Modularity of elliptic curves over totally real cubic fields

Filip Najman

University of Zagreb

joint with Maarten Derickx (MIT) and Samir Siksek (Warwick)

Barcelona Fall Workshop on Number Theory II,
December 6th 2019.

Definition

An elliptic curve E over $\mathbb{Q}$ is **modular** if there exists a modular form f of weight 2 such that

$$L(E, s) = L(f, s).$$

Proof of Fermat's last theorem

Theorem (Fermat's last theorem)

All solutions of $x^n + y^n = z^n$ in $\mathbb{Z}$ for $n \geq 3$ satisfy $xyz = 0$.

Proof of Fermat's last theorem

Theorem (Fermat's last theorem)

All solutions of $x^n + y^n = z^n$ in $\mathbb{Z}$ for $n \geq 3$ satisfy $xyz = 0$.

1. Suffices to consider $n = 4$ (Fermat) or $n = p$ prime.

Proof of Fermat's last theorem

Theorem (Fermat's last theorem)

All solutions of $x^n + y^n = z^n$ in $\mathbb{Z}$ for $n \geq 3$ satisfy $xyz = 0$.

1. Suffices to consider $n = 4$ (Fermat) or $n = p$ prime.
2. (Frey) To a solution (a, b, c) one can associate the (semistable) elliptic curve $y^2 = x(x - a^p)(x + b^p)$.

Proof of Fermat's last theorem

Theorem (Fermat's last theorem)

All solutions of $x^n + y^n = z^n$ in $\mathbb{Z}$ for $n \geq 3$ satisfy $xyz = 0$.

1. Suffices to consider $n = 4$ (Fermat) or $n = p$ prime.
2. (Frey) To a solution (a, b, c) one can associate the (semistable) elliptic curve $y^2 = x(x - a^p)(x + b^p)$.
3. (Wiles - modularity) The Frey curve corresponds to a modular form f of level

$$\prod_{q \mid abc \text{ and } q \text{ prime}} q \text{ and weight 2.}$$

Proof of Fermat's last theorem

Theorem (Fermat's last theorem)

All solutions of $x^n + y^n = z^n$ in $\mathbb{Z}$ for $n \geq 3$ satisfy $xyz = 0$.

1. Suffices to consider $n = 4$ (Fermat) or $n = p$ prime.
2. (Frey) To a solution (a, b, c) one can associate the (semistable) elliptic curve $y^2 = x(x - a^p)(x + b^p)$.
3. (Wiles - modularity) The Frey curve corresponds to a modular form f of level
$$\prod_{q | abc \text{ and } q \text{ prime}} q \text{ and weight } 2.$$
4. (Ribet) This form is congruent mod p to one of level 2 and weight 2.

Proof of Fermat's last theorem

Theorem (Fermat's last theorem)

All solutions of $x^n + y^n = z^n$ in $\mathbb{Z}$ for $n \geq 3$ satisfy $xyz = 0$.

1. Suffices to consider $n = 4$ (Fermat) or $n = p$ prime.
2. (Frey) To a solution (a, b, c) one can associate the (semistable) elliptic curve $y^2 = x(x - a^p)(x + b^p)$.
3. (Wiles - modularity) The Frey curve corresponds to a modular form f of level

$$\prod_{q|abc \text{ and } q \text{ prime}} q \text{ and weight } 2.$$

4. (Ribet) This form is congruent mod p to one of level 2 and weight 2.
5. There are no modular forms of level 2 and weight 2.

Modularity over $\mathbb{Q}$

Theorem (Wiles, Taylor & Wiles, 1995.)

All semistable elliptic curves over $\mathbb{Q}$ are modular.

Modularity over $\mathbb{Q}$

Theorem (Wiles, Taylor & Wiles, 1995.)

All semistable elliptic curves over $\mathbb{Q}$ are modular.

Corollary (Wiles, 1995.)

Fermat's last theorem is true.

Modularity over $\mathbb{Q}$

Theorem (Wiles, Taylor & Wiles, 1995.)

All semistable elliptic curves over $\mathbb{Q}$ are modular.

Corollary (Wiles, 1995.)

Fermat's last theorem is true.

Theorem (Breuil, Conrad, Diamond & Taylor 2001.)

All elliptic curves over $\mathbb{Q}$ are modular.

Modularity over totally real number fields

Hilbert modular forms are generalizations of classical modular forms. They are "defined" over totally real number fields.

Hilbert modular forms are generalizations of classical modular forms. They are "defined" over totally real number fields.

As with classical modular forms, one can define the L-function $L(f, s)$ of a Hilbert modular form f.

Modularity over totally real number fields

Hilbert modular forms are generalizations of classical modular forms. They are "defined" over totally real number fields.

As with classical modular forms, one can define the L-function $L(f, s)$ of a Hilbert modular form f.

Definition

An elliptic curve E over a totally real number field K is **modular** if there exists a Hilbert modular form f over K of parallel weight 2 such that

$$L(E, s) = L(f, s).$$

A conjecture and known results

Conjecture

All elliptic curves over all totally real number fields are modular.

A conjecture and known results

Conjecture

All elliptic curves over all totally real number fields are modular.

Theorem (Jarvis and Manoharmayum 2008.)

Semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{17})$ *are modular.*

A conjecture and known results

Conjecture

All elliptic curves over all totally real number fields are modular.

Theorem (Jarvis and Manoharmayum 2008.)

Semistable elliptic curves over $\mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{17})$ *are modular.*

Theorem (Freitas, Le Hung, Siksek 2015.)

All elliptic curves over all real quadratic fields are modular.

Our result

Theorem (Derickx, N., Siksek 2018.)

All elliptic curves over all totally real cubic fields are modular.

Some definitions

Let K be a number field, $G_K := \mathrm{Gal}(\overline{K}/K)$, E/K an elliptic curve and p a prime.

Some definitions

Let K be a number field, $G_K := \mathrm{Gal}(\overline{K}/K)$, E/K an elliptic curve and p a prime.

$$E[p] := \left\{P \in E(\overline{K}) : [p]P = O\right\} = \ker[p].$$

Some definitions

Let K be a number field, $G_K := \mathrm{Gal}(\overline{K}/K)$, E/K an elliptic curve and p a prime.

$$E[p] := \{P \in E(\overline{K}) : [p]P = O\} = \ker[p].$$

G_K acts on $E[p]$ inducing a group homomorphism

$$\overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

called the mod p Galois representation attached to E.

Images of Galois

Let $G_E(p) := \overline{\rho}_{E,p}(G_K) \leq \mathrm{GL}_2(\mathbb{F}_p)$. Then one of the following is true:

(i) $G_E(p) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$.

Images of Galois

Let $G_E(p) := \overline{\rho}_{E,p}(G_K) \leq \mathrm{GL}_2(\mathbb{F}_p)$. Then one of the following is true:

(i) $G_E(p) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$.

(ii) The image $G_E(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is A_4, S_4 or A_5.

Images of Galois

Let $G_E(p) := \overline{\rho}_{E,p}(G_K) \leq \mathrm{GL}_2(\mathbb{F}_p)$. Then one of the following is true:

(i) $G_E(p) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$.

(ii) The image $G_E(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is A_4, S_4 or A_5.

(iii) $G_E(p)$ is conjugate to a subgroup of the Borel subgroup $B(p)$, the subgroup of upper triangular matrices.

Images of Galois

Let $G_E(p) := \overline{\rho}_{E,p}(G_K) \leq \mathrm{GL}_2(\mathbb{F}_p)$. Then one of the following is true:

(i) $G_E(p) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$.

(ii) The image $G_E(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is A_4, S_4 or A_5.

(iii) $G_E(p)$ is conjugate to a subgroup of the Borel subgroup $B(p)$, the subgroup of upper triangular matrices.

(iv) $G_E(p)$ is conjugate to a subgroup of the normalizer of the split Cartan subgroup $C_s^+(p)$.

Images of Galois

Let $G_E(p) := \overline{\rho}_{E,p}(G_K) \leq \mathrm{GL}_2(\mathbb{F}_p)$. Then one of the following is true:

(i) $G_E(p) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$.

(ii) The image $G_E(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is A_4, S_4 or A_5.

(iii) $G_E(p)$ is conjugate to a subgroup of the Borel subgroup $B(p)$, the subgroup of upper triangular matrices.

(iv) $G_E(p)$ is conjugate to a subgroup of the normalizer of the split Cartan subgroup $C_{\mathrm{s}}^{+}(p)$.

(v) $G_E(p)$ is conjugate to a subgroup of the normalizer of the non-split Cartan subgroup $C_{\mathrm{ns}}^{+}(p)$.

Let $G_E(p) := \overline{\rho}_{E,p}(G_K) \leq \mathrm{GL}_2(\mathbb{F}_p)$. Then one of the following is true:

(i) $G_E(p) \supseteq \mathrm{SL}_2(\mathbb{F}_p)$.

(ii) The image $G_E(p)$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is A_4, S_4 or A_5.

(iii) $G_E(p)$ is conjugate to a subgroup of the Borel subgroup $B(p)$, the subgroup of upper triangular matrices.

(iv) $G_E(p)$ is conjugate to a subgroup of the normalizer of the split Cartan subgroup $C_{\mathrm{s}}^{+}(p)$.

(v) $G_E(p)$ is conjugate to a subgroup of the normalizer of the non-split Cartan subgroup $C_{\mathrm{ns}}^{+}(p)$.

The K-points on the modular curves $X_0(p)$, $X_s(p)$ and $X_{ns}(p)$ correspond to elliptic curves over K for which $G_E(p)$ is in the cases (iii), (iv) and (v), respectively.

Theorem (Wiles, Breuil, Diamond, Kisin, Barnett–Lamb-Gee-Geraghty + Langlands-Tunnel)

Let K be a totally real number field and E an elliptic curve over K. Suppose that

- $\overline{\rho}_{E,3}$ *is irreducible ($\iff G_E(3) \not\subseteq B(3)$), and*
- $G_E(3)$ *is not contained in the normaliser of a split Cartan subgroup.*

Modularity lifting theorems

Theorem (Wiles, Breuil, Diamond, Kisin, Barnett–Lamb-Gee-Geraghty + Langlands-Tunnel)

Let K be a totally real number field and E an elliptic curve over K. Suppose that

- $\overline{\rho}_{E,3}$ *is irreducible* ($\Longleftrightarrow G_E(3) \not\subseteq B(3)$), *and*
- $G_E(3)$ *is not contained in the normaliser of a split Cartan subgroup.*

Then E is modular.

Theorem (Wiles, Breuil, Diamond, Kisin, Barnett–Lamb-Gee-Geraghty + Langlands-Tunnel)

Let K be a totally real number field and E an elliptic curve over K. Suppose that

- $\overline{\rho}_{E,3}$ *is irreducible* ($\iff G_E(3) \not\subseteq B(3)$), *and*
- $G_E(3)$ *is not contained in the normaliser of a split Cartan subgroup.*

Then E is modular.

So if E/K is not modular then $G_E(3)$ is contained in $B(3)$ or $C_s^+(3)$.

Modularity lifting theorems

Theorem (Thorne 2016)

Let E be an elliptic curve over a totally real number field K and suppose 5 is not a square in K and $G_E(5) \not\subseteq B(5)$. Then E is modular.

Modularity lifting theorems

Theorem (Thorne 2016)

Let E be an elliptic curve over a totally real number field K and suppose 5 is not a square in K and $G_E(5) \not\subseteq B(5)$. Then E is modular.

So if E/K is not modular then $G_E(5)$ is contained in $B(5)$.

Modularity lifting theorems

Theorem (Thorne 2016)

Let E be an elliptic curve over a totally real number field K and suppose 5 is not a square in K and $G_E(5) \not\subseteq B(5)$. Then E is modular.

So if E/K is not modular then $G_E(5)$ is contained in $B(5)$.

Theorem (Kalyanswamy 2016)

Let K be a totally real number field and E an elliptic curve over K and

- $K \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$.
- $G_E(7) \not\subseteq B(7)$
- $G_E(7) \not\subseteq C_{\mathrm{ns}}^{+}(7)$.

Then E is modular.

Modularity lifting theorems

Theorem (Thorne 2016)

Let E be an elliptic curve over a totally real number field K and suppose 5 is not a square in K and $G_E(5) \not\subseteq B(5)$. Then E is modular.

So if E/K is not modular then $G_E(5)$ is contained in $B(5)$.

Theorem (Kalyanswamy 2016)

Let K be a totally real number field and E an elliptic curve over K and

- $K \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$.
- $G_E(7) \not\subseteq B(7)$
- $G_E(7) \not\subseteq C_{\mathrm{ns}}^{+}(7)$.

Then E is modular.

So if $K \neq \mathbb{Q}(\zeta_7)^+$, and E/K is not modular then $G_E(7)$ is contained in $B(7)$ or $C_{\mathrm{ns}}^{+}(7)$.

Points on modular curves

It follows that: if E is not modular it gives rise to a K-point on $X_u(3) \times_{X(1)} X_0(5) \times_{X(1)} X_w(7)$ for some $u \in \{0, s\}$ and $w \in \{0, ns\}$.

Points on modular curves

It follows that: if E is not modular it gives rise to a K-point on $X_u(3) \times_{X(1)} X_0(5) \times_{X(1)} X_w(7)$ for some $u \in \{0, s\}$ and $w \in \{0, ns\}$.

Let $X(u3, b5, w7) := X_u(3) \times_{X(1)} X_0(5) \times_{X(1)} X_w(7)$, with "b" instead of "0", i.e.

$$X(b3, b5, ns7) = X_0(3) \times_{X(1)} X_0(5) \times_{X(1)} X_{ns}(7).$$

Points on modular curves

It follows that: if E is not modular it gives rise to a K-point on $X_u(3) \times_{X(1)} X_0(5) \times_{X(1)} X_w(7)$ for some $u \in \{0, s\}$ and $w \in \{0, ns\}$.

Let $X(u3, b5, w7) := X_u(3) \times_{X(1)} X_0(5) \times_{X(1)} X_w(7)$, with "b" instead of "0", i.e.

$$X(b3, b5, ns7) = X_0(3) \times_{X(1)} X_0(5) \times_{X(1)} X_{ns}(7).$$

If one finds the set of all the points of degree d on $X(b5, w7)$ for some $w \in \{0, ns\}$, then this set will contain all the points of degree d on $X(u3, b5, w7)$, for any u.

Freitas, Le Hung, Siksek needed to finding all quadratic points on 7 modular curves of genera $3, 3, 4, 73, 97, 113$ and 153, as the modularity lifting results known then were weaker.

Modularity over quadratic fields

Freitas, Le Hung, Siksek needed to finding all quadratic points on 7 modular curves of genera $3, 3, 4, 73, 97, 113$ and 153, as the modularity lifting results known then were weaker.

Remarkably, they manage to show that all the quadratic points on these curves correspond to modular elliptic curves.

The modular curves we need to consider

We will prove

(1) All elliptic curves over $\mathbb{Q}(\zeta_7)^+$ are modular.

(2) The modular curve $X(b5, b7)$ has no totally real non-cuspidal cubic points.

(3) The modular curve $X(b5, ns7)$ has no totally real non-cuspidal cubic points.

Dealing with $K = \mathbb{Q}(\zeta_7)^+$

The modular curves $X(b3, b5)$ and $X(s3, b5)$ are elliptic curves of conductor 15.

Dealing with $K = \mathbb{Q}(\zeta_7)^+$

The modular curves $X(b3, b5)$ and $X(s3, b5)$ are elliptic curves of conductor 15.

It is easy to check that their rank over K is 0, find all the elliptic curves corresponding to K-rational points on these modular curves.

Dealing with $K = \mathbb{Q}(\zeta_7)^+$

The modular curves $X(b3, b5)$ and $X(s3, b5)$ are elliptic curves of conductor 15.

It is easy to check that their rank over K is 0, find all the elliptic curves corresponding to K-rational points on these modular curves.

It turns out that all such curves are twists of elliptic curves defined over $\mathbb{Q}$, which are known to be modular.

The modular curve $X_0(35)$

The modular curve $X := X(b5, b7) = X_0(35)$ is a hyperelliptic curve of genus 3.

The modular curve $X := X(b5, b7) = X_0(35)$ is a hyperelliptic curve of genus 3.

We first want to show that X has finitely many cubic points.

The modular curve $X_0(35)$

The modular curve $X := X(b5, b7) = X_0(35)$ is a hyperelliptic curve of genus 3.

We first want to show that X has finitely many cubic points.

Theorem (Abramovich and Harris)

A curve defined over a number field K has infinitely many points of degree $d = 2$ or 3 over K iff it has a degree d map to $\mathbb{P}^1$ or an elliptic curve with poitive rank over K.

Finitely many cubic points on $X_0(35)$

Lemma

X has no degree 3 maps to $\mathbb{P}^1$.

Finitely many cubic points on $X_0(35)$

Lemma

X has no degree 3 maps to $\mathbb{P}^1$.

Proof:

Theorem (Castelnuovo-Severi inequality)

Let k be a perfect field, and X, Y, Z curves over k. Let $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ be morphisms of degree m and n respectively, and assume that there is no morphism $X \to X'$ of degree > 1 through which both π_Y and π_Z factor. Then

$$g(X) \leq m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1).$$

Finitely many cubic points on $X_0(35)$

Lemma

X has no degree 3 maps to $\mathbb{P}^1$.

Proof:

Theorem (Castelnuovo-Severi inequality)

Let k be a perfect field, and X, Y, Z curves over k. Let $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ be morphisms of degree m and n respectively, and assume that there is no morphism $X \to X'$ of degree > 1 through which both π_Y and π_Z factor. Then

$$g(X) \leq m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1).$$

Taking $Y = Z = \mathbb{P}^1$, $m = 2$, $n = 3$, we see that if X has a maps of both degree 2 and 3 to $\mathbb{P}^1$, then $g(X) \leq 2$. □

Finitely many cubic points on $X_0(35)$

Lemma

X has no degree 3 maps to an elliptic curve with positive rank over $\mathbb{Q}$.

Finitely many cubic points on $X_0(35)$

Lemma

X has no degree 3 maps to an elliptic curve with positive rank over $\mathbb{Q}$.

Proof: By modularity over $\mathbb{Q}$, if such an elliptic curve existed, it would have to have conductor dividing 35, and we check in LMFDB that the curves with conductor dividing 35 do not have positive rank.

The modular curve $X_0(35)$

X has 4 cusps, all defined over $\mathbb{Q}$, and has the following model:

$$X \;:\; y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1).$$

The modular curve $X_0(35)$

X has 4 cusps, all defined over $\mathbb{Q}$, and has the following model:

$$X \; : \; y^2 = (x^2 + x - 1)(x^6 - 5x^5 - 9x^3 - 5x - 1).$$

Denote $J := J(X)$. We have $J(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

The modular curve $X_0(35)$

Let K be a totally real cubic field, and for a point $P \in X(K)$, $P \notin X(\mathbb{Q})$, let P_1, P_2, P_3 be the conjugates of P given by the embeddings of K into $\overline{\mathbb{Q}}$.

The modular curve $X_0(35)$

Let K be a totally real cubic field, and for a point $P \in X(K)$, $P \notin X(\mathbb{Q})$, let P_1, P_2, P_3 be the conjugates of P given by the embeddings of K into $\overline{\mathbb{Q}}$.

Then $D = P_1 + P_2 + P_3$ is an irreducible $\mathbb{Q}$-divisor of degree 3.

The modular curve $X_0(35)$

Let K be a totally real cubic field, and for a point $P \in X(K)$, $P \notin X(\mathbb{Q})$, let P_1, P_2, P_3 be the conjugates of P given by the embeddings of K into $\overline{\mathbb{Q}}$.

Then $D = P_1 + P_2 + P_3$ is an irreducible $\mathbb{Q}$-divisor of degree 3.

Let $D_1, \ldots, D_{48}$ be $\mathbb{Q}$-divisors of degree 0 representing the 48 classes in $J(\mathbb{Q})$, and let $T_i = D_i + 3\infty_+$.

Let K be a totally real cubic field, and for a point $P \in X(K)$, $P \notin X(\mathbb{Q})$, let P_1, P_2, P_3 be the conjugates of P given by the embeddings of K into $\overline{\mathbb{Q}}$.

Then $D = P_1 + P_2 + P_3$ is an irreducible $\mathbb{Q}$-divisor of degree 3.

Let $D_1, \ldots, D_{48}$ be $\mathbb{Q}$-divisors of degree 0 representing the 48 classes in $J(\mathbb{Q})$, and let $T_i = D_i + 3\infty_+$.

Hence $D \sim T_i$, for some i.

The modular curve $X_0(35)$

Let K be a totally real cubic field, and for a point $P \in X(K)$, $P \notin X(\mathbb{Q})$, let P_1, P_2, P_3 be the conjugates of P given by the embeddings of K into $\overline{\mathbb{Q}}$.

Then $D = P_1 + P_2 + P_3$ is an irreducible $\mathbb{Q}$-divisor of degree 3.

Let $D_1, \ldots, D_{48}$ be $\mathbb{Q}$-divisors of degree 0 representing the 48 classes in $J(\mathbb{Q})$, and let $T_i = D_i + 3\infty_+$.

Hence $D \sim T_i$, for some i.

Let $L(T_i)$ be the Riemann–Roch space corresponding to T_i, $\ell(T_i)$ it's dimension, and $|T_i|$ be the corresponding complete linear system.

The modular curve $X_0(35)$

Let K be a totally real cubic field, and for a point $P \in X(K)$, $P \notin X(\mathbb{Q})$, let P_1, P_2, P_3 be the conjugates of P given by the embeddings of K into $\overline{\mathbb{Q}}$.

Then $D = P_1 + P_2 + P_3$ is an irreducible $\mathbb{Q}$-divisor of degree 3.

Let $D_1, \ldots, D_{48}$ be $\mathbb{Q}$-divisors of degree 0 representing the 48 classes in $J(\mathbb{Q})$, and let $T_i = D_i + 3\infty_+$.

Hence $D \sim T_i$, for some i.

Let $L(T_i)$ be the Riemann–Roch space corresponding to T_i, $\ell(T_i)$ it's dimension, and $|T_i|$ be the corresponding complete linear system.

Clifford's theorem on special divisors implies $\ell(T_i) = 1$ or 2.

The modular curve $X_0(35)$

Of the 48 possible T_i, 4 have $\ell(T_i) = 2$.

The modular curve $X_0(35)$

Of the 48 possible T_i, 4 have $\ell(T_i) = 2$.

If $\ell(T_i) = 2$, then $|T_i|$ contains a base point, so cannot contain an irreducible divisor.

The modular curve $X_0(35)$

Of the 48 possible T_i, 4 have $\ell(T_i) = 2$.

If $\ell(T_i) = 2$, then $|T_i|$ contains a base point, so cannot contain an irreducible divisor.

Let now $\ell(T_i) = 1$. Then $L(T_i) = \mathbb{Q}f_i$ for some f_i in $\mathbb{Q}(X)$, and $D \sim T_i + \text{div } f_i$.

Of the 48 possible T_i, 4 have $\ell(T_i) = 2$.

If $\ell(T_i) = 2$, then $|T_i|$ contains a base point, so cannot contain an irreducible divisor.

Let now $\ell(T_i) = 1$. Then $L(T_i) = \mathbb{Q}f_i$ for some f_i in $\mathbb{Q}(X)$, and $D \sim T_i + \operatorname{div} f_i$.

We can explicitly compute these R-R spaces using an algorithm of Hess.

The modular curve $X_0(35)$

Of the 48 possible T_i, 4 have $\ell(T_i) = 2$.

If $\ell(T_i) = 2$, then $|T_i|$ contains a base point, so cannot contain an irreducible divisor.

Let now $\ell(T_i) = 1$. Then $L(T_i) = \mathbb{Q}f_i$ for some f_i in $\mathbb{Q}(X)$, and $D \sim T_i + \operatorname{div} f_i$.

We can explicitly compute these R-R spaces using an algorithm of Hess.

We get that 28 of the remaining 44 T_i are irreducible, and all of the irreducible ones split over cubic fields with complex embeddings.

The modular curve $X(b5, ns7)$

Let from now on $X := X(b5, ns7)$, $J := J(X)$.

The modular curve $X(b5, ns7)$

Let from now on $X := X(b5, ns7)$, $J := J(X)$.

X is non-hyperelliptic of genus 6.

The modular curve $X(b5, ns7)$

Let from now on $X := X(b5, ns7)$, $J := J(X)$.

X is non-hyperelliptic of genus 6.

We prove that the gonality (the smallest degree of a map to $\mathbb{P}^1$) of X is 4 and that there will be only finitely many cubic points.

The modular curve $X(b5, ns7)$

Let from now on $X := X(b5, ns7)$, $J := J(X)$.

X is non-hyperelliptic of genus 6.

We prove that the gonality (the smallest degree of a map to $\mathbb{P}^1$) of X is 4 and that there will be only finitely many cubic points.

X has the following model:

The modular curve $X(b5, ns7)$

Let from now on $X := X(b5, ns7)$, $J := J(X)$.

X is non-hyperelliptic of genus 6.

We prove that the gonality (the smallest degree of a map to $\mathbb{P}^1$) of X is 4 and that there will be only finitely many cubic points.

X has the following model:

$$5u^6 - 50u^5v + 206u^4v^2 - 408u^3v^3 + 321u^2v^4 + 10uv^5 - 100v^6 + 9u^4w^2 - 60u^3vw^2 + 80u^2v^2w^2 + 48uv^3w^2 + 15v^4w^2 + 3u^2w^4 - 10uvw^4 + 6v^2w^4 - w^6 = 0.$$

The modular curve $X(b5, ns7)$

Let from now on $X := X(b5, ns7)$, $J := J(X)$.

X is non-hyperelliptic of genus 6.

We prove that the gonality (the smallest degree of a map to $\mathbb{P}^1$) of X is 4 and that there will be only finitely many cubic points.

X has the following model:

$$5u^6 - 50u^5v + 206u^4v^2 - 408u^3v^3 + 321u^2v^4 + 10uv^5 - 100v^6 + 9u^4w^2 - 60u^3vw^2 + 80u^2v^2w^2 + 48uv^3w^2 + 15v^4w^2 + 3u^2w^4 - 10uvw^4 + 6v^2w^4 - w^6 = 0.$$

Le Hung (2014): $J \sim A_1 \times A_2 \times A_3$, where A_i are absolutely simple modular abelian surfaces defined over $\mathbb{Q}$.

The modular curve $X(b5, ns7)$

Let from now on $X := X(b5, ns7)$, $J := J(X)$.

X is non-hyperelliptic of genus 6.

We prove that the gonality (the smallest degree of a map to $\mathbb{P}^1$) of X is 4 and that there will be only finitely many cubic points.

X has the following model:

$$5u^6 - 50u^5v + 206u^4v^2 - 408u^3v^3 + 321u^2v^4 + 10uv^5 - 100v^6 + 9u^4w^2 - 60u^3vw^2 + 80u^2v^2w^2 + 48uv^3w^2 + 15v^4w^2 + 3u^2w^4 - 10uvw^4 + 6v^2w^4 - w^6 = 0.$$

Le Hung (2014): $J \sim A_1 \times A_2 \times A_3$, where A_i are absolutely simple modular abelian surfaces defined over $\mathbb{Q}$.

We compute that the analytic ranks of A_1, A_2, A_3 over $\mathbb{Q}$ are $2, 0, 0$, respectively, so by results of Kolyvagin and Logachev, these are their ranks over $\mathbb{Q}$.

The modular curve $X(b5, ns7)$

The cusps of X form two Galois orbits of size 3. Denote by c_0, c_∞ divisors obtained by summing the cusps in each orbit.

The modular curve $X(b5, ns7)$

The cusps of X form two Galois orbits of size 3. Denote by c_0, c_∞ divisors obtained by summing the cusps in each orbit.

Proposition

$\mathrm{Aut}_{\mathbb{Q}} X = \langle w_5 \rangle \cong \mathbb{Z}/2\mathbb{Z}$

The modular curve $X(b5, ns7)$

The cusps of X form two Galois orbits of size 3. Denote by c_0, c_∞ divisors obtained by summing the cusps in each orbit.

Proposition

$\mathrm{Aut}_{\mathbb{Q}} X = \langle w_5 \rangle \cong \mathbb{Z}/2\mathbb{Z}$

The involution w_5 interchanges c_0 and c_∞.

The modular curve $X(b5, ns7)$

Proposition

$A := \mathrm{im}(w_5 - 1) \subseteq J$ *is a subabelian variety of dimension* 4 *with* $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$.

The modular curve $X(b5, ns7)$

Proposition

$A := \mathrm{im}(w_5 - 1) \subseteq J$ is a subabelian variety of dimension 4 with $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$.

Proof: We show that $A \sim A_2 \times A_3$, so the rank of $A(\mathbb{Q})$ is zero.

Proposition

$A := \mathrm{im}(w_5 - 1) \subseteq J$ *is a subabelian variety of dimension* 4 *with* $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$.

Proof: We show that $A \sim A_2 \times A_3$, so the rank of $A(\mathbb{Q})$ is zero.

We compute that the order of $[c_0 - c_\infty]$ is 7 and

$$(w_5 - 1)([3c_0 - 3c_\infty]) = 6[c_\infty - c_0] = [c_0 - c_\infty].$$

Therefore $[c_0 - c_\infty] \in A(\mathbb{Q})$.

Proposition

$A := \mathrm{im}(w_5 - 1) \subseteq J$ is a subabelian variety of dimension 4 with $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$.

Proof: We show that $A \sim A_2 \times A_3$, so the rank of $A(\mathbb{Q})$ is zero.

We compute that the order of $[c_0 - c_\infty]$ is 7 and

$$(w_5 - 1)([3c_0 - 3c_\infty]) = 6[c_\infty - c_0] = [c_0 - c_\infty].$$

Therefore $[c_0 - c_\infty] \in A(\mathbb{Q})$.

Also,

$$J(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/(7 \cdot 23)\mathbb{Z},$$

and

$$J(\mathbb{F}_{17}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2^2 \cdot 7^3 \cdot 31 \cdot 271)\mathbb{Z}.$$

Definition

A morphism $f : X \to Y$ of Noetherian schemes is a formal immersion at $x \in X$ if

$$\widehat{f} : \widehat{O_{Y,f(x)}} \to \widehat{O_{X,x}}$$

is surjective.

Formal immersions

Let K be a number field, $\wp$ a prime ideal of K. We define

$$\text{Res}_{\wp}(x) := \{x' \in X(K_{\wp}) : x \equiv x' \pmod{\wp}\}.$$

Formal immersions

Let K be a number field, $\wp$ a prime ideal of K. We define

$$\mathrm{Res}_\wp(x) := \{x' \in X(K_\wp) : x \equiv x' \pmod{\wp}\}.$$

Proposition

Let K be a number field, $\wp$ a prime ideal not dividing 2, $f : X \to Y$ a morphism of schemes, where Y is an abelian variety of rank 0 over K, and X, Y have good reduction at $\wp$, and let f be a formal immersion at $x \in X(\mathcal{O}_K/\wp)$. Then

$$X(K) \cap \mathrm{Res}_\wp(x) = \{x\}.$$

Completing the proof

Let $x \in X^{(3)}(\mathbb{Q})$.

Completing the proof

Let $x \in X^{(3)}(\mathbb{Q})$.

Since $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$, it follows that

$$(1 - w_5)[x - c_\infty] = \ell[c_0 - c_\infty], \text{ for some } \ell \in \mathbb{Z}/7\mathbb{Z}.$$

Completing the proof

Let $x \in X^{(3)}(\mathbb{Q})$.

Since $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$, it follows that

$$(1 - w_5)[x - c_\infty] = \ell[c_0 - c_\infty], \text{ for some } \ell \in \mathbb{Z}/7\mathbb{Z}.$$

We have $w_5(c_\infty) = c_0$, so we can rewrite the equation above as

$$(x - w_5(x)) \sim k \cdot (c_0 - c_\infty),$$

for some $k \in \{-3, \dots, 3\}$.

Let $x \in X^{(3)}(\mathbb{Q})$.

Since $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$, it follows that

$$(1 - w_5)[x - c_\infty] = \ell[c_0 - c_\infty], \text{ for some } \ell \in \mathbb{Z}/7\mathbb{Z}.$$

We have $w_5(c_\infty) = c_0$, so we can rewrite the equation above as

$$(x - w_5(x)) \sim k \cdot (c_0 - c_\infty),$$

for some $k \in \{-3, \dots, 3\}$.

Let $\widetilde{x}, \widetilde{c_\infty}, \widetilde{c_0} \in X^{(3)}(\mathbb{F}_3)$ be the reductions of x, c_∞, c_0 mod 3. So,

$$(\widetilde{x} - w_5(\widetilde{x})) \sim k \cdot (\widetilde{c_0} - \widetilde{c_\infty}).$$

Completing the proof

Let $x \in X^{(3)}(\mathbb{Q})$.

Since $A(\mathbb{Q}) = \langle [c_0 - c_\infty] \rangle \simeq \mathbb{Z}/7\mathbb{Z}$, it follows that

$$(1 - w_5)[x - c_\infty] = \ell[c_0 - c_\infty], \text{ for some } \ell \in \mathbb{Z}/7\mathbb{Z}.$$

We have $w_5(c_\infty) = c_0$, so we can rewrite the equation above as

$$(x - w_5(x)) \sim k \cdot (c_0 - c_\infty),$$

for some $k \in \{-3, \ldots, 3\}$.

Let $\widetilde{x}, \widetilde{c_\infty}, \widetilde{c_0} \in X^{(3)}(\mathbb{F}_3)$ be the reductions of x, c_∞, c_0 mod 3. So,

$$(\widetilde{x} - w_5(\widetilde{x})) \sim k \cdot (\widetilde{c_0} - \widetilde{c_\infty}).$$

We tested the above relation and get that it holds for only $\widetilde{x} = \widetilde{c_0}$ and $k = 1$ and $\widetilde{x} = \widetilde{c_\infty}$ and $k = -1$.

Completing the proof

Suppose WLOG that $\widetilde{x} = \widetilde{c_\infty}$. We want to show that $x = c_\infty$.

Completing the proof

Suppose WLOG that $\widetilde{x} = \widetilde{c_\infty}$. We want to show that $x = c_\infty$.

To do that we prove that $f : X^{(3)} \to A$ defined as the composition of the Abel-Jacobi map $\iota : X^{(3)} \to J$ and $(1 - w_5) : J \to A$ is a formal immersion at $\widetilde{c_\infty}$ using a criterion of Derickx, Kamienny, Stein and Stoll.

Completing the proof

Suppose WLOG that $\widetilde{x} = \widetilde{c_\infty}$. We want to show that $x = c_\infty$.

To do that we prove that $f : X^{(3)} \to A$ defined as the composition of the Abel-Jacobi map $\iota : X^{(3)} \to J$ and $(1 - w_5) : J \to A$ is a formal immersion at $\widetilde{c_\infty}$ using a criterion of Derickx, Kamienny, Stein and Stoll.

This completes the proof.

Thank you for your attention!