321866528980865595427518152371811 1232x^3$$

$$-1920783944359448882293698894383617711522787722 7364352x^2$$

$$+457975288082151501362489753632018607243512256948024 11520x -$$

$$18273883965326272223717626628647422907813731016193733558272$$

Dedekind's η-function

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

which leads to the Weber functions:

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

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

What is special about them?

They are modular functions

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013

Dedekind's η-function

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

which leads to the Weber functions:

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

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

What is special about them?

They are modular functions

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

Dedekind's η-function

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

which leads to the Weber functions:

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

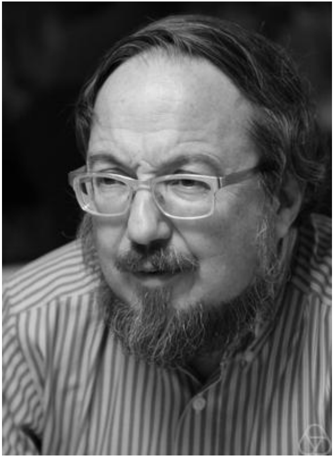
Which can also producte the Hilbert class field (D. Zagier- N. Yui).

What is special about them?

They are modular functions

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013

D. Zagier - N. Yui



Modular functions of level N

We consider the group

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

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 $\mathrm{Im}(s) = 0$. 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

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

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 $\mathrm{Im}(s) = 0$. 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

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

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 $\mathrm{Im}(s) = 0$. 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

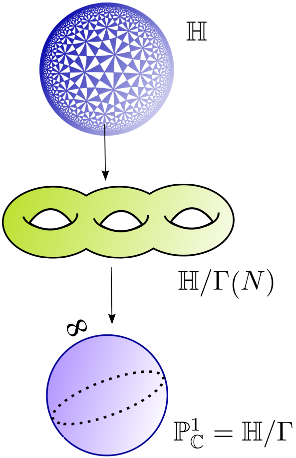
We consider the group

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

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 $\mathrm{Im}(s) = 0$. 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 $\mathbb{Q}(\zeta_N)$.

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013 ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

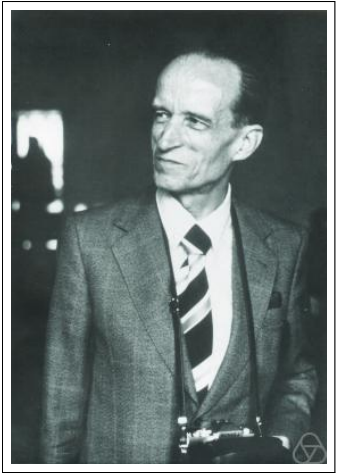
Modular functions of level N



$$\left.\begin{array}{c}\mathcal{M}(X(N))\\ \Big\uparrow \\ \mathbb{C}(t)\end{array}\right\}\ \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$$

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 θ. 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

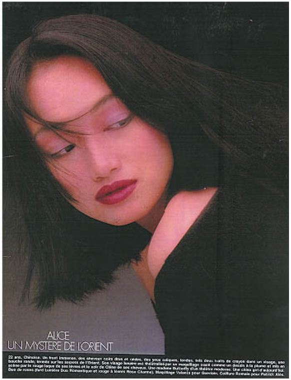
$$A_i = \begin{pmatrix} a_i - Bb_i & -Cb_i \\ b_i & a_i \end{pmatrix}.$$

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.

G. Shimura - P. Stevenhagen - A. Gee



S. Ramanujan

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

$$\tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \bmod 24$$

n	$p_n(t)$
11	$t-1$
35	t^2+1-1
59	t^3+2t-1
83	t^3+2t^2+2t-1
107	t^3-2t^2+4t-1

Claim p_n generate the Hilbert class field.

S. Ramanujan

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

$$\tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \bmod 24$$

n	$p_n(t)$
11	$t-1$
35	t^2+1-1
59	t^3+2t-1
83	t^3+2t^2+2t-1
107	t^3-2t^2+4t-1

Claim p_n generate the Hilbert class field.

S. Ramanujan

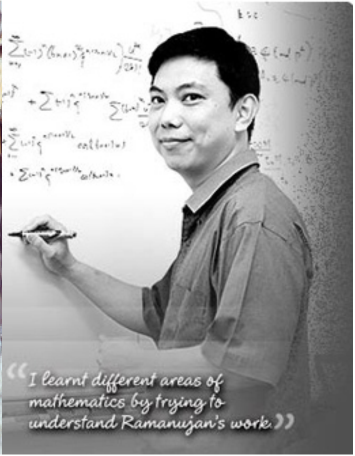
$$t_n = \sqrt{3}\frac{\eta(3\tau_n)\eta(\frac{1}{3}\tau_n+\frac{2}{3})}{\eta^2(\tau_n)},$$

$$\tau_n = -\frac{1}{2} + i\frac{\sqrt{n}}{2}, n \equiv 11 \bmod 24$$

n	$p_n(t)$
11	$t-1$
35	t^2+1-1
59	t^3+2t-1
83	t^3+2t^2+2t-1
107	t^3-2t^2+4t-1

Claim p_n generate the Hilbert class field.

B. Berndt & Heng Huat Chan



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

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

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013

E. Konstantinou

H.H. Chan

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

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.

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013

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

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

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 $g \circ T = g(z+1) \in V$.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

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

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

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 $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is acting on V. We write $a \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$.

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

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 $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ is acting on V. We write $a \in \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$.

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

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 $g \circ T = g(z+1) \in V$.

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013

Actions

Finaly the action $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ is given by the action of elements $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on Fourier coefficients.

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

$$\begin{tikzcd} \left(\frac{\mathcal{O}}{N\mathcal{O}}\right)^* \arrow[r, "\phi"] \arrow[rr, bend left, "\rho"] & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{GL}(V), \end{tikzcd} \tag{1}$$

where ϕ is the natural homomorphisms.

Actions

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

$$\begin{tikzcd} \left(\frac{\mathcal{O}}{N\mathcal{O}}\right)^* \arrow[r, "\phi"] \arrow[rr, bend left, "\rho"] & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{GL}(V), \end{tikzcd} \tag{1}$$

where ϕ is the natural homomorphisms.

Cocylces

The function ρ as it is defined is not a homomorphism, but it satisfies the cocycle condition

$$\rho(\sigma\tau) = \rho(\tau)\rho(\sigma)^{\tau} \tag{2}$$

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

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

is a homomorphism.

Cocylces

The function ρ as it is defined is not a homomorphism, but it satisfies the cocycle condition

$$\rho(\sigma\tau) = \rho(\tau)\rho(\sigma)^\tau \tag{2}$$

and gives rise to a class in $H^1(G, \mathrm{GL}(V))$, where $G = (\mathcal{O}/N\mathcal{O})^*$. The restriction of ρ 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

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

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

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

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013

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

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

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

The action of G/H on V_n gives a cocycle

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

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

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

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013

Select a basis $e_1, \dots, e_m$ of V
Invariant theory gives us effective methods (Reynolds operator, diagonalization) for computing the ring of invariants $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H$.
We select the vector space V_n of invariant polynomials of degree n.
The action of G/H on V_n gives a cocycle

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

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

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

Computing P

Modified version of Glasby-Howlett probabilistic algorithm

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

If we find a 2×2 matrix in $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ 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

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

If we find a 2×2 matrix in $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ 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

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

If we find a 2×2 matrix in $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ 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!

Generalized Weber functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)},\ \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},$$

$$\mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)},\ \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

They are modular functions of level 72.

Examples

Generalized Weber functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)},\ \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},$$

$$\mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)},\ \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

They are modular functions of level 72.

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

Example

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

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^{6})\mathfrak{g}_1\mathfrak{g}_2$$

are invariant under the action of H.

Final invariants

$$e_1 := (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + 12\zeta_{72}^{6}\mathfrak{g}_0\mathfrak{g}_3 + 12\mathfrak{g}_1\mathfrak{g}_2 + 12\mathfrak{g}_1\mathfrak{g}_3,$$

$$e_2 := 12\zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_2 + (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + (-12\zeta_{72}^{12} + 12)\mathfrak{g}_1\mathfrak{g}_3 + 12\zeta_{72}^{12}\mathfrak{g}_1\mathfrak{g}_3$$

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

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^{6})\mathfrak{g}_1\mathfrak{g}_2$$

are invariant under the action of H.

Final invariants

$$e_1 := (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + 12\zeta_{72}^{6}\mathfrak{g}_0\mathfrak{g}_3 + 12\mathfrak{g}_1\mathfrak{g}_2 + 12\mathfrak{g}_1\mathfrak{g}_3,$$

$$e_2 := 12\zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_2 + (-12\zeta_{72}^{18} + 12\zeta_{72}^{6})\mathfrak{g}_0\mathfrak{g}_3 + (-12\zeta_{72}^{12} + 12)\mathfrak{g}_1\mathfrak{g}_3 + 12\zeta_{72}^{12}\mathfrak{g}_1\mathfrak{g}_3$$

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

Examples

Invariant	polynomial
Hilbert	$t^5 + 400497845154831586723701480652800t^4 + 818520809154613065770038265334290448384t^3 + 4398250752422094811238689419574422303726895104t^2 - 16319730975176203906274913715913862844512542392320t + 15283054453672803818066421650036653646232315192410112$
$\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}$	$t^5 - 5433338830617345268674t^4 + 90705913519542658324778088t^3 - 3049357177530030535811751619728t^2 - 390071826912221442431043741686448t - 12509992052647780072147837007511456$
e_1	$t^5 - 936t^4 - 60912t^3 - 2426112t^2 - 40310784t - 3386105856$
e_2	$t^5 - 1512t^4 - 29808t^3 + 979776t^2 + 3359232t - 423263232$

Generalized Weber Functions

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

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

Ευρωπαϊκή Ένωση
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013

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

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

Action of $\mathrm{SL}(2,\mathbb{Z})$

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

$$\eta \circ T(z) = \zeta_{24}\eta(z) \text{ and } \eta \circ S(z) = \zeta_8^{-1}\sqrt{iz}\eta(z).$$

We compute that

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

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

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

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

where $c = -k^{-1} \bmod N$.

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:

$$\begin{aligned} I_1 &= (-1224\zeta^{28} + 612\zeta^{20} + 2740\zeta^{16} + 1516\zeta^{4} - 612)\nu_{5,0} \\ &+(4256\zeta^{28} - 2128\zeta^{20} - 1516\zeta^{16} + 2740\zeta^{4} + 2128)\nu_{0,5} \\ &+(-1224\zeta^{31} - 2740\zeta^{27} + 612\zeta^{15} + 1224\zeta^{11} + 1516\zeta^{3})\nu_{1,5} \\ &+(1516\zeta^{29} - 612\zeta^{25} + 1224\zeta^{13} - 1516\zeta^{9} - 2740\zeta)\nu_{3,5}, \end{aligned}$$

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

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 - furhter research

1. Select the best invariantsMinimizing height in a lattice
2. By examples we see that the best invariants are in the case of monomials
3. There are cases $n \bmod 24$ where no monomial invariants exist. In these cases our method gives us the best known results.

Questions - furhter research

1. Select the best invariantsMinimizing height in a lattice
2. By examples we see that the best invariants are in the case of monomials
3. There are cases $n \bmod 24$ where no monomial invariants exist. In these cases our method gives us the best known results.

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013

Questions - furhter research

1. Select the best invariantsMinimizing height in a lattice
2. By examples we see that the best invariants are in the case of monomials
3. There are cases $n \bmod 24$ where no monomial invariants exist. In these cases our method gives us the best known results.

Questions - furhter research

1. Select the best invariantsMinimizing 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!

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

- E. Konstantinou, A. Kontogeorgis Computing polynomials of the Ramanujan t_n class invariants
Canad. Math. Bull., Vol. 52, No. 4, pg. 583--597, 2009.
- E. Konstantinou, A. Kontogeorgis
Ramanujan invariants for discriminants congruent to $5 \pmod{2}4$
em Int. J. Number Theory, Vol. 8, No. 1, pg. 265--287, 2012.
- A. Kontogeorgis
Constructing class invariants
In *Math. Comp.*, Vol. 83, No. 287, pg. 1477--1488, 2014.

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2007-2013