CM-Points on Straight Lines

A joint work with **Amalia Pizarro-Madariaga**

Bill Allombert & Yuri Bilu

Bordeaux
September 23, 2014

Lattices

Lattice in $\mathbb{C}$: a discrete (additive) group of rank 2

Lattices

Lattice in $\mathbb{C}$: a discrete (additive) group of rank 2

Example: $\{a + bi : a, b \in \mathbb{Z}\} = \langle i, 1 \rangle$.

Lattices

Lattice in $\mathbb{C}$: a discrete (additive) group of rank 2

Example: $\{a + bi : a, b \in \mathbb{Z}\} = \langle i, 1 \rangle$.

Isomorphism of lattices: $\Lambda \cong \Lambda'$ if $\Lambda' = \alpha\Lambda, \qquad \alpha \in \mathbb{C}$.

Lattices

Lattice in $\mathbb{C}$: a discrete (additive) group of rank 2

Example: $\{a + bi : a, b \in \mathbb{Z}\} = \langle i, 1 \rangle$.

Isomorphism of lattices: $\Lambda \cong \Lambda'$ if $\Lambda' = \alpha\Lambda, \qquad \alpha \in \mathbb{C}$.

- Every lattice is isomorphic to $\langle \tau, 1 \rangle$, $\quad \mathrm{Im}\,\tau > 0$

Lattices

Lattice in $\mathbb{C}$: a discrete (additive) group of rank 2

Example: $\{a + bi : a, b \in \mathbb{Z}\} = \langle i, 1\rangle$.

Isomorphism of lattices: $\Lambda \cong \Lambda'$ if $\Lambda' = \alpha\Lambda, \qquad \alpha \in \mathbb{C}$.

- Every lattice is isomorphic to $\langle \tau, 1\rangle$, $\quad \mathrm{Im}\,\tau > 0$

Lattices

Lattice in $\mathbb{C}$: a discrete (additive) group of rank 2

Example: $\{a + bi : a, b \in \mathbb{Z}\} = \langle i, 1 \rangle$.

Isomorphism of lattices: $\Lambda \cong \Lambda'$ if $\Lambda' = \alpha\Lambda, \qquad \alpha \in \mathbb{C}$.

- Every lattice is isomorphic to $\langle \tau, 1 \rangle$, $\quad \mathrm{Im}\, \tau > 0$
- $\langle \tau, 1 \rangle \cong \langle \tau', 1 \rangle$ if and only if $\tau' = \frac{a\tau + b}{c\tau + d}, \quad \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$

Lattices

Lattice in $\mathbb{C}$: a discrete (additive) group of rank 2

Example: $\{a + bi : a, b \in \mathbb{Z}\} = \langle i, 1 \rangle$.

Isomorphism of lattices: $\Lambda \cong \Lambda'$ if $\Lambda' = \alpha\Lambda, \qquad \alpha \in \mathbb{C}$.

- Every lattice is isomorphic to $\langle \tau, 1 \rangle$, $\quad \mathrm{Im}\,\tau > 0$
- $\langle \tau, 1 \rangle \cong \langle \tau', 1 \rangle$ if and only if $\tau' = \frac{a\tau + b}{c\tau + d}, \quad \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$
- $\{\text{lattices up to isomorphism}\} = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$

  $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}\,\tau > 0\}$ "Poincaré (half)plane"

j-invariant

- ***j*-invariant**: $\mathrm{SL}_2(\mathbb{Z})$-automorphic function on $\mathbb{H}$ satisfying
$$j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \qquad j(\infty) = \infty$$

j-invariant

- **j-invariant**: $\mathrm{SL}_2(\mathbb{Z})$-automorphic function on $\mathbb{H}$ satisfying
  $j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \qquad j(\infty) = \infty$
- " $\mathrm{SL}_2(\mathbb{Z})$-automorphic" means: $j(\tau) = j\left(\frac{a\tau+b}{c\tau+d}\right)$,
  $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$

j-invariant

- **j-invariant**: $\mathrm{SL}_2(\mathbb{Z})$-automorphic function on $\mathbb{H}$ satisfying
  $$j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \qquad j(\infty) = \infty$$
- " $\mathrm{SL}_2(\mathbb{Z})$-automorphic" means: $j(\tau) = j\left(\frac{a\tau+b}{c\tau+d}\right)$, $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$
- **"Fourier expansion"**
  $$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots,$$
  $$q = q(\tau) = e^{2\pi i\tau}$$

j-invariant

- **j-invariant**: $\mathrm{SL}_2(\mathbb{Z})$-automorphic function on $\mathbb{H}$ satisfying
  $j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \qquad j(\infty) = \infty$
- "$\mathrm{SL}_2(\mathbb{Z})$-automorphic" means: $j(\tau) = j\left(\frac{a\tau+b}{c\tau+d}\right)$,
  $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$
- **"Fourier expansion"**
  $j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots,$
  $q = q(\tau) = e^{2\pi i\tau}$
- (remark important in the sequel)
  $|q|$ small when $\mathrm{Im}\,\tau$ large

j-invariant

- **j-invariant**: $\mathrm{SL}_2(\mathbb{Z})$-automorphic function on $\mathbb{H}$ satisfying
  $j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \qquad j(\infty) = \infty$
- " $\mathrm{SL}_2(\mathbb{Z})$-automorphic" means: $j(\tau) = j\left(\frac{a\tau+b}{c\tau+d}\right)$,
  $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$
- **"Fourier expansion"**
  $j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots,$
  $q = q(\tau) = e^{2\pi i\tau}$
- (remark important in the sequel)
  $|q|$ small when $\mathrm{Im}\,\tau$ large

j-invariant

- **j-invariant**: $\mathrm{SL}_2(\mathbb{Z})$-automorphic function on $\mathbb{H}$ satisfying
  $j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \qquad j(\infty) = \infty$
- "$\mathrm{SL}_2(\mathbb{Z})$-automorphic" means: $j(\tau) = j\left(\frac{a\tau+b}{c\tau+d}\right)$,
  $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$
- **"Fourier expansion"**
  $j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots,$

  $q = q(\tau) = e^{2\pi i\tau}$
- (remark important in the sequel)
  $|q|$ small when $\mathrm{Im}\,\tau$ large $\Longrightarrow |j(\tau)|$ large when $\mathrm{Im}\,\tau$ large

j-invariant

- **j-invariant**: $\mathrm{SL}_2(\mathbb{Z})$-automorphic function on $\mathbb{H}$ satisfying
  $j(i) = 1728, \qquad j\left(\frac{1+\sqrt{-3}}{2}\right) = 0, \qquad j(\infty) = \infty$
- " $\mathrm{SL}_2(\mathbb{Z})$-automorphic" means: $j(\tau) = j\left(\frac{a\tau+b}{c\tau+d}\right)$,
  $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$
- **"Fourier expansion"**
  $j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots,$
  $q = q(\tau) = e^{2\pi i\tau}$
- (remark important in the sequel)
  $|q|$ small when $\mathrm{Im}\,\tau$ large $\Longrightarrow$ $|j(\tau)|$ large when $\mathrm{Im}\,\tau$ large
- j-invariant "classifies lattices":
  $\langle \tau, 1\rangle \cong \langle \tau', 1\rangle \Longleftrightarrow j(\tau) = j(\tau')$

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$;

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$;

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\quad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\Longleftrightarrow [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\qquad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\qquad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\Longleftrightarrow [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\qquad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;
  - $D = D_K < 0$ the **fundamental discriminant**;

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\quad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;
  - $D = D_K < 0$ the **fundamental discriminant**;
  - $f = [\mathcal{O}_K : \mathcal{O}]$ the **conductor**;

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\qquad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;
  - $D = D_K < 0$ the **fundamental discriminant**;
  - $f = [\mathcal{O}_K : \mathcal{O}]$ the **conductor**;
  - $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right] =: \mathcal{O}_\Delta$;

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\quad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\Longleftrightarrow [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;
  - $D = D_K < 0$ the **fundamental discriminant**;
  - $f = [\mathcal{O}_K : \mathcal{O}]$ the **conductor**;
  - $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta + \sqrt{\Delta}}{2}\right] =: \mathcal{O}_\Delta$;
  - if τ is root of $at^2 + bt + c \in \mathbb{Z}[t]$,

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\Longleftrightarrow [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;
  - $D = D_K < 0$ the **fundamental discriminant**;
  - $f = [\mathcal{O}_K : \mathcal{O}]$ the **conductor**;
  - $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right] =: \mathcal{O}_\Delta$;
  - if τ is root of $at^2 + bt + c \in \mathbb{Z}[t]$,

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\quad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;
  - $D = D_K < 0$ the **fundamental discriminant**;
  - $f = [\mathcal{O}_K : \mathcal{O}]$ the **conductor**;
  - $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right] =: \mathcal{O}_\Delta$;
  - if τ is root of $at^2 + bt + c \in \mathbb{Z}[t]$, $\quad (a, b, c) = 1$

Complex Multiplication

- $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$; $\quad \mathrm{End}\Lambda \supseteq \mathbb{Z}$
- Λ has **Complex Multiplication** if $\mathrm{End}\Lambda \supsetneq \mathbb{Z}$
- $\Lambda = \langle \tau, 1 \rangle$ has CM $\iff [\mathbb{Q}(\tau) : \mathbb{Q}] = 2$
- In this case:
  - $\mathcal{O} = \mathrm{End}\Lambda$ is an order in $K = \mathbb{Q}(\tau)$ of discriminant $\Delta = Df^2$;
  - $D = D_K < 0$ the **fundamental discriminant**;
  - $f = [\mathcal{O}_K : \mathcal{O}]$ the **conductor**;
  - $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right] =: \mathcal{O}_\Delta$;
  - if τ is root of $at^2 + bt + c \in \mathbb{Z}[t]$, $\quad (a, b, c) = 1$ then $\Delta = b^2 - 4ac$ and $\tau = \frac{-b+\sqrt{\Delta}}{2a}$.

Class Field Theory

- $j(\tau)$ algebraic number (even algebraic integer)

Class Field Theory

- $j(\tau)$ algebraic number (even algebraic integer)
- $K(j(\tau))$ is abelian extension of $K = \mathbb{Q}(\tau)$ (the "Ring Class Field")

Class Field Theory

- $j(\tau)$ algebraic number (even algebraic integer)
- $K(j(\tau))$ is abelian extension of $K = \mathbb{Q}(\tau)$ (the "Ring Class Field")
- $[K(j(\tau)) : K] = [\mathbb{Q}(j(\tau)) : \mathbb{Q}] = h(\Delta)$

Class Field Theory

- $j(\tau)$ algebraic number (even algebraic integer)
- $K(j(\tau))$ is abelian extension of $K = \mathbb{Q}(\tau)$ (the "Ring Class Field")
- $[K(j(\tau)) : K] = [\mathbb{Q}(j(\tau)) : \mathbb{Q}] = h(\Delta)$
- $h(\Delta)$ the class number of the order $\mathcal{O}_\Delta$

Class Field Theory

- $j(\tau)$ algebraic number (even algebraic integer)
- $K(j(\tau))$ is abelian extension of $K = \mathbb{Q}(\tau)$ (the "Ring Class Field")
- $[K(j(\tau)) : K] = [\mathbb{Q}(j(\tau)) : \mathbb{Q}] = h(\Delta)$
- $h(\Delta)$ the class number of the order $\mathcal{O}_\Delta$
- moreover: $\mathrm{Gal}(K(j(\tau))/K) = \mathrm{Cl}(\Delta)$

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)
- In other words, for $h \in \mathbb{Z}_{>0}$ there exist finitely many Δ with $h(\Delta) = h$.

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)
- In other words, for $h \in \mathbb{Z}_{>0}$ there exist finitely many Δ with $h(\Delta) = h$.
- In particular (Heegner-Stark) there exist thirteen Δ with $h(\Delta) = 1$ (the corresponding j belong to $\mathbb{Z}$):

Δ	-3	$-3 \cdot 2^2$	$-3 \cdot 3^3$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
j	0	$2^4 3^3 5^3$	$-2^{15} 3 \cdot 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$

Δ	-11	-19	-43	-67	-163
j	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)
- In other words, for $h \in \mathbb{Z}_{>0}$ there exist finitely many Δ with $h(\Delta) = h$.
- In particular (Heegner-Stark) there exist thirteen Δ with $h(\Delta) = 1$ (the corresponding j belong to $\mathbb{Z}$):

Δ	-3	$-3 \cdot 2^2$	$-3 \cdot 3^3$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
j	0	$2^4 3^3 5^3$	$-2^{15} 3 \cdot 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$

Δ	-11	-19	-43	-67	-163
j	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$

- A funny example (Hermite): $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007\ldots$

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)
- In other words, for $h \in \mathbb{Z}_{>0}$ there exist finitely many Δ with $h(\Delta) = h$.
- In particular (Heegner-Stark) there exist thirteen Δ with $h(\Delta) = 1$ (the corresponding j belong to $\mathbb{Z}$):

Δ	-3	$-3 \cdot 2^2$	$-3 \cdot 3^3$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
j	0	$2^4 3^3 5^3$	$-2^{15} 3 \cdot 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$

Δ	-11	-19	-43	-67	-163
j	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$

- A funny example (Hermite): $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007\ldots$

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)
- In other words, for $h \in \mathbb{Z}_{>0}$ there exist finitely many Δ with $h(\Delta) = h$.
- In particular (Heegner-Stark) there exist thirteen Δ with $h(\Delta) = 1$ (the corresponding j belong to $\mathbb{Z}$):

Δ	-3	$-3 \cdot 2^2$	$-3 \cdot 3^3$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
j	0	$2^4 3^3 5^3$	$-2^{15} 3 \cdot 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$

Δ	-11	-19	-43	-67	-163
j	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$

- A funny example (Hermite): $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007\ldots$
  - $\tau = \frac{1+\sqrt{-163}}{2}$

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)
- In other words, for $h \in \mathbb{Z}_{>0}$ there exist finitely many Δ with $h(\Delta) = h$.
- In particular (Heegner-Stark) there exist thirteen Δ with $h(\Delta) = 1$ (the corresponding j belong to $\mathbb{Z}$):

Δ	-3	$-3 \cdot 2^2$	$-3 \cdot 3^3$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
j	0	$2^4 3^3 5^3$	$-2^{15} 3 \cdot 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$

Δ	-11	-19	-43	-67	-163
j	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$

- A funny example (Hermite): $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007\ldots$
  - $\tau = \frac{1+\sqrt{-163}}{2}$
  - $e^{\pi\sqrt{163}} = -e^{2\pi i \tau} \approx -j(\tau) + 744 \in \mathbb{Z}$

The Class Number

- $h(\Delta) \to \infty$ as $|\Delta| \to \infty$ (Siegel)
- In other words, for $h \in \mathbb{Z}_{>0}$ there exist finitely many Δ with $h(\Delta) = h$.
- In particular (Heegner-Stark) there exist thirteen Δ with $h(\Delta) = 1$ (the corresponding j belong to $\mathbb{Z}$):

Δ	-3	$-3 \cdot 2^2$	$-3 \cdot 3^3$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
j	0	$2^4 3^3 5^3$	$-2^{15} 3 \cdot 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$

Δ	-11	-19	-43	-67	-163
j	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$

- A funny example (Hermite): $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007\ldots$
  - $\tau = \frac{1+\sqrt{-163}}{2}$
  - $e^{\pi\sqrt{163}} = -e^{2\pi i \tau} \approx -j(\tau) + 744 \in \mathbb{Z}$
- Currently all Δ with $h_\Delta \leq 100$ are known (Watkins 2006).

Special Points and Special Curves

τ imaginary quadratic $\Rightarrow j(\tau) \in \bar{\mathbb{Q}}$

Special Points and Special Curves

τ imaginary quadratic $\Rightarrow j(\tau) \in \bar{\mathbb{Q}}$

CM-point or **special point** on $\mathbb{C}^2$: $\quad \big(j(\tau_1), j(\tau_2)\big)$.

Special Points and Special Curves

τ imaginary quadratic $\Rightarrow j(\tau) \in \bar{\mathbb{Q}}$

CM-point or **special point** on $\mathbb{C}^2$: $\quad \big(j(\tau_1), j(\tau_2)\big)$.

Question: can an irreducible plane curve $F(x_1, x_2) = 0$ contain infinitely many CM-points?

Special Points and Special Curves

τ imaginary quadratic $\Rightarrow j(\tau) \in \bar{\mathbb{Q}}$

CM-point or **special point** on $\mathbb{C}^2$: $\big(j(\tau_1), j(\tau_2)\big)$.

Question: can an irreducible plane curve $F(x_1, x_2) = 0$ contain infinitely many CM-points?

Special curves:

- vertical line $x_1 = j(\tau_1)$

Special Points and Special Curves

τ imaginary quadratic $\Rightarrow j(\tau) \in \bar{\mathbb{Q}}$

CM-point or **special point** on $\mathbb{C}^2$: $\quad \big(j(\tau_1), j(\tau_2)\big)$.

Question: can an irreducible plane curve $F(x_1, x_2) = 0$ contain infinitely many CM-points?

Special curves:

- vertical line $x_1 = j(\tau_1)$
- horizontal line $x_2 = j(\tau_2)$

Special Points and Special Curves

τ imaginary quadratic $\Rightarrow j(\tau) \in \bar{\mathbb{Q}}$

CM-point or **special point** on $\mathbb{C}^2$: $\quad \big(j(\tau_1), j(\tau_2)\big)$.

Question: can an irreducible plane curve $F(x_1, x_2) = 0$ contain infinitely many CM-points?

Special curves:

- vertical line $x_1 = j(\tau_1)$
- horizontal line $x_2 = j(\tau_2)$
- $Y_0(N)$ realized as $\Phi_N(x_1, x_2) = 0$

Modular Curves and Modular Polynomials

- $\Phi_N(x_1, x_2)$ Nth "modular polynomial": $\Phi_N\big(j(z), j(Nz)\big) = 0$

Modular Curves and Modular Polynomials

- $\Phi_N(x_1, x_2)$ Nth "modular polynomial": $\Phi_N\big(j(z), j(Nz)\big) = 0$
- $\big(j(\tau), j(N\tau)\big) \in Y_0(N)$ for every τ.

Modular Curves and Modular Polynomials

- $\Phi_N(x_1, x_2)$ Nth "modular polynomial": $\Phi_N\big(j(z), j(Nz)\big) = 0$
- $\big(j(\tau), j(N\tau)\big) \in Y_0(N)$ for every τ.
- More generally:
  for $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ there exists N such that
  $\big(j(\tau), j(\gamma\tau)\big) \in Y_0(N)$ for every τ.

Modular Curves and Modular Polynomials

- $\Phi_N(x_1, x_2)$ Nth "modular polynomial": $\Phi_N\big(j(z), j(Nz)\big) = 0$
- $\big(j(\tau), j(N\tau)\big) \in Y_0(N)$ for every τ.
- More generally:
  for $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ there exists N such that
  $\big(j(\tau), j(\gamma\tau)\big) \in Y_0(N)$ for every τ.

Modular Curves and Modular Polynomials

- $\Phi_N(x_1, x_2)$ Nth "modular polynomial": $\Phi_N\big(j(z), j(Nz)\big) = 0$
- $\big(j(\tau), j(N\tau)\big) \in Y_0(N)$ for every τ.
- More generally:
  for $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ there exists N such that
  $\big(j(\tau), j(\gamma\tau)\big) \in Y_0(N)$ for every τ.

Polynomials Φ_N, $N \le 3$

$$\Phi_1(x, y) = x - y$$

$$\begin{aligned}\Phi_2(x, y) = &- x^2y^2 + x^3 + y^3 + 1488x^2y + 1488xy^2 + 40773375xy \\ &- 162000x^2 - 162000y^2 + 8748000000x + 8748000000y - 157464000000000\end{aligned}$$

$$\begin{aligned}\Phi_3(x, y) = &\ x^4 + y^4 - x^3y^3 + 2232x^3y^2 + 2232x^2y^3 - 1069956x^3y - 1069956xy^3 \\ &+ 36864000x^3 + 36864000y^3 + 2587918086x^2y^2 \\ &+ 8900222976000x^2y + 8900222976000xy^2 + 452984832000000x^2 + 452984832000000y^2 \\ &- 770845966336000000xy + 1855425871872000000000x + 1855425871872000000000y\end{aligned}$$

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer
- Breuer (2001, GRH, effective)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer
- Breuer (2001, GRH, effective)
- B., Masser, Zannier (2013, effective)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer
- Breuer (2001, GRH, effective)
- B., Masser, Zannier (2013, effective)
- Kühne (2012, 2013, effective)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer
- Breuer (2001, GRH, effective)
- B., Masser, Zannier (2013, effective)
- Kühne (2012, 2013, effective)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer
- Breuer (2001, GRH, effective)
- B., Masser, Zannier (2013, effective)
- Kühne (2012, 2013, effective)

Particular cases:

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer
- Breuer (2001, GRH, effective)
- B., Masser, Zannier (2013, effective)
- Kühne (2012, 2013, effective)

Particular cases:

- no CM-points on $x_1 + x_2 = 1$ (Kühne 2013)

Theorem of André

Theorem (André, 1998) A non-special irreducible plane curve can have only finitely many special points.

Different proofs:

- André (1998)
- Edixhoven (1998, GRH)
- Pila (2009, extends to higher dimension)

  All non-effective, use Siegel-Brauer
- Breuer (2001, GRH, effective)
- B., Masser, Zannier (2013, effective)
- Kühne (2012, 2013, effective)

Particular cases:

- no CM-points on $x_1 + x_2 = 1$ (Kühne 2013)
- no CM-points on $x_1 x_2 = 1$ (B., Masser, Zannier 2013)

Kühne's "uniformity observation"

Kühne (2013):

- If $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over a n.f. L, then $|\Delta_1|, |\Delta_2| \leq c_{\mathrm{eff}}([L : \mathbb{Q}])$.

Kühne's "uniformity observation"

Kühne (2013):

- If $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over a n.f. L, then $|\Delta_1|, |\Delta_2| \leq c_{\mathrm{eff}}([L : \mathbb{Q}])$.

  (Δ_i discriminant of the CM-order $\mathrm{End}\langle\tau_i, 1\rangle$)

Kühne's "uniformity observation"

Kühne (2013):

- If $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over a n.f. L, then $|\Delta_1|, |\Delta_2| \leq c_{\mathrm{eff}}([L : \mathbb{Q}])$.

  (Δ_i discriminant of the CM-order $\mathrm{End}\langle\tau_i, 1\rangle$)
- In particular: all CM-points belonging to non-special straight lines defined over $\mathbb{Q}$ can (in principle) be listed explicitly.

Kühne's "uniformity observation"

Kühne (2013):

- If $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over a n.f. L, then $|\Delta_1|, |\Delta_2| \leq c_{\mathrm{eff}}([L:\mathbb{Q}])$.

  (Δ_i discriminant of the CM-order $\mathrm{End}\langle\tau_i, 1\rangle$)
- In particular: all CM-points belonging to non-special straight lines defined over $\mathbb{Q}$ can (in principle) be listed explicitly.
- Bajolet (2014): software to determine all CM-points on a given line.

CM-Points on Straight Lines

Special straight lines:

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

Obvious cases $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over $\mathbb{Q}$ in one of the following cases:

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

Obvious cases $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over $\mathbb{Q}$ in one of the following cases:

- $j(\tau_1), j(\tau_2) \in \mathbb{Q}$;

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

Obvious cases $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over $\mathbb{Q}$ in one of the following cases:

- $j(\tau_1), j(\tau_2) \in \mathbb{Q}$;
- $j(\tau_1) \neq j(\tau_2)$, $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = K$, $[K : \mathbb{Q}] = 2$.

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

Obvious cases $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over $\mathbb{Q}$ in one of the following cases:

- $j(\tau_1), j(\tau_2) \in \mathbb{Q}$;
- $j(\tau_1) \neq j(\tau_2)$, $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = K$, $[K : \mathbb{Q}] = 2$.

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

Obvious cases $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over $\mathbb{Q}$ in one of the following cases:

- $j(\tau_1), j(\tau_2) \in \mathbb{Q}$;
- $j(\tau_1) \neq j(\tau_2)$, $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = K$, $[K : \mathbb{Q}] = 2$.

(Can be easily listed.)

CM-Points on Straight Lines

Special straight lines:

- vertical $x_1 = j(\tau_1)$ and horizontal $x_2 = j(\tau_2)$ lines;
- $x_1 = x_2$ (which is $Y_0(1)$).

Obvious cases $(j(\tau_1), j(\tau_2))$ belongs to a non-special straight line over $\mathbb{Q}$ in one of the following cases:

- $j(\tau_1), j(\tau_2) \in \mathbb{Q}$;
- $j(\tau_1) \neq j(\tau_2)$, $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = K$, $[K : \mathbb{Q}] = 2$.

(Can be easily listed.)

Theorem (A., B., Pizarro; May 2014) If a CM-points belongs to a non-special straight line over $\mathbb{Q}$ then we have one of the two cases above.

Equality of CM-fields

Theorem ECMF (based on ideas of André, Edixhoven and Kühne) Assume that $L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.

Equality of CM-fields

Theorem ECMF (based on ideas of André, Edixhoven and Kühne) Assume that $L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.

- If $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ then L is the table:

Field L	Δ	$\mathrm{Cl}(\Delta)$
$\mathbb{Q}$	$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$	trivial
$\mathbb{Q}(\sqrt{2})$	$-24, -32, -64, -88$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{3})$	$-36, -48$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{5})$	$-15, -20, -35, -40, -60, -75, -100, -115, -235$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{13})$	$-52, -91, -403$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{17})$	$-51, -187$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$-96, -192, -288$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	$-180, -240$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	$-195, -520, -715$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	$-120, -160, -280, -760$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	$-340, -595$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	$-480, -960$	$(\mathbb{Z}/2\mathbb{Z})^3$

Equality of CM-fields

Theorem ECMF (based on ideas of André, Edixhoven and Kühne) Assume that $L = \mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.

- If $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ then L is the table:

Field L	Δ	$\mathrm{Cl}(\Delta)$
$\mathbb{Q}$	$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$	trivial
$\mathbb{Q}(\sqrt{2})$	$-24, -32, -64, -88$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{3})$	$-36, -48$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{5})$	$-15, -20, -35, -40, -60, -75, -100, -115, -235$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{13})$	$-52, -91, -403$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{17})$	$-51, -187$	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	$-96, -192, -288$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	$-180, -240$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	$-195, -520, -715$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	$-120, -160, -280, -760$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	$-340, -595$	$(\mathbb{Z}/2\mathbb{Z})^2$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	$-480, -960$	$(\mathbb{Z}/2\mathbb{Z})^3$

- If $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$ then $\Delta_1/\Delta_2 \in \{1, 4, 1/4\}$ or $\Delta_1, \Delta_2 \in \{-3, -12, -27\}$.

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;

The Proof

May assume:

- $\tau_i = \frac{-b_i + \sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L : \mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$

The Proof

May assume:

- $\tau_i = \frac{-b_i + \sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L : \mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L:\mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L:\mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

Crucial steps:

- $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$;

The Proof

May assume:

- $\tau_i = \frac{-b_i + \sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L : \mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

Crucial steps:

- $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$;
- $a_1 = a_2 = 1$;

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L : \mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

Crucial steps:

- $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$;
- $a_1 = a_2 = 1$;

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L:\mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

Crucial steps:

- $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$;
- $a_1 = a_2 = 1$;

Consequences:

- $\Delta_1 = \Delta$, $\Delta_2 = \Delta$ or 4Δ.

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L : \mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

Crucial steps:

- $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$;
- $a_1 = a_2 = 1$;

Consequences:

- $\Delta_1 = \Delta$, $\Delta_2 = \Delta$ or 4Δ.
- $\tau_1 = \frac{-b_1+\sqrt{\Delta}}{2}$, $\tau_2 = \frac{-b_2+\sqrt{\Delta}}{2}$ or $\tau_2 = \frac{-b_2+2\sqrt{\Delta}}{2}$

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L : \mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

Crucial steps:

- $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$;
- $a_1 = a_2 = 1$;

Consequences:

- $\Delta_1 = \Delta$, $\Delta_2 = \Delta$ or 4Δ.
- $\tau_1 = \frac{-b_1+\sqrt{\Delta}}{2}$, $\tau_2 = \frac{-b_2+\sqrt{\Delta}}{2}$ or $\tau_2 = \frac{-b_2+2\sqrt{\Delta}}{2}$
- In the first case $j(\tau_1) = j(\tau_2)$

The Proof

May assume:

- $\tau_i = \frac{-b_i+\sqrt{\Delta_i}}{2a_i}$;
- $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2)) = L$
- $[L : \mathbb{Q}] = h(\Delta_1) = h(\Delta_2) \geq 3$
- $j(\tau_1) \neq j(\tau_2)$.

Crucial steps:

- $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$;
- $a_1 = a_2 = 1$;

Consequences:

- $\Delta_1 = \Delta$, $\Delta_2 = \Delta$ or 4Δ.
- $\tau_1 = \frac{-b_1+\sqrt{\Delta}}{2}$, $\tau_2 = \frac{-b_2+\sqrt{\Delta}}{2}$ or $\tau_2 = \frac{-b_2+2\sqrt{\Delta}}{2}$
- In the first case $j(\tau_1) = j(\tau_2)$
- In the second case $(j(\tau_1), j(\tau_2)) \in Y_0(2)$.

The Proof (continued)

- $Y_0(2)$ is curve of degree 4

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap \text{(straight line)}| \leq 4$

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap \text{(straight line)}| \leq 4$
- Hence $3 \leq h(\Delta) = h(4\Delta) \leq 4$

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap \text{(straight line)}| \leq 4$
- Hence $3 \leq h(\Delta) = h(4\Delta) \leq 4$
- There is only five Δ with this property:

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap \text{(straight line)}| \leq 4$
- Hence $3 \leq h(\Delta) = h(4\Delta) \leq 4$
- There is only five Δ with this property:

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap \text{(straight line)}| \leq 4$
- Hence $3 \leq h(\Delta) = h(4\Delta) \leq 4$
- There is only five Δ with this property:

$h = 3$: $-23, -31$;

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap \text{(straight line)}| \leq 4$
- Hence $3 \leq h(\Delta) = h(4\Delta) \leq 4$
- There is only five Δ with this property:

$h = 3$: $-23, -31$;
$h = 4$: $-7 \cdot 3^2, -39, -55$.

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap \text{(straight line)}| \leq 4$
- Hence $3 \leq h(\Delta) = h(4\Delta) \leq 4$
- There is only five Δ with this property:

$h = 3$: -23, -31;
$h = 4$: $-7 \cdot 3^2$, -39, -55.

The Proof (continued)

- $Y_0(2)$ is curve of degree 4
- Hence $|Y_0(2) \cap (\text{straight line})| \leq 4$
- Hence $3 \leq h(\Delta) = h(4\Delta) \leq 4$
- There is only five Δ with this property:

$h = 3$: $-23, -31$;
$h = 4$: $-7 \cdot 3^2, -39, -55$.

One rules them out using PARI. $\square$

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$
$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$
$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$
$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$
$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$
$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$
$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$
$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$
$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$
$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$
$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$
$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$
$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$
$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$
$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

- **Weinberger** (1973): All field discriminants D with $\mathrm{Cl}(D)^2 = 1$ belong to the list above

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$
$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$
$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$
$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$
$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$
$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$
$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$
$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

- **Weinberger** (1973): All field discriminants D with $\mathrm{Cl}(D)^2 = 1$ belong to the list above

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$

$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$

$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$

$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$

$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$

$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$

$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$

$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

- **Weinberger** (1973): All field discriminants D with $\mathrm{Cl}(D)^2 = 1$ belong to the list above **with at most one exception**.

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$
$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$
$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$
$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$
$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$
$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$
$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$
$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

- **Weinberger** (1973): All field discriminants D with $\mathrm{Cl}(D)^2 = 1$ belong to the list above **with at most one exception**.
- **Corollary:** There exists D^* such that: if $\Delta = Df^2$ with $\mathrm{Cl}(\Delta)^2 = 1$ is **not** in the list then $D = D^*$.

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$
$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$
$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$
$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$
$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$
$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$
$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$
$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

- **Weinberger** (1973): All field discriminants D with $\mathrm{Cl}(D)^2 = 1$ belong to the list above **with at most one exception**.
- **Corollary:** There exists D^* such that: if $\Delta = Df^2$ with $\mathrm{Cl}(\Delta)^2 = 1$ is **not** in the list then $D = D^*$.
- Class numbers of discriminants from the list are at most 16.

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$
$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$
$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$
$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$
$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$
$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$
$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$
$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

- **Weinberger** (1973): All field discriminants D with $\mathrm{Cl}(D)^2 = 1$ belong to the list above **with at most one exception**.
- **Corollary:** There exists D^* such that: if $\Delta = Df^2$ with $\mathrm{Cl}(\Delta)^2 = 1$ is **not** in the list then $D = D^*$.
- Class numbers of discriminants from the list are at most 16.
- **Watkins** (2006): the list contains all Δ with $|\mathrm{Cl}(\Delta)^2| = 1$ and $h(\Delta) \leq 64$.

Discriminants with Class Group Annihilated by 2

Known Δ with $\mathrm{Cl}(\Delta)^2 = 1$

$-3, -3\cdot 2^2, -3\cdot 3^2, -3\cdot 4^2, -3\cdot 5^2, -3\cdot 7^2, -3\cdot 8^2, -4, -4\cdot 2^2, -4\cdot 3^2, -4\cdot 4^2, -4\cdot 5^2,$
$-7, -7\cdot 2^2, -7\cdot 4^2, -7\cdot 8^2, -8, -8\cdot 2^2, -8\cdot 3^2, -8\cdot 6^2, -11, -11\cdot 3^2,$
$-15, -15\cdot 2^2, -15\cdot 4^2, -15\cdot 8^2, -19, -20, -20\cdot 3^2, -24, -24\cdot 2^2, -35, -35\cdot 3^2, -40, -40\cdot 2^2,$
$-43, -51, -52, -67, -84, -88, -88\cdot 2^2, -91, -115, -120, -120\cdot 2^2, -123, -132, -148, -163,$
$-168, -168\cdot 2^2, -187, -195, -228, -232, -232\cdot 2^2, -235, -267, -280, -280\cdot 2^2, -312, -312\cdot 2^2,$
$-340, -372, -403, -408, -408\cdot 2^2, -420, -427, -435, -483, -520, -520\cdot 2^2, -532, -555, -595,$
$-627, -660, -708, -715, -760, -760\cdot 2^2, -795, -840, -840\cdot 2^2, -1012, -1092, -1155,$
$-1320, -1320\cdot 2^2, -1380, -1428, -1435, -1540, -1848, -1848\cdot 2^2, -1995, -3003, -3315, -5460.$

- **Weinberger** (1973): All field discriminants D with $\mathrm{Cl}(D)^2 = 1$ belong to the list above **with at most one exception**.
- **Corollary:** There exists D^* such that: if $\Delta = Df^2$ with $\mathrm{Cl}(\Delta)^2 = 1$ is **not** in the list then $D = D^*$.
- Class numbers of discriminants from the list are at most 16.
- **Watkins** (2006): the list contains all Δ with $|\mathrm{Cl}(\Delta)^2| = 1$ and $h(\Delta) \leq 64$.
- Hence: if Δ with $\mathrm{Cl}(\Delta)^2 = 1$ is **not** in the list then $h(\Delta) \geq 128$.

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$
\begin{tikzcd}
 & \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[ur, dash] \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] & & M \\
 & \mathbb{Q}(\tau_2) \arrow[ur, dash] \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] & & \mathbb{Q}(\tau_2, j(\tau_2)) \arrow[ur, dash] &
\end{tikzcd}
$$

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$
\begin{tikzcd}
 & \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] & & M \\
 & \mathbb{Q}(\tau_2) \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] \arrow[ur, dash] & & \mathbb{Q}(\tau_2, j(\tau_2)) \arrow[ur, dash] &
\end{tikzcd}
$$

- Consequence: each $\mathrm{Cl}(\Delta_i)$ is of type $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$.

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$\begin{tikzcd}
 & \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[ur, dash] \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] & & M \\
 & \mathbb{Q}(\tau_2) \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] \arrow[ur, dash] & & \mathbb{Q}(\tau_2, j(\tau_2)) \arrow[ur, dash] &
\end{tikzcd}$$

- Consequence: each $\mathrm{Cl}(\Delta_i)$ is of type $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$.
- Simple group theory: first type is impossible. Hence both $\mathrm{Cl}(\Delta_i)$ are annihilated by 2.

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$
\begin{tikzcd}
 & \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] \arrow[dl, dash] & & M \arrow[dl, dash] \\
 & \mathbb{Q}(\tau_2) \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] & & \mathbb{Q}(\tau_2, j(\tau_2)) &
\end{tikzcd}
$$

- Consequence: each $\mathrm{Cl}(\Delta_i)$ is of type $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$.
- Simple group theory: first type is impossible. Hence both $\mathrm{Cl}(\Delta_i)$ are annihilated by 2.
- Weinberger: since $D_1 \neq D_2$

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$
\begin{tikzcd}
 & \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[ur, dash] \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] & & M \\
 & \mathbb{Q}(\tau_2) \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] \arrow[ur, dash] & & \mathbb{Q}(\tau_2, j(\tau_2)) \arrow[ur, dash] &
\end{tikzcd}
$$

- Consequence: each $\mathrm{Cl}(\Delta_i)$ is of type $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$.
- Simple group theory: first type is impossible. Hence both $\mathrm{Cl}(\Delta_i)$ are annihilated by 2.
- Weinberger: since $D_1 \neq D_2$

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$
\begin{tikzcd}
 & \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[ur, dash] \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] & & M \\
 & \mathbb{Q}(\tau_2) \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] \arrow[ur, dash] & & \mathbb{Q}(\tau_2, j(\tau_2)) \arrow[ur, dash] &
\end{tikzcd}
$$

- Consequence: each $\mathrm{Cl}(\Delta_i)$ is of type $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$.
- Simple group theory: first type is impossible. Hence both $\mathrm{Cl}(\Delta_i)$ are annihilated by 2.
- Weinberger: since $D_1 \neq D_2$ **one of Δ_1, Δ_2 is in the list**.

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$
\begin{tikzcd}
& \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[ur, dash] \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] & & M \\
& \mathbb{Q}(\tau_2) \arrow[ur, dash] \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] & & \mathbb{Q}(\tau_2, j(\tau_2)) \arrow[ur, dash] &
\end{tikzcd}
$$

- Consequence: each $\mathrm{Cl}(\Delta_i)$ is of type $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$.
- Simple group theory: first type is impossible. Hence both $\mathrm{Cl}(\Delta_i)$ are annihilated by 2.
- Weinberger: since $D_1 \neq D_2$ **one of Δ_1, Δ_2 is in the list**.
- Hence the other is in the list as well.

Proof of Theorem ECMF

- Assume that $\mathbb{Q}(\tau_1) \neq \mathbb{Q}(\tau_2)$ and $\mathbb{Q}(j(\tau_1)) = \mathbb{Q}(j(\tau_2))$.
- Set $M = \mathbb{Q}(\tau_1, \tau_2, j(\tau_1)) = \mathbb{Q}(\tau_1, \tau_2, j(\tau_2))$.
- **André, Edixhoven** (1998): $G = \mathrm{Gal}(M/\mathbb{Q}(\tau_1, \tau_2))$ is annihilated by 2.

$$
\begin{tikzcd}
 & \mathbb{Q}(\tau_1) \arrow[rr, dash, "\mathrm{Cl}(\Delta_1)"] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, j(\tau_1)) \arrow[dr, dash] & \\
\mathbb{Q} \arrow[ur, dash] \arrow[rr, dash] \arrow[dr, dash] & & \mathbb{Q}(\tau_1, \tau_2) \arrow[rr, dash, "G"] & & M \\
 & \mathbb{Q}(\tau_2) \arrow[rr, dash, "\mathrm{Cl}(\Delta_2)"] \arrow[ur, dash] & & \mathbb{Q}(\tau_2, j(\tau_2)) \arrow[ur, dash] &
\end{tikzcd}
$$

- Consequence: each $\mathrm{Cl}(\Delta_i)$ is of type $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$ or $\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2$.
- Simple group theory: first type is impossible. Hence both $\mathrm{Cl}(\Delta_i)$ are annihilated by 2.
- Weinberger: since $D_1 \neq D_2$ **one of Δ_1, Δ_2 is in the list**.
- Hence the other is in the list as well.
- Verification with PARI completes the proof.