Singular Moduli

Alex J. Best

WIMP 2014

29/11/2014

In this talk:

Observations (Hermite, 1859):

$$e^{\pi\sqrt{43}} \approx 884736743.999777466$$

Observations (Hermite, 1859):

$$e^{\pi\sqrt{43}} \approx 884736743.999777466$$

$$e^{\pi\sqrt{67}} \approx 147197952743.999998662454$$

Observations (Hermite, 1859):

$$e^{\pi\sqrt{43}} \approx 884736743.999777466$$

$$e^{\pi\sqrt{67}} \approx 147197952743.999998662454$$

$$e^{\pi\sqrt{163}} \approx 262537412640768743.99999999999925007$$

Observations (Hermite, 1859):

$$
\begin{aligned}
e^{\pi\sqrt{43}} &\approx 884736743.999777466 \\
&\approx 12^3(9^2-1)^3 + 744 - 10^{-4}\cdot 2.225\ldots \\
e^{\pi\sqrt{67}} &\approx 147197952743.999998662454 \\
&\approx 12^3(21^2-1)^3 + 744 - 10^{-6}\cdot 1.337\ldots \\
e^{\pi\sqrt{163}} &\approx 262537412640768743.99999999999925007 \\
&\approx 12^3(231^2-1)^3 + 744 - 10^{-13}\cdot 7.499\ldots
\end{aligned}
$$

Some definitions

Definition

A finite Galois extension $L|K$ is **abelian** extension if $\mathrm{Gal}(L|K)$ is abelian.

Some definitions

Definition

A finite Galois extension $L|K$ is **abelian** extension if $\mathrm{Gal}(L|K)$ is abelian.

Examples:

Some definitions

Definition

A finite Galois extension $L|K$ is **abelian** extension if $\mathrm{Gal}(L|K)$ is abelian.

Examples:

Non-examples:

The ideal class group

Given a number field K we let

$$I(\mathbf{Z}_K) = \{\}$$

be the set of **fractional** ideals of $\mathbf{Z}_K$.

The ideal class group

Given a number field K we let

$$I(\mathbf{Z}_K) = \{\}$$

be the set of **fractional** ideals of $\mathbf{Z}_K$. This is an (abelian) group!

The ideal class group

Given a number field K we let

$$I(\mathbf{Z}_K) = \{\}$$

be the set of **fractional** ideals of $\mathbf{Z}_K$. This is an (abelian) group!
The set

$$P(\mathbf{Z}_K) = \{a\mathbf{Z}_K : a \in K\}$$

of **principal** ideals is a subgroup.

The ideal class group

Given a number field K we let

$$I(\mathbf{Z}_K) = \{\}$$

be the set of **fractional** ideals of $\mathbf{Z}_K$. This is an (abelian) group! The set

$$P(\mathbf{Z}_K) = \{a\mathbf{Z}_K : a \in K\}$$

of **principal** ideals is a subgroup.

Definition

The **ideal class group** of a number field K is the quotient

$$\mathrm{cl}(\mathbf{Z}_K) = I(\mathbf{Z}_K)/P(\mathbf{Z}_K).$$

The ideal class group

Given a number field K we let

$$I(\mathbf{Z}_K) = \{\}$$

be the set of **fractional** ideals of $\mathbf{Z}_K$. This is an (abelian) group! The set

$$P(\mathbf{Z}_K) = \{a\mathbf{Z}_K : a \in K\}$$

of **principal** ideals is a subgroup.

Definition

The **ideal class group** of a number field K is the quotient

$$\mathrm{cl}(\mathbf{Z}_K) = I(\mathbf{Z}_K)/P(\mathbf{Z}_K).$$

$\mathrm{cl}(\mathbf{Z}_K)$ **measures** how far $\mathbf{Z}_K$ is from having unique factorisation.

The Hilbert class field (of an imaginary quadratic field)

Let K be an **imaginary quadratic** number field, i.e. $K = \mathbf{Q}(\sqrt{-n})$ for some $n \in \mathbf{Z}_{\geq 1}$.

The Hilbert class field (of an imaginary quadratic field)

Let K be an **imaginary quadratic** number field, i.e. $K = \mathbf{Q}(\sqrt{-n})$ for some $n \in \mathbf{Z}_{\geq 1}$.

Definition

An extension $L|K$ is **unramified** if for all prime ideals $\mathfrak{p}$ of $\mathbf{Z}_K$ we have a factorisation

$$\mathfrak{p}\,\mathbf{Z}_L = \mathfrak{P}_1\,\mathfrak{P}_2\cdots\mathfrak{P}_n$$

into **distinct** prime ideals $\mathfrak{P}_i$ of $\mathbf{Z}_L$.

The Hilbert class field (of an imaginary quadratic field)

Let K be an **imaginary quadratic** number field, i.e. $K = \mathbf{Q}(\sqrt{-n})$ for some $n \in \mathbf{Z}_{\geq 1}$.

Definition

An extension $L|K$ is **unramified** if for all prime ideals $\mathfrak{p}$ of $\mathbf{Z}_K$ we have a factorisation

$$\mathfrak{p}\,\mathbf{Z}_L = \mathfrak{P}_1\,\mathfrak{P}_2 \cdots \mathfrak{P}_n$$

into **distinct** prime ideals $\mathfrak{P}_i$ of $\mathbf{Z}_L$.

Definition

The **Hilbert class field** of K is the maximal unramified abelian extension of K.

The Hilbert class field (of an imaginary quadratic field)

Definition

The **Hilbert class field** of K is the maximal unramified abelian extension of K.

Examples

K	Hilbert class field L	$\mathrm{Gal}(L\vert K)$
$\mathbf{Q}(\sqrt{-1})$	$\mathbf{Q}(\sqrt{-1})$	1

The Hilbert class field (of an imaginary quadratic field)

Definition

The **Hilbert class field** of K is the maximal unramified abelian extension of K.

Examples

K	Hilbert class field L	$\mathrm{Gal}(L\mid K)$
$\mathbf{Q}(\sqrt{-1})$	$\mathbf{Q}(\sqrt{-1})$	1
$\mathbf{Q}(\sqrt{-31})$	$\mathbf{Q}(\sqrt{-31})[x]/(x^3+x-1)$	C_3

The Hilbert class field (of an imaginary quadratic field)

Definition

The **Hilbert class field** of K is the maximal unramified abelian extension of K.

Examples

K	Hilbert class field L	$\mathrm{Gal}(L\|K)$
$\mathbf{Q}(\sqrt{-1})$	$\mathbf{Q}(\sqrt{-1})$	1
$\mathbf{Q}(\sqrt{-31})$	$\mathbf{Q}(\sqrt{-31})[x]/(x^3+x-1)$	C_3
$\mathbf{Q}(\sqrt{-159})$	$\mathbf{Q}(\sqrt{-159})[x]/(x^{10}-3x^9+6x^8 -6x^7+3x^6+3x^5-9x^4 +13x^3-12x^2+6x-1)$	C_{10}

The Hilbert class field (of an imaginary quadratic field)

Definition

The **Hilbert class field** of K is the maximal unramified abelian extension of K.

Examples

K	Hilbert class field L	$\mathrm{Gal}(L\|K)$
$\mathbf{Q}(\sqrt{-1})$	$\mathbf{Q}(\sqrt{-1})$	1
$\mathbf{Q}(\sqrt{-31})$	$\mathbf{Q}(\sqrt{-31})[x]/(x^3+x-1)$	C_3
$\mathbf{Q}(\sqrt{-159})$	$\mathbf{Q}(\sqrt{-159})[x]/(x^{10}-3x^9+6x^8-6x^7+3x^6+3x^5-9x^4+13x^3-12x^2+6x-1)$	C_{10}
$\mathbf{Q}(\sqrt{-163})$	$\mathbf{Q}(\sqrt{-163})$	1

The Artin reciprocity theorem for the Hilbert class field

Theorem

If K is a number field and L is its Hilbert class field then

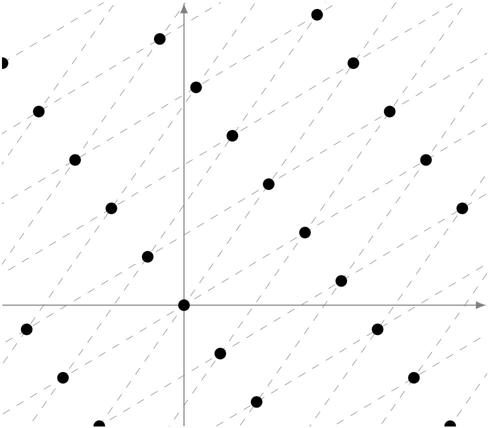
$$\mathrm{cl}(\mathbf{Z}_K) \cong \mathrm{Gal}(L|K).$$

$$\begin{tikzcd} L \arrow[d, dash, "\mathrm{Gal}(L|K)"] \\ K \arrow[d, dash] \\ \mathbf{Q} \end{tikzcd}$$

Lattices

Definition

A **lattice** is an additive subgroup of $\mathbf{C}$ that is isomorphic to $\mathbf{Z}^2$.



Homothety

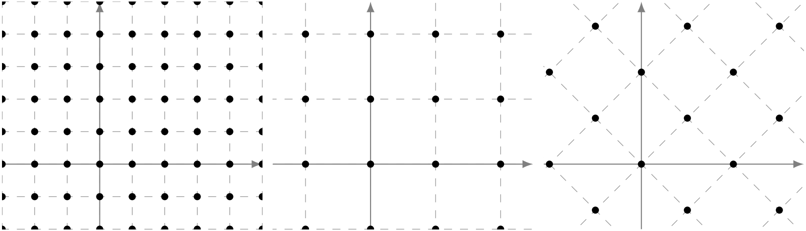
Definition

Two lattices L and L' are called **homothetic** if $L = \lambda L'$ for some $\lambda \in \mathbf{C}^*$.

Homothety

Definition

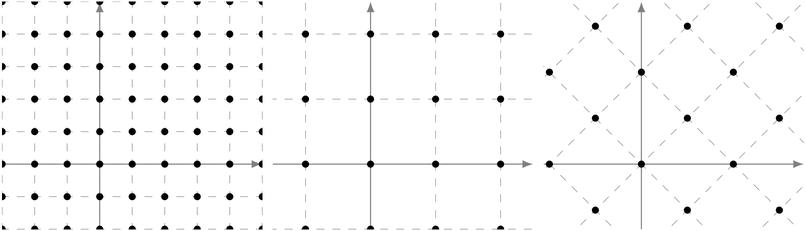
Two lattices L and L' are called **homothetic** if $L = \lambda L'$ for some $\lambda \in \mathbf{C}^*$.



Homothety

Definition

Two lattices L and L' are called **homothetic** if $L = \lambda L'$ for some $\lambda \in \mathbf{C}^*$.



Every lattice is homothetic to one of the form $\mathbf{Z} + \mathbf{Z}\tau$ for some $\tau \in \mathbf{C}$ with positive imaginary part.

The j-invariant

The j-invariant is a function

$$j\colon \{\text{lattices}\} \to \mathbf{C}$$

such that $j(L) = j(L') \iff L$ and L' are homothetic.

The j-invariant

The j-invariant is a function

$$j\colon \{\text{lattices}\} \to \mathbf{C}$$

such that $j(L) = j(L') \iff L$ and L' are homothetic.
We can define j on the upper half plane by $j(\tau) = j(\mathbf{Z} + \mathbf{Z}\,\tau)$.
Letting $q = e^{2\pi i \tau}$ we have

$$\begin{aligned} j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 \\ + 864299970q^3 + 20245856256q^4 + \cdots . \end{aligned}$$

The j-invariant

Singular moduli

Definition

The values $j(\tau)$ for τ imaginary quadratic are called **singular moduli**.

Singular moduli

Definition

The values $j(\tau)$ for τ imaginary quadratic are called **singular moduli**.

Examples

$$j(i) = 1728,$$

$$j\left(\frac{1+\sqrt{-3}}{2}\right) = 0,$$

$$j\left(\frac{1+\sqrt{-15}}{2}\right) = \frac{-191025 - 85995\sqrt{5}}{2}.$$

(A corollary of) The first main theorem of class field theory

Theorem

If K is an imaginary quadratic field, $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau$ then:

1. $j(\tau)$ is an algebraic integer.

(A corollary of) The first main theorem of class field theory

Theorem

If K is an imaginary quadratic field, $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau$ then:

1. $j(\tau)$ is an algebraic integer.
2. The Hilbert class field of K is $K(j(\tau))$.

(A corollary of) The first main theorem of class field theory

Theorem

If K is an imaginary quadratic field, $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau$ then:

1. $j(\tau)$ is an algebraic integer.
2. The Hilbert class field of K is $K(j(\tau))$.

A (partial) converse (Schneider)

If τ is an algebraic number that is not imaginary quadratic then $j(\tau)$ is transcendental.

Explaining Hermite's observations

$$K = \mathbf{Q}(\sqrt{-d}) \text{ with } \mathrm{cl}(\mathbf{Z}_K) = 1,\ \mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau.$$

Explaining Hermite's observations

$$K = \mathbf{Q}(\sqrt{-d}) \text{ with } \mathrm{cl}(\mathbf{Z}_K) = 1,\ \mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau.$$

$$\Downarrow$$

The Hilbert class field of K is K.

Explaining Hermite's observations

$$K = \mathbf{Q}(\sqrt{-d}) \text{ with } \mathrm{cl}(\mathbf{Z}_K) = 1,\ \mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau.$$

$$\Downarrow$$

The Hilbert class field of K is K.

$$\Downarrow$$

$$j(\tau) \in \mathbf{Z}_K\,.$$

Explaining Hermite's observations

$$K = \mathbf{Q}(\sqrt{-d}) \text{ with } \mathrm{cl}(\mathbf{Z}_K) = 1,\ \mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau.$$

$$\Downarrow$$

The Hilbert class field of K is K.

$$\Downarrow$$

$$j(\tau) \in \mathbf{Z}_K\,.$$

$$\Downarrow$$

$$e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + \ldots \in \mathbf{Z}_K \cap \mathbf{R}$$

Explaining Hermite's observations

$$K = \mathbf{Q}(\sqrt{-d}) \text{ with } \mathrm{cl}(\mathbf{Z}_K) = 1,\ \mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\,\tau.$$

$$\Downarrow$$

The Hilbert class field of K is K.

$$\Downarrow$$

$$j(\tau) \in \mathbf{Z}_K\,.$$

$$\Downarrow$$

$$e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + \ldots \in \mathbf{Z}_K \cap \mathbf{R} = \mathbf{Z}\,.$$

Explaining Hermite's observations

So if $d = 163$ we have $\tau = (1 + \sqrt{-163})/2$

Explaining Hermite's observations

So if $d = 163$ we have $\tau = (1 + \sqrt{-163})/2$ and so

$$\begin{aligned} j(\tau) &= e^{-\pi i(1+i\sqrt{163})} + 744 + 196884 e^{\pi i(1+i\sqrt{163})} + \dots \\ &= -e^{\pi\sqrt{163}} + 744 - 196884 e^{-\pi\sqrt{163}} + \dots \end{aligned}$$

is an integer.

Explaining Hermite's observations

So if $d = 163$ we have $\tau = (1 + \sqrt{-163})/2$ and so

$$\begin{aligned} j(\tau) &= e^{-\pi i(1+i\sqrt{163})} + 744 + 196884 e^{\pi i(1+i\sqrt{163})} + \dots \\ &= -e^{\pi\sqrt{163}} + 744 - 196884 e^{-\pi\sqrt{163}} + \dots \end{aligned}$$

is an integer.
The trailing terms are tiny here giving

$$e^{\pi\sqrt{163}} \approx -j(\tau) + 744.$$

The class number 1 problem

Theorem (Stark-Heegner)

The only imaginary quadratic number fields with trivial class group are $\mathbf{Q}(\sqrt{-d})$ for

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

The class number 1 problem

Theorem (Stark-Heegner)

The only imaginary quadratic number fields with trivial class group are $\mathbf{Q}(\sqrt{-d})$ for

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

So we expect $e^{\pi\sqrt{19}}$ to be close to an integer too:

$$e^{\pi\sqrt{19}} = .$$

The class number 1 problem

Theorem (Stark-Heegner)

The only imaginary quadratic number fields with trivial class group are $\mathbf{Q}(\sqrt{-d})$ for

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

So we expect $e^{\pi\sqrt{19}}$ to be close to an integer too:

$$e^{\pi\sqrt{19}} = .$$

The value is not as close as $e^{-\pi\sqrt{d}}$ has larger absolute value for smaller d.

A formula of Gross-Zagier

We have that $j() =$ and $j() =$ and so

$$j(\sqrt{}) - j(\sqrt{}) = .$$

A formula of Gross-Zagier

Theorem (Gross-Zagier, '84)

Closing remarks

- Singular moduli are not particularly complex objects in and of themselves.

Closing remarks

- Singular moduli are not particularly complex objects in and of themselves.
- But their relation between different areas of mathematics ensures that they are still a research topic to this day.

Sources

I used some of the following when preparing this talk, and so they are probably good places to look to learn more about the topic:

- "Primes of the form $x^2 + ny^2$" – David A. Cox