Modular Curves, Divisors and Twists

Ekin Ozman

Max Planck Institute for Mathematics-Bonn

June 15, 2011

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to an indeterminite polynomial equation.
- $ax + by = c$
- $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve
- Diophantine equations define algebraic curves and algebraic surfaces.

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to an indeterminite polynomial equation.
- $ax + by = c$
- $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve
- Diophantine equations define algebraic curves and algebraic surfaces.

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to an indeterminite polynomial equation.
- $ax + by = c$
- $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve
- Diophantine equations define algebraic curves and algebraic surfaces.

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to an indeterminite polynomial equation.
- $ax + by = c$
- $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve
- Diophantine equations define algebraic curves and algebraic surfaces.

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to an indeterminite polynomial equation.
- $ax + by = c$
- $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve
- Diophantine equations define algebraic curves and algebraic surfaces.

Diophantine Equations

- Diophantine equation $\Rightarrow$ integer solutions to an indeterminite polynomial equation.
- $ax + by = c$
- $x^n + y^n = z^n \Rightarrow$ Fermat's Equation
- $y^2 = x^3 + ax + b \Rightarrow$ Elliptic Curve
- Diophantine equations define algebraic curves and algebraic surfaces.

Elliptic Curves

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b are in a field k such that characteristic of k is not $2, 3$.
- Such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form an abelian group with identity element O.
- Field of definition matters. An elliptic curve is a torus over $\mathbb{C}$, but can be just a bunch of points over $\mathbb{Q}$ e.g. there are only 4 rational solutions to E above.

Elliptic Curves

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b are in a field k such that characteristic of k is not $2, 3$.
- Such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form an abelian group with identity element O.
- Field of definition matters. An elliptic curve is a torus over $\mathbb{C}$, but can be just a bunch of points over $\mathbb{Q}$ e.g. there are only 4 rational solutions to E above.

Elliptic Curves

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b are in a field k such that characteristic of k is not $2, 3$.
- Such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form an abelian group with identity element O.
- Field of definition matters. An elliptic curve is a torus over $\mathbb{C}$, but can be just a bunch of points over $\mathbb{Q}$ e.g. there are only 4 rational solutions to E above.

Elliptic Curves

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b are in a field k such that characteristic of k is not $2, 3$.
- Such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form an abelian group with identity element O.
- Field of definition matters. An elliptic curve is a torus over $\mathbb{C}$, but can be just a bunch of points over $\mathbb{Q}$ e.g. there are only 4 rational solutions to E above.

Elliptic Curves

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b are in a field k such that characteristic of k is not $2, 3$.
- Such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form an abelian group with identity element O.
- Field of definition matters. An elliptic curve is a torus over $\mathbb{C}$, but can be just a bunch of points over $\mathbb{Q}$ e.g. there are only 4 rational solutions to E above.

Elliptic Curves

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b are in a field k such that characteristic of k is not $2, 3$.
- Such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form an abelian group with identity element O.
- Field of definition matters. An elliptic curve is a torus over $\mathbb{C}$, but can be just a bunch of points over $\mathbb{Q}$ e.g. there are only 4 rational solutions to E above.

Elliptic Curves

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point O. The point O is called point at infinity.

- Given by $y^2 = x^3 + ax + b$, when a, b are in a field k such that characteristic of k is not $2, 3$.
- Such as $E : y^2 = x(x-1)(x+1)$.
- No cusp or self-intersection.
- Solutions form an abelian group with identity element O.
- Field of definition matters. An elliptic curve is a torus over $\mathbb{C}$, but can be just a bunch of points over $\mathbb{Q}$ e.g. there are only 4 rational solutions to E above.

Rational Points of Elliptic Curves

Definition

Given a field k and an elliptic curve $E : y^2 = x^3 + ax + b$ such that $a, b \in k$, $E(k)$ denotes the set of tuples $(x, y) \in k \times k$ that satisfy the equation of E. We call $E(k)$ **the set of k-rational points of E.**

Theorem (Mordell-Weil,1928)

Let K be a finite extension of $\mathbb{Q}$. Then $E(K)$ is a finitely generated abelian group.

So $E(K) = \mathbb{Z}^r \times$ torsion part,

- What are the possibilities for the torsion part?
- What can we say about the rank r?

Rational Points of Elliptic Curves

Definition

Given a field k and an elliptic curve $E : y^2 = x^3 + ax + b$ such that $a, b \in k$, $E(k)$ denotes the set of tuples $(x, y) \in k \times k$ that satisfy the equation of E. We call $E(k)$ **the set of k-rational points of E.**

Theorem (Mordell-Weil,1928)

Let K be a finite extension of $\mathbb{Q}$. Then $E(K)$ is a finitely generated abelian group.

So $E(K) = \mathbb{Z}^r \times$ torsion part,

- What are the possibilities for the torsion part?
- What can we say about the rank r?

Rational Points of Elliptic Curves

Definition

Given a field k and an elliptic curve $E : y^2 = x^3 + ax + b$ such that $a, b \in k$, $E(k)$ denotes the set of tuples $(x, y) \in k \times k$ that satisfy the equation of E. We call $E(k)$ **the set of k-rational points of E.**

Theorem (Mordell-Weil,1928)

Let K be a finite extension of $\mathbb{Q}$. Then $E(K)$ is a finitely generated abelian group.

So $E(K) = \mathbb{Z}^r \times$ torsion part,

- What are the possibilities for the torsion part?
- What can we say about the rank r?

Rational Points of Elliptic Curves

Definition

Given a field k and an elliptic curve $E : y^2 = x^3 + ax + b$ such that $a, b \in k$, $E(k)$ denotes the set of tuples $(x, y) \in k \times k$ that satisfy the equation of E. We call $E(k)$ **the set of k-rational points of E.**

Theorem (Mordell-Weil,1928)

Let K be a finite extension of $\mathbb{Q}$. Then $E(K)$ is a finitely generated abelian group.

So $E(K) = \mathbb{Z}^r \times$ torsion part,

- What are the possibilities for the torsion part?
- What can we say about the rank r?

Rational Points of Elliptic Curves

Definition

Given a field k and an elliptic curve $E : y^2 = x^3 + ax + b$ such that $a, b \in k$, $E(k)$ denotes the set of tuples $(x, y) \in k \times k$ that satisfy the equation of E. We call $E(k)$ **the set of k-rational points of E.**

Theorem (Mordell-Weil,1928)

Let K be a finite extension of $\mathbb{Q}$. Then $E(K)$ is a finitely generated abelian group.

So $E(K) = \mathbb{Z}^r \times$ torsion part,

- What are the possibilities for the torsion part?
- What can we say about the rank r?

Rank

Rank is a complete mystery, even for elliptic curves over $\mathbb{Q}$.

Conjecture: The rank of $E(\mathbb{Q})$ is arbitrarily large.

- The biggest exactly known rank is 18 (Elkies).
- Elliptic curves of rank at least 28 are known.
- One of the Clay's Millennium Problems *the Birch and Swinnerton-Dyer conjecture* is concerned with determining the rank.

Rank

Rank is a complete mystery, even for elliptic curves over $\mathbb{Q}$.

Conjecture: The rank of $E(\mathbb{Q})$ is arbitrarily large.

- The biggest exactly known rank is 18 (Elkies).
- Elliptic curves of rank at least 28 are known.
- One of the Clay's Millennium Problems *the Birch and Swinnerton-Dyer conjecture* is concerned with determining the rank.

Rank

Rank is a complete mystery, even for elliptic curves over $\mathbb{Q}$.

Conjecture: The rank of $E(\mathbb{Q})$ is arbitrarily large.

- The biggest exactly known rank is 18 (Elkies).
- Elliptic curves of rank at least 28 are known.
- One of the Clay's Millennium Problems *the Birch and Swinnerton-Dyer conjecture* is concerned with determining the rank.

Rank

Rank is a complete mystery, even for elliptic curves over $\mathbb{Q}$.

Conjecture: The rank of $E(\mathbb{Q})$ is arbitrarily large.

- The biggest exactly known rank is 18 (Elkies).
- Elliptic curves of rank at least 28 are known.
- One of the Clay's Millennium Problems *the Birch and Swinnerton-Dyer conjecture* is concerned with determining the rank.

Rank

Rank is a complete mystery, even for elliptic curves over $\mathbb{Q}$.

Conjecture: The rank of $E(\mathbb{Q})$ is arbitrarily large.

- The biggest exactly known rank is 18 (Elkies).
- Elliptic curves of rank at least 28 are known.
- One of the Clay's Millennium Problems *the Birch and Swinnerton-Dyer conjecture* is concerned with determining the rank.

Rank

Rank is a complete mystery, even for elliptic curves over $\mathbb{Q}$.

Conjecture: The rank of $E(\mathbb{Q})$ is arbitrarily large.

- The biggest exactly known rank is 18 (Elkies).
- Elliptic curves of rank at least 28 are known.
- One of the Clay's Millennium Problems *the Birch and Swinnerton-Dyer conjecture* is concerned with determining the rank.

Mazur's Theorem

Torsion part is well-studied. For instance:

Theorem (Mazur, 1977)

The torsion subgroup of $E(\mathbb{Q})$ is one of the 15 following groups: $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, ..., 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ with $N = 1, 2, 3, 4$. And examples for every case are known.

Classical Modular Curve $\Rightarrow$ classifes elliptic curves with torsion subgroup.

Mazur's Theorem

Torsion part is well-studied. For instance:

Theorem (Mazur, 1977)

The torsion subgroup of $E(\mathbb{Q})$ is one of the 15 following groups: $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, ..., 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ with $N = 1, 2, 3, 4$. And examples for every case are known.

Classical Modular Curve $\Rightarrow$ classifes elliptic curves with torsion subgroup.

Mazur's Theorem

Torsion part is well-studied. For instance:

Theorem (Mazur, 1977)

The torsion subgroup of $E(\mathbb{Q})$ is one of the 15 following groups: $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 2, ..., 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ with $N = 1, 2, 3, 4$. And examples for every case are known.

Classical Modular Curve $\Rightarrow$ classifes elliptic curves with torsion subgroup.

Maps Between Elliptic Curves

Definition

Let E_1, E_2 be two elliptic curves, an *isogeny* $\phi : E_1 \to E_2$ is a surjective morphism that maps O_1 to O_2.

- Every isogeny induces a homomorphism between K-rational points of E_1 and E_2.
- Isogenies have finite kernel.
- Conversely, for every finite subgroup G of $E(K)$, there exists an isogeny ϕ defined over K such that $ker(\phi) \cong G$.
- Every isogeny $\phi : E_1 \to E_2$ has a *dual*, $\hat{\phi} : E_2 \to E_1$.

isogenies $\Leftrightarrow$ finite subgroups

Maps Between Elliptic Curves

Definition

Let E_1, E_2 be two elliptic curves, an *isogeny* $\phi : E_1 \to E_2$ is a surjective morphism that maps O_1 to O_2.

- Every isogeny induces a homomorphism between K-rational points of E_1 and E_2.
- Isogenies have finite kernel.
- Conversely, for every finite subgroup G of $E(K)$, there exists an isogeny ϕ defined over K such that $ker(\phi) \cong G$.
- Every isogeny $\phi : E_1 \to E_2$ has a *dual*, $\hat{\phi} : E_2 \to E_1$.

isogenies $\Leftrightarrow$ finite subgroups

Maps Between Elliptic Curves

Definition

Let E_1, E_2 be two elliptic curves, an *isogeny* $\phi : E_1 \to E_2$ is a surjective morphism that maps O_1 to O_2.

- Every isogeny induces a homomorphism between K-rational points of E_1 and E_2.
- Isogenies have finite kernel.
- Conversely, for every finite subgroup G of $E(K)$, there exists an isogeny ϕ defined over K such that $ker(\phi) \cong G$.
- Every isogeny $\phi : E_1 \to E_2$ has a *dual*, $\hat{\phi} : E_2 \to E_1$.

isogenies $\Leftrightarrow$ finite subgroups

Maps Between Elliptic Curves

Definition

Let E_1, E_2 be two elliptic curves, an *isogeny* $\phi : E_1 \to E_2$ is a surjective morphism that maps O_1 to O_2.

- Every isogeny induces a homomorphism between K-rational points of E_1 and E_2.
- Isogenies have finite kernel.
- Conversely, for every finite subgroup G of $E(K)$, there exists an isogeny ϕ defined over K such that $ker(\phi) \cong G$.
- Every isogeny $\phi : E_1 \to E_2$ has a *dual*, $\hat{\phi} : E_2 \to E_1$.

isogenies $\Leftrightarrow$ finite subgroups

Maps Between Elliptic Curves

Definition

Let E_1, E_2 be two elliptic curves, an *isogeny* $\phi : E_1 \to E_2$ is a surjective morphism that maps O_1 to O_2.

- Every isogeny induces a homomorphism between K-rational points of E_1 and E_2.
- Isogenies have finite kernel.
- Conversely, for every finite subgroup G of $E(K)$, there exists an isogeny ϕ defined over K such that $ker(\phi) \cong G$.
- Every isogeny $\phi : E_1 \to E_2$ has a *dual*, $\hat{\phi} : E_2 \to E_1$.

isogenies $\Leftrightarrow$ finite subgroups

Maps Between Elliptic Curves

Definition

Let E_1, E_2 be two elliptic curves, an *isogeny* $\phi : E_1 \to E_2$ is a surjective morphism that maps O_1 to O_2.

- Every isogeny induces a homomorphism between K-rational points of E_1 and E_2.
- Isogenies have finite kernel.
- Conversely, for every finite subgroup G of $E(K)$, there exists an isogeny ϕ defined over K such that $ker(\phi) \cong G$.
- Every isogeny $\phi : E_1 \to E_2$ has a *dual*, $\hat{\phi} : E_2 \to E_1$.

isogenies $\Leftrightarrow$ finite subgroups

Moduli Space

Definition

A *moduli space* is a geometric space whose points represent other algebro-geometric objects of a fixed kind.

Definition

Quotient of upper half plane with the action of $\Gamma_0(N) := \{M \in SL_2(\mathbb{Z}) | M \mod N \text{ is upper triangular}\}$ is called **classical modular curve**, denoted as $X_0(N)$.

$X_0(N)$ is an algebraic curve, moreover it is a moduli space i.e.
$P \in X_0(N)(\mathbb{Q}) \Leftrightarrow (E, C)$ s.t. E is an ell. c. over $\mathbb{Q}$ and
$C \cong \mathbb{Z}/N\mathbb{Z}$ subgroup of N-torsion points of E, defined over $\mathbb{Q}$.
(elliptic curve + N-cyclic subgroup) $\Leftrightarrow$(elliptic curve + isogeny)
$\Leftrightarrow$ point on $X_0(N)$
To study $\mathbb{Q}$-rational torsion subgroups of E, we study $X_0(N)(\mathbb{Q})$

Moduli Space

Definition

A *moduli space* is a geometric space whose points represent other algebro-geometric objects of a fixed kind.

Definition

Quotient of upper half plane with the action of $\Gamma_0(N) := \{M \in SL_2(\mathbb{Z}) | M \mod N \text{ is upper triangular}\}$ is called **classical modular curve**, denoted as $X_0(N)$.

$X_0(N)$ is an algebraic curve, moreover it is a moduli space i.e.
$P \in X_0(N)(\mathbb{Q}) \Leftrightarrow (E, C)$ s.t. E is an ell. c. over $\mathbb{Q}$ and
$C \cong \mathbb{Z}/N\mathbb{Z}$ subgroup of N-torsion points of E, defined over $\mathbb{Q}$.
(elliptic curve + N-cyclic subgroup) $\Leftrightarrow$(elliptic curve + isogeny)
$\Leftrightarrow$ point on $X_0(N)$
To study $\mathbb{Q}$-rational torsion subgroups of E, we study $X_0(N)(\mathbb{Q})$

Moduli Space

Definition

A *moduli space* is a geometric space whose points represent other algebro-geometric objects of a fixed kind.

Definition

Quotient of upper half plane with the action of $\Gamma_0(N) := \{M \in SL_2(\mathbb{Z}) | M \mod N \text{ is upper triangular}\}$ is called **classical modular curve**, denoted as $X_0(N)$.

$X_0(N)$ is an algebraic curve, moreover it is a moduli space i.e. $P \in X_0(N)(\mathbb{Q}) \Leftrightarrow (E, C)$ s.t. E is an ell. c. over $\mathbb{Q}$ and $C \cong \mathbb{Z}/N\mathbb{Z}$ subgroup of N-torsion points of E, defined over $\mathbb{Q}$.
(elliptic curve + N-cyclic subgroup) $\Leftrightarrow$(elliptic curve + isogeny) $\Leftrightarrow$ point on $X_0(N)$
To study $\mathbb{Q}$-rational torsion subgroups of E, we study $X_0(N)(\mathbb{Q})$

Moduli Space

Definition

A *moduli space* is a geometric space whose points represent other algebro-geometric objects of a fixed kind.

Definition

Quotient of upper half plane with the action of $\Gamma_0(N) := \{M \in SL_2(\mathbb{Z}) | M \mod N \text{ is upper triangular}\}$ is called **classical modular curve**, denoted as $X_0(N)$.

$X_0(N)$ is an algebraic curve, moreover it is a moduli space i.e.
$P \in X_0(N)(\mathbb{Q}) \Leftrightarrow (E, C)$ s.t. E is an ell. c. over $\mathbb{Q}$ and $C \cong \mathbb{Z}/N\mathbb{Z}$ subgroup of N-torsion points of E, defined over $\mathbb{Q}$.
(elliptic curve + N-cyclic subgroup) $\Leftrightarrow$(elliptic curve + isogeny) $\Leftrightarrow$ point on $X_0(N)$
To study $\mathbb{Q}$-rational torsion subgroups of E, we study $X_0(N)(\mathbb{Q})$

Moduli Space

Definition

A *moduli space* is a geometric space whose points represent other algebro-geometric objects of a fixed kind.

Definition

Quotient of upper half plane with the action of $\Gamma_0(N) := \{M \in SL_2(\mathbb{Z}) | M \mod N \text{ is upper triangular}\}$ is called **classical modular curve**, denoted as $X_0(N)$.

$X_0(N)$ is an algebraic curve, moreover it is a moduli space i.e. $P \in X_0(N)(\mathbb{Q}) \Leftrightarrow (E, C)$ s.t. E is an ell. c. over $\mathbb{Q}$ and $C \cong \mathbb{Z}/N\mathbb{Z}$ subgroup of N-torsion points of E, defined over $\mathbb{Q}$.
(elliptic curve + N-cyclic subgroup) $\Leftrightarrow$(elliptic curve + isogeny) $\Leftrightarrow$ point on $X_0(N)$
To study $\mathbb{Q}$-rational torsion subgroups of E, we study $X_0(N)(\mathbb{Q})$

Moduli Space

Definition

A *moduli space* is a geometric space whose points represent other algebro-geometric objects of a fixed kind.

Definition

Quotient of upper half plane with the action of $\Gamma_0(N) := \{M \in SL_2(\mathbb{Z}) | M \mod N \text{ is upper triangular}\}$ is called **classical modular curve**, denoted as $X_0(N)$.

$X_0(N)$ is an algebraic curve, moreover it is a moduli space i.e. $P \in X_0(N)(\mathbb{Q}) \Leftrightarrow (E, C)$ s.t. E is an ell. c. over $\mathbb{Q}$ and $C \cong \mathbb{Z}/N\mathbb{Z}$ subgroup of N-torsion points of E, defined over $\mathbb{Q}$.
(elliptic curve + N-cyclic subgroup) $\Leftrightarrow$(elliptic curve + isogeny) $\Leftrightarrow$ point on $X_0(N)$
To study $\mathbb{Q}$-rational torsion subgroups of E, we study $X_0(N)(\mathbb{Q})$

Moduli Space

Definition

A *moduli space* is a geometric space whose points represent other algebro-geometric objects of a fixed kind.

Definition

Quotient of upper half plane with the action of $\Gamma_0(N) := \{M \in SL_2(\mathbb{Z}) | M \mod N \text{ is upper triangular}\}$ is called **classical modular curve**, denoted as $X_0(N)$.

$X_0(N)$ is an algebraic curve, moreover it is a moduli space i.e. $P \in X_0(N)(\mathbb{Q}) \Leftrightarrow (E, C)$ s.t. E is an ell. c. over $\mathbb{Q}$ and $C \cong \mathbb{Z}/N\mathbb{Z}$ subgroup of N-torsion points of E, defined over $\mathbb{Q}$.
(elliptic curve + N-cyclic subgroup) $\Leftrightarrow$(elliptic curve + isogeny) $\Leftrightarrow$ point on $X_0(N)$
To study $\mathbb{Q}$-rational torsion subgroups of E, we study $X_0(N)(\mathbb{Q})$

Twisting

Definition

Given a curve X over $\mathbb{Q}$ its *twist* is another curve over $\mathbb{Q}$ that is isomorphic to X over $\bar{\mathbb{Q}}$.

Remark

Geometrically a curve and its twist are the same.
but arithmetically not... action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *differs.*

Twisting

Definition

Given a curve X over $\mathbb{Q}$ its *twist* is another curve over $\mathbb{Q}$ that is isomorphic to X over $\bar{\mathbb{Q}}$.

Remark

Geometrically a curve and its twist are the same.
but arithmetically not... action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *differs.*

Twisting

Definition

Given a curve X over $\mathbb{Q}$ its *twist* is another curve over $\mathbb{Q}$ that is isomorphic to X over $\bar{\mathbb{Q}}$.

Remark

Geometrically a curve and its twist are the same.
but arithmetically not... action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ differs.

Twisting

Definition

Given a curve X over $\mathbb{Q}$ its *twist* is another curve over $\mathbb{Q}$ that is isomorphic to X over $\bar{\mathbb{Q}}$.

Remark

Geometrically a curve and its twist are the same.
but arithmetically not... action of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *differs.*

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = < \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = < \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.

Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi)$, E ell. c. and $\phi : E \to E'$ an isogeny.

Definition

Involution w_N on $X_0(N)$: $(E, \phi) \Leftrightarrow (E', \hat{\phi})$

Let $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) =< \sigma >$.
Redefine the action of σ on $X_0(N)$ as: $P^\sigma := w_N \circ \sigma(P)$.

- This is a twist of $X_0(N)$! Denoted by $X^d(N)$.
- $X_0(N)$ and $X^d(N)$ are isomorphic over K.
- $X^d(N)(\mathbb{Q}) = \{P \in X_0(N)(K) | P = w_N(\sigma(P))\}$
- $X^d(N)$ is also a moduli space!
  Rational points of $X^d(N) \Leftrightarrow$ "'Quadratic $\mathbb{Q}$-curves of degree N"'

$\mathbb{Q}$-curves

Definition

A quadratic $\mathbb{Q}$-curve of degree N is an elliptic curve E defined over a quadratic field $\mathbb{Q}(\sqrt{d})$ such that E and its Galois conjugate E^σ are isogenous via $\phi : E \to E^\sigma$, kernel of ϕ is $\mathbb{Z}/N\mathbb{Z}$.

Why do we care???

Fermat's Last Theoem

- $x^n + y^n = z^n \Leftrightarrow$ elliptic curves over $\mathbb{Q}$.
- *twisted* Fermat, $x^n + y^m = z^k \Leftrightarrow \mathbb{Q}$-curves.

Definition

A quadratic $\mathbb{Q}$-curve of degree N is an elliptic curve E defined over a quadratic field $\mathbb{Q}(\sqrt{d})$ such that E and its Galois conjugate E^σ are isogenous via $\phi : E \to E^\sigma$, kernel of ϕ is $\mathbb{Z}/N\mathbb{Z}$.

Why do we care???

Fermat's Last Theoem

- $x^n + y^n = z^n \Leftrightarrow$ elliptic curves over $\mathbb{Q}$.
- *twisted* Fermat, $x^n + y^m = z^k \Leftrightarrow \mathbb{Q}$-curves.

Definition

A quadratic $\mathbb{Q}$-curve of degree N is an elliptic curve E defined over a quadratic field $\mathbb{Q}(\sqrt{d})$ such that E and its Galois conjugate E^σ are isogenous via $\phi : E \to E^\sigma$, kernel of ϕ is $\mathbb{Z}/N\mathbb{Z}$.

Why do we care???

Fermat's Last Theoem

- $x^n + y^n = z^n \Leftrightarrow$ elliptic curves over $\mathbb{Q}$.
- *twisted* Fermat, $x^n + y^m = z^k \Leftrightarrow$ $\mathbb{Q}$-curves.

Definition

A quadratic $\mathbb{Q}$-curve of degree N is an elliptic curve E defined over a quadratic field $\mathbb{Q}(\sqrt{d})$ such that E and its Galois conjugate E^σ are isogenous via $\phi : E \to E^\sigma$, kernel of ϕ is $\mathbb{Z}/N\mathbb{Z}$.

Why do we care???

Fermat's Last Theoem

- $x^n + y^n = z^n \Leftrightarrow$ elliptic curves over $\mathbb{Q}$.
- *twisted* Fermat, $x^n + y^m = z^k \Leftrightarrow \mathbb{Q}$-curves.

Definition

A quadratic $\mathbb{Q}$-curve of degree N is an elliptic curve E defined over a quadratic field $\mathbb{Q}(\sqrt{d})$ such that E and its Galois conjugate E^σ are isogenous via $\phi : E \to E^\sigma$, kernel of ϕ is $\mathbb{Z}/N\mathbb{Z}$.

Why do we care???

Fermat's Last Theoem

- $x^n + y^n = z^n \Leftrightarrow$ elliptic curves over $\mathbb{Q}$.
- *twisted* Fermat, $x^n + y^m = z^k \Leftrightarrow \mathbb{Q}$-curves.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties. (Frey, 1984)
Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties. (Frey, 1984)
Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties. (Frey, 1984)

Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties.
(Frey, 1984)

Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties. (Frey, 1984)
Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties.
(Frey, 1984)
Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties. (Frey, 1984)
Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Theorem (Wiles,1995)

There are no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.

Say (a, b, c) is a solution for exponent $n > 2$, then the corresponding elliptic curve
$y^2 = x(x - a^n)(x + b^n)$ would have very unusual properties. (Frey, 1984)
Similarly, say (A, B, C) are coprime positive integers such that $A^4 + B^2 = C^p$ then the $\mathbb{Q}$-curve
$E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$ would have very unusual properties. (Ellenberg-Skinner, 2001)

Theorem (Ellenberg, 2004)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Field of Definition

Given C, a quadratic $\mathbb{Q}$-curve of degree N: Which quadratic field it is defined over? *if over* $\mathbb{Q}(\sqrt{d})$ *then* C *corresponds to a* $P \in X^d(N)(\mathbb{Q})$.

For which (d, N), $X^d(N)(\mathbb{Q}) \neq \emptyset$?

Quick answer: *Not for all* d *and* N.

Field of Definition

Given C, a quadratic $\mathbb{Q}$-curve of degree N: Which quadratic field it is defined over? *if over $\mathbb{Q}(\sqrt{d})$ then C corresponds to a $P \in X^d(N)(\mathbb{Q})$.*

For which (d, N), $X^d(N)(\mathbb{Q}) \neq \emptyset$?

Quick answer: *Not for all d and N.*

Field of Definition

Given C, a quadratic $\mathbb{Q}$-curve of degree N: Which quadratic field it is defined over? *if over* $\mathbb{Q}(\sqrt{d})$ *then* C *corresponds to a* $P \in X^d(N)(\mathbb{Q})$.

For which (d, N), $X^d(N)(\mathbb{Q}) \neq \emptyset$?

Quick answer: *Not for all* d *and* N.

Field of Definition

Given C, a quadratic $\mathbb{Q}$-curve of degree N: Which quadratic field it is defined over? *if over* $\mathbb{Q}(\sqrt{d})$ *then* C *corresponds to a* $P \in X^d(N)(\mathbb{Q})$.

For which (d, N), $X^d(N)(\mathbb{Q}) \neq \emptyset$?

Quick answer: *Not for all* d *and* N.

Field of Definition

Given C, a quadratic $\mathbb{Q}$-curve of degree N: Which quadratic field it is defined over? *if over* $\mathbb{Q}(\sqrt{d})$ *then* C *corresponds to a* $P \in X^d(N)(\mathbb{Q})$.

For which (d, N), $X^d(N)(\mathbb{Q}) \neq \emptyset$?

Quick answer: *Not for all* d *and* N.

Local Points

Checking all the *local points* is the first thing to do.

If $X^d(N)(\mathbb{Q})$ is non-empty then $X^d(\mathbb{Q}_p)$ is non-empty for all p as well.
Question: Given (N, d, p) what can be said about $X^d(N)(\mathbb{Q}_p)$?

Theorem (O,2009)

Given $(N, d, p) \Rightarrow$ necessary and sufficient conditions for $X^d(N)(\mathbb{Q}_p)$ to be non-empty.

Local Points

Checking all the *local points* is the first thing to do.

If $X^d(N)(\mathbb{Q})$ is non-empty then $X^d(\mathbb{Q}_p)$ is non-empty for all p as well.

Question: Given (N, d, p) what can be said about $X^d(N)(\mathbb{Q}_p)$?

Theorem (O,2009)

Given $(N, d, p) \Rightarrow$ necessary and sufficient conditions for $X^d(N)(\mathbb{Q}_p)$ to be non-empty.

Local Points

Checking all the *local points* is the first thing to do.

If $X^d(N)(\mathbb{Q})$ is non-empty then $X^d(\mathbb{Q}_p)$ is non-empty for all p as well.
Question: Given (N, d, p) what can be said about $X^d(N)(\mathbb{Q}_p)$?

Theorem (O,2009)

Given $(N, d, p) \Rightarrow$ necessary and sufficient conditions for $X^d(N)(\mathbb{Q}_p)$ to be non-empty.

Local Points

Checking all the *local points* is the first thing to do.

If $X^d(N)(\mathbb{Q})$ is non-empty then $X^d(\mathbb{Q}_p)$ is non-empty for all p as well.
Question: Given (N, d, p) what can be said about $X^d(N)(\mathbb{Q}_p)$?

Theorem (O,2009)

Given $(N, d, p) \Rightarrow$ necessary and sufficient conditions for $X^d(N)(\mathbb{Q}_p)$ to be non-empty.

Violations of the Hasse Principle

Given a curve C, if $P \in C(\mathbb{Q})$ then $P \in C(\mathbb{Q}_p)$. What about the reverse?

Definition

If a curve C has real and $\mathbb{Q}_p$-points for every prime p but no $\mathbb{Q}$-points then we say that C violates **the Hasse Principle.**

A conic never violates the Hasse Principle but for higher genus curves there are many examples of the violation.

Violations of the Hasse Principle

Given a curve C, if $P \in C(\mathbb{Q})$ then $P \in C(\mathbb{Q}_p)$. What about the reverse?

Definition

If a curve C has real and $\mathbb{Q}_p$-points for every prime p but no $\mathbb{Q}$-points then we say that C violates **the Hasse Principle.**

A conic never violates the Hasse Principle but for higher genus curves there are many examples of the violation.

Violations of the Hasse Principle

Given a curve C, if $P \in C(\mathbb{Q})$ then $P \in C(\mathbb{Q}_p)$. What about the reverse?

Definition

If a curve C has real and $\mathbb{Q}_p$-points for every prime p but no $\mathbb{Q}$-points then we say that C violates **the Hasse Principle.**

A conic never violates the Hasse Principle but for higher genus curves there are many examples of the violation.

Example

Let $N = 23, d = 17$ then the genus 2 twisted modular curve $X^d(N)$ violates the Hasse Principle.

Theorem (Ozman,2010)

Given N, the number of the twists $X^d(N)$ which violate the Hasse Principle is given by an explicit asymptotic. In particular they have positive density.

Example

Let $N = 23, d = 17$ then the genus 2 twisted modular curve $X^d(N)$ violates the Hasse Principle.

Theorem (Ozman,2010)

Given N, the number of the twists $X^d(N)$ which violate the Hasse Principle is given by an explicit asymptotic. In particular they have positive density.

Brauer-Manin Obstruction

What is the reason for the violation of the Hasse Principle?

Conjecture: For curves, *Brauer-Manin Obstruction* explains the violation of the Hasse Principle.

- Given a curve C, we consider a subset C^{Br} of $\prod_p C(\mathbb{Q}_p)$ which contains $C(\mathbb{Q})$.
- If C^{Br} is empty then $C(\mathbb{Q})$ is empty.
- If C violates the Hasse Principle and C^{Br} is empty then we say that Brauer-Manin obstruction explains the violation of the Hasse Principle.

Remark: The violation of the twisted curve $X^d(N)$ with $N = 23, d = 17$ mentioned before is explained by Brauer-Manin obstruction.

Brauer-Manin Obstruction

What is the reason for the violation of the Hasse Principle?
Conjecture: For curves, *Brauer-Manin Obstruction* explains the violation of the Hasse Principle.

- Given a curve C, we consider a subset C^{Br} of $\prod_p C(\mathbb{Q}_p)$ which contains $C(\mathbb{Q})$.
- If C^{Br} is empty then $C(\mathbb{Q})$ is empty.
- If C violates the Hasse Principle and C^{Br} is empty then we say that Brauer-Manin obstruction explains the violation of the Hasse Principle.

Remark: The violation of the twisted curve $X^d(N)$ with $N = 23, d = 17$ mentioned before is explained by Brauer-Manin obstruction.

Brauer-Manin Obstruction

What is the reason for the violation of the Hasse Principle?
Conjecture: For curves, *Brauer-Manin Obstruction* explains the violation of the Hasse Principle.

- Given a curve C, we consider a subset C^{Br} of $\prod_p C(\mathbb{Q}_p)$ which contains $C(\mathbb{Q})$.
- If C^{Br} is empty then $C(\mathbb{Q})$ is empty.
- If C violates the Hasse Principle and C^{Br} is empty then we say that Brauer-Manin obstruction explains the violation of the Hasse Principle.

Remark: The violation of the twisted curve $X^d(N)$ with $N = 23, d = 17$ mentioned before is explained by Brauer-Manin obstruction.

Brauer-Manin Obstruction

What is the reason for the violation of the Hasse Principle?
Conjecture: For curves, *Brauer-Manin Obstruction* explains the violation of the Hasse Principle.

- Given a curve C, we consider a subset C^{Br} of $\prod_p C(\mathbb{Q}_p)$ which contains $C(\mathbb{Q})$.
- If C^{Br} is empty then $C(\mathbb{Q})$ is empty.
- If C violates the Hasse Principle and C^{Br} is empty then we say that Brauer-Manin obstruction explains the violation of the Hasse Principle.

Remark: The violation of the twisted curve $X^d(N)$ with $N = 23, d = 17$ mentioned before is explained by Brauer-Manin obstruction.

Brauer-Manin Obstruction

What is the reason for the violation of the Hasse Principle?
Conjecture: For curves, *Brauer-Manin Obstruction* explains the violation of the Hasse Principle.

- Given a curve C, we consider a subset C^{Br} of $\prod_p C(\mathbb{Q}_p)$ which contains $C(\mathbb{Q})$.
- If C^{Br} is empty then $C(\mathbb{Q})$ is empty.
- If C violates the Hasse Principle and C^{Br} is empty then we say that Brauer-Manin obstruction explains the violation of the Hasse Principle.

Remark: The violation of the twisted curve $X^d(N)$ with $N = 23, d = 17$ mentioned before is explained by Brauer-Manin obstruction.

Brauer-Manin Obstruction

What is the reason for the violation of the Hasse Principle?
Conjecture: For curves, *Brauer-Manin Obstruction* explains the violation of the Hasse Principle.

- Given a curve C, we consider a subset C^{Br} of $\prod_p C(\mathbb{Q}_p)$ which contains $C(\mathbb{Q})$.
- If C^{Br} is empty then $C(\mathbb{Q})$ is empty.
- If C violates the Hasse Principle and C^{Br} is empty then we say that Brauer-Manin obstruction explains the violation of the Hasse Principle.

Remark: The violation of the twisted curve $X^d(N)$ with $N = 23, d = 17$ mentioned before is explained by Brauer-Manin obstruction.

Period-Index Problems

To check BM obstruction explains the violation of the Hasse Principle we need a rational degree one divisor.

Definition

A divisor of a curve is formal sum of its points. Given a divisor $D = \sum n_i P_i$ where $n_i \in \mathbb{Z}$, the degree of D is sum of n_i's. The group of divisors of degree one on a curve C is denoted as $\mathrm{Pic}^1(C)$.

Question: Given curve C, $\mathrm{Pic}^1(C)(\mathbb{Q})$ is empty or not?

Example

Let E be the elliptic curve $y^2 + y = x^3$ defined over $\mathbb{Q}(\sqrt{-3})$. Then $P_1 = (-1, 1/2(\sqrt{-3} - 1))$, $P_2 = (-1, 1/2(-\sqrt{-3} - 1))$ are points on E and $D = P_1 + P_2$ is a divisor on E. Moreover degree of D is 2 and D is defined over $\mathbb{Q}$, since P_1, P_2 are Galois conjugate.

Period-Index Problems

To check BM obstruction explains the violation of the Hasse Principle we need a rational degree one divisor.

Definition

A divisor of a curve is formal sum of its points. Given a divisor $D = \sum n_i P_i$ where $n_i \in \mathbb{Z}$, the degree of D is sum of n_i's. The group of divisors of degree one on a curve C is denoted as $\mathrm{Pic}^1(C)$.

Question: Given curve C, $\mathrm{Pic}^1(C)(\mathbb{Q})$ is empty or not?

Example

Let E be the elliptic curve $y^2 + y = x^3$ defined over $\mathbb{Q}(\sqrt{-3})$. Then $P_1 = (-1, 1/2(\sqrt{-3} - 1))$, $P_2 = (-1, 1/2(-\sqrt{-3} - 1))$ are points on E and $D = P_1 + P_2$ is a divisor on E. Moreover degree of D is 2 and D is defined over $\mathbb{Q}$, since P_1, P_2 are Galois conjugate.

Period-Index Problems

To check BM obstruction explains the violation of the Hasse Principle we need a rational degree one divisor.

Definition

A divisor of a curve is formal sum of its points. Given a divisor $D = \sum n_i P_i$ where $n_i \in \mathbb{Z}$, the degree of D is sum of n_i's. The group of divisors of degree one on a curve C is denoted as $\mathrm{Pic}^1(C)$.

Question: Given curve C, $\mathrm{Pic}^1(C)(\mathbb{Q})$ is empty or not?

Example

Let E be the elliptic curve $y^2 + y = x^3$ defined over $\mathbb{Q}(\sqrt{-3})$. Then $P_1 = (-1, 1/2(\sqrt{-3} - 1))$, $P_2 = (-1, 1/2(-\sqrt{-3} - 1))$ are points on E and $D = P_1 + P_2$ is a divisor on E. Moreover degree of D is 2 and D is defined over $\mathbb{Q}$, since P_1, P_2 are Galois conjugate.

Period-Index Problems

To check BM obstruction explains the violation of the Hasse Principle we need a rational degree one divisor.

Definition

A divisor of a curve is formal sum of its points. Given a divisor $D = \sum n_i P_i$ where $n_i \in \mathbb{Z}$, the degree of D is sum of n_i's. The group of divisors of degree one on a curve C is denoted as $\mathrm{Pic}^1(C)$.

Question: Given curve C, $\mathrm{Pic}^1(C)(\mathbb{Q})$ is empty or not?

Example

Let E be the elliptic curve $y^2 + y = x^3$ defined over $\mathbb{Q}(\sqrt{-3})$. Then $P_1 = (-1, 1/2(\sqrt{-3} - 1))$, $P_2 = (-1, 1/2(-\sqrt{-3} - 1))$ are points on E and $D = P_1 + P_2$ is a divisor on E. Moreover degree of D is 2 and D is defined over $\mathbb{Q}$, since P_1, P_2 are Galois conjugate.

Period-Index Problems

To check BM obstruction explains the violation of the Hasse Principle we need a rational degree one divisor.

Definition

A divisor of a curve is formal sum of its points. Given a divisor $D = \sum n_i P_i$ where $n_i \in \mathbb{Z}$, the degree of D is sum of n_i's. The group of divisors of degree one on a curve C is denoted as $\mathrm{Pic}^1(C)$.

Question: Given curve C, $\mathrm{Pic}^1(C)(\mathbb{Q})$ is empty or not?

Example

Let E be the elliptic curve $y^2 + y = x^3$ defined over $\mathbb{Q}(\sqrt{-3})$. Then $P_1 = (-1, 1/2(\sqrt{-3} - 1))$, $P_2 = (-1, 1/2(-\sqrt{-3} - 1))$ are points on E and $D = P_1 + P_2$ is a divisor on E. Moreover degree of D is 2 and D is defined over $\mathbb{Q}$, since P_1, P_2 are Galois conjugate.

Period-Index Problems

To check BM obstruction explains the violation of the Hasse Principle we need a rational degree one divisor.

Definition

A divisor of a curve is formal sum of its points. Given a divisor $D = \sum n_i P_i$ where $n_i \in \mathbb{Z}$, the degree of D is sum of n_i's. The group of divisors of degree one on a curve C is denoted as $\mathrm{Pic}^1(C)$.

Question: Given curve C, $\mathrm{Pic}^1(C)(\mathbb{Q})$ is empty or not?

Example

Let E be the elliptic curve $y^2 + y = x^3$ defined over $\mathbb{Q}(\sqrt{-3})$. Then $P_1 = (-1, 1/2(\sqrt{-3} - 1))$, $P_2 = (-1, 1/2(-\sqrt{-3} - 1))$ are points on E and $D = P_1 + P_2$ is a divisor on E. Moreover degree of D is 2 and D is defined over $\mathbb{Q}$, since P_1, P_2 are Galois conjugate.

Period-Index Results

Theorem (Ozman,2010)

Let $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ for all p and N be a prime number with numerator of $\frac{N-1}{12}$ is odd. Then there is a rational degree one divisor on $X^d(N)$.

Theorem (Ozman,2010)

Let $N > 3$ be a prime that is inert in the quadratic number field K. Then $\mathrm{Pic}^1(X^d(N))(\mathbb{Q}_N)$ is empty if and only if numerator of $\frac{N-1}{12}$ is even.

Period-Index Results

Theorem (Ozman,2010)

Let $X^d(N)(\mathbb{Q}_p) \neq \emptyset$ for all p and N be a prime number with numerator of $\frac{N-1}{12}$ is odd. Then there is a rational degree one divisor on $X^d(N)$.

Theorem (Ozman,2010)

Let $N > 3$ be a prime that is inert in the quadratic number field K. Then $\mathrm{Pic}^1(X^d(N))(\mathbb{Q}_N)$ is empty if and only if numerator of $\frac{N-1}{12}$ is even.

Thank you!