

# Singular Moduli

Alex J. Best

WIMP 2014

29/11/2014

# In this talk:

- 1 Introduction
- 2 Background
- 3 The Hilbert class field
- 4 Singular moduli
- 5 Modern work
- 6 Conclusion

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):

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

$$\approx 12^3(9^2 - 1)^3 + 744 - 10^{-4} \cdot 2.225 \dots$$

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

$$\approx 12^3(21^2 - 1)^3 + 744 - 10^{-6} \cdot 1.337 \dots$$

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

$$\approx 12^3(231^2 - 1)^3 + 744 - 10^{-13} \cdot 7.499 \dots$$

# Abelian extensions

## Definition

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

# Abelian extensions

## Definition

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

Examples:

$$\mathbb{Q}(\sqrt{2})|\mathbb{Q},$$

# Abelian extensions

## Definition

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

Examples:

$$\mathbb{Q}(\sqrt{2})| \mathbb{Q},$$

$$\mathbb{Q}(i, \zeta_7)| \mathbb{Q}(i).$$

# Abelian extensions

## Definition

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

Examples:

$$\mathbb{Q}(\sqrt{2})| \mathbb{Q},$$

$$\mathbb{Q}(i, \zeta_7)| \mathbb{Q}(i).$$

Non-examples:

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3)| \mathbb{Q},$$

# Abelian extensions

## Definition

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

Examples:

$$\mathbb{Q}(\sqrt{2})| \mathbb{Q},$$

$$\mathbb{Q}(i, \zeta_7)| \mathbb{Q}(i).$$

Non-examples:

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3)| \mathbb{Q},$$

$$\mathbb{Q}(\sqrt[3]{2})| \mathbb{Q}.$$

# The ideal class group

Given a number field  $K$  we let  $I(\mathbf{Z}_K)$  be the set

$$\{M \text{ subgroup of } K : \mathbf{Z}_K M \subset M, \exists a \in \mathbf{Z}_k \text{ s.t. } aM \subset \mathbf{Z}_K, M \neq 0\}$$

of (non-zero) **fractional** ideals of  $\mathbf{Z}_K$ .

# The ideal class group

Given a number field  $K$  we let  $I(\mathbf{Z}_K)$  be the set

$$\{M \text{ subgroup of } K : \mathbf{Z}_K M \subset M, \exists a \in \mathbf{Z}_k \text{ s.t. } aM \subset \mathbf{Z}_K, M \neq 0\}$$

of (non-zero) **fractional** ideals of  $\mathbf{Z}_K$ . This is an (abelian) group under multiplication!

# The ideal class group

Given a number field  $K$  we let  $I(\mathbf{Z}_K)$  be the set

$$\{M \text{ subgroup of } K : \mathbf{Z}_K M \subset M, \exists a \in \mathbf{Z}_k \text{ s.t. } aM \subset \mathbf{Z}_K, M \neq 0\}$$

of (non-zero) **fractional** ideals of  $\mathbf{Z}_K$ . This is an (abelian) group under multiplication! The set

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

of (non-zero) **principal** ideals is a subgroup.

# The ideal class group

Given a number field  $K$  we let  $I(\mathbf{Z}_K)$  be the set

$$\{M \text{ subgroup of } K : \mathbf{Z}_K M \subset M, \exists a \in \mathbf{Z}_k \text{ s.t. } aM \subset \mathbf{Z}_K, M \neq 0\}$$

of (non-zero) **fractional** ideals of  $\mathbf{Z}_K$ . This is an (abelian) group under multiplication! The set

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

of (non-zero) **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

$$\{M \text{ subgroup of } K : \mathbf{Z}_K M \subset M, \exists a \in \mathbf{Z}_k \text{ s.t. } aM \subset \mathbf{Z}_K, M \neq 0\}$$

of (non-zero) **fractional** ideals of  $\mathbf{Z}_K$ . This is an (abelian) group under multiplication! The set

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

of (non-zero) **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.  $K = \mathbb{Q}(\sqrt{-n})$  for some  $n \in \mathbb{Z}_{\geq 1}$ .

# The Hilbert class field (of an imaginary quadratic field)

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

## Definition

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

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

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

# The Hilbert class field (of an imaginary quadratic field)

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

## Definition

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

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

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

## 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 $L$	$\text{Gal}(L K)$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-1})$	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 $L$	$\text{Gal}(L K)$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-1})$	1
$\mathbb{Q}(\sqrt{-31})$	$\mathbb{Q}(\sqrt{-31})[x]/(x^3 + x - 1)$	$C_3$

# 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 $L$	$\text{Gal}(L K)$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-1})$	$1$
$\mathbb{Q}(\sqrt{-31})$	$\mathbb{Q}(\sqrt{-31})[x]/(x^3 + x - 1)$	$C_3$
$\mathbb{Q}(\sqrt{-159})$	$\mathbb{Q}(\sqrt{-159})[x]/(x^{10} - 3x^9 + 6x^8 - 6x^7 + 3x^6 + 3x^5 - 9x^4 + 13x^3 - 12x^2 + 6x - 1)$	$C_{10}$

# 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

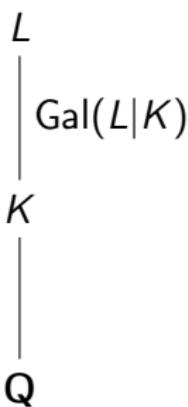
$K$	Hilbert class field $L$	$\text{Gal}(L K)$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-1})$	1
$\mathbb{Q}(\sqrt{-31})$	$\mathbb{Q}(\sqrt{-31})[x]/(x^3 + x - 1)$	$C_3$
$\mathbb{Q}(\sqrt{-159})$	$\mathbb{Q}(\sqrt{-159})[x]/(x^{10} - 3x^9 + 6x^8 - 6x^7 + 3x^6 + 3x^5 - 9x^4 + 13x^3 - 12x^2 + 6x - 1)$	$C_{10}$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

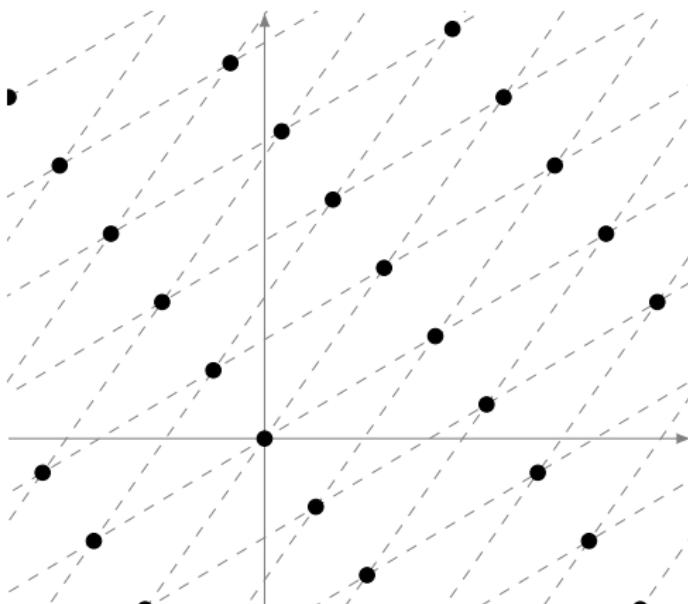
$$\text{cl}(\mathbb{Z}_K) \cong \text{Gal}(L|K).$$



# Lattices

## Definition

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



# Homothety

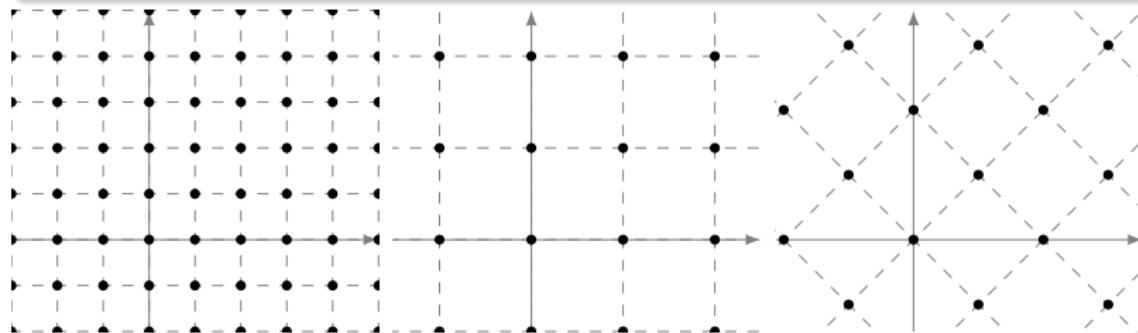
## Definition

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

# Homothety

## Definition

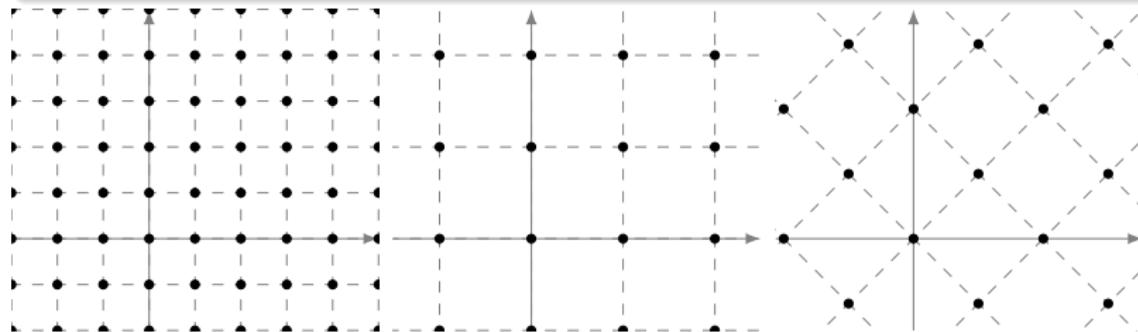
Two lattices  $L$  and  $L'$  are called **homothetic** if  $L = \lambda L'$  for some  $\lambda \in \mathbf{C}^*$ .



# 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

$$j: \{\text{lattices}\} \rightarrow \mathbf{C}$$

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

# The $j$ -invariant

The  $j$ -invariant is a function

$$j: \{\text{lattices}\} \rightarrow \mathbf{C}$$

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  $q = e^{2\pi i\tau}$  it turns out that

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

# The $j$ -invariant

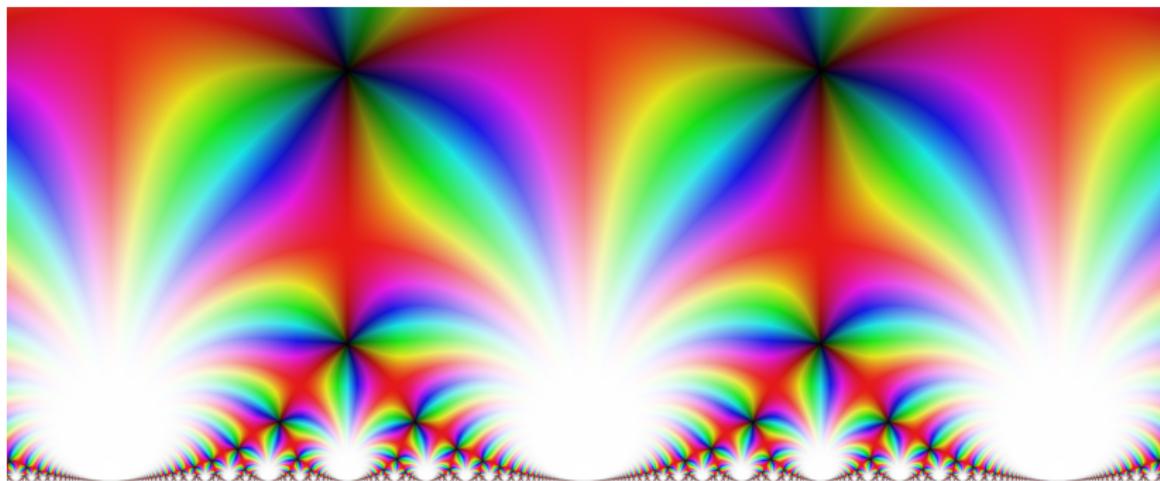


Figure : The  $j$ -invariant, picture by Fredrik Johansson

# Singular moduli

## Definition

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

# Singular moduli

## Definition

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

## Examples

$$j(i) = 1728,$$

# Singular moduli

## Definition

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

## Examples

$$j(i) = 1728,$$

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

# Singular moduli

## Definition

The values  $j(\tau)$  for  $\tau$  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,  $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\tau$  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,  $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\tau$  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,  $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\tau$  then:

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

## A (kind of) converse (Schneider)

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

# Explaining Hermite's observations

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

# Explaining Hermite's observations

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



The Hilbert class field of  $K$  is  $K$ .

# Explaining Hermite's observations

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



The Hilbert class field of  $K$  is  $K$ .



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

# Explaining Hermite's observations

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



The Hilbert class field of  $K$  is  $K$ .



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



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

# Explaining Hermite's observations

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



The Hilbert class field of  $K$  is  $K$ .



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



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

# 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

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

is an integer.

# Explaining Hermite's observations

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

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

is an integer.

The trailing terms are tiny (of order  $10^{-13}$ ) 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 might expect  $e^{\pi\sqrt{19}}$  to be close to an integer too, however

$$e^{\pi\sqrt{19}} = 885479.77768\dots$$

isn't really.

# 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 might expect  $e^{\pi\sqrt{19}}$  to be close to an integer too, however

$$e^{\pi\sqrt{19}} = 885479.77768\dots$$

isn't really. The value is not as close to the corresponding singular modulus as  $e^{-\pi\sqrt{d}}$  has larger absolute value for smaller  $d$ .

# A formula of Gross-Zagier

We have that  $j((1 + \sqrt{-67})/2) = 12^3(21^2 - 1)^3$  and  
 $j((1 + \sqrt{-163})/2) = 12^3(231^2 - 1)^3$  and so

$$j\left(\frac{1 + \sqrt{-163}}{2}\right) - j\left(\frac{1 + \sqrt{-67}}{2}\right) = 2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 139 \cdot 331.$$

# A formula of Gross-Zagier

Theorem (Gross-Zagier, '84)

Letting  $\epsilon(n) =$  we have that

$$N(j(\tau_1) - j(\tau_2))^2 = \prod_{\substack{x^2 \equiv D \\ (\text{mod } 4)}} F\left(\frac{D - x^2}{4}\right)$$

where

$$F(m) = \prod_{\substack{n, n' > 0 \\ nn' = m}} n^{-\epsilon(n)}.$$

# 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