Rational points on Shimura curves

Carlos de Vera Piquero

Universitat Politècnica de Catalunya

March 23rd - Sázava, Česká republika

Outline

Why Shimura curves?

- General theory: Shimura (1959-1970), Čerednik-Drinfeld (1976), Morita (1981), Jordan-Livné (1986),...
- Diophantine properties: Jordan-Livné (1985, 1987), Ogg (1985), Elkies (1998),...

Why Shimura curves?

- General theory: Shimura (1959-1970), Čerednik-Drinfeld (1976), Morita (1981), Jordan-Livné (1986),...
- Diophantine properties: Jordan-Livné (1985, 1987), Ogg (1985), Elkies (1998),...

- They generalize modular curves and have connections with Fermat's Last Theorem.
- Connections with p-adic L-functions and BSD conjecture.
- Applications to the theory of error-correcting-codes.
- ...

Modular interpretation and rational points

- Shimura curves are moduli spaces for abelian surfaces whose endomorphism ring contains an order in an indefinite rational quaternion algebra.

Modular interpretation and rational points

- Shimura curves are moduli spaces for abelian surfaces whose endomorphism ring contains an order in an indefinite rational quaternion algebra.
  - $\rightsquigarrow$ Studying these abelian surfaces we can describe some properties of Shimura curves.

Modular interpretation and rational points

- Shimura curves are moduli spaces for abelian surfaces whose endomorphism ring contains an order in an indefinite rational quaternion algebra.
  - $\rightsquigarrow$ Studying these abelian surfaces we can describe some properties of Shimura curves.

- Shimura curves have no real points, hence no rational points.

Modular interpretation and rational points

- Shimura curves are moduli spaces for abelian surfaces whose endomorphism ring contains an order in an indefinite rational quaternion algebra.
  - $\rightsquigarrow$ Studying these abelian surfaces we can describe some properties of Shimura curves.

- Shimura curves have no real points, hence no rational points.
- Over number fields, the existence of local points is well characterized, but Shimura curves are expected to fail having global points in "many cases".

Modular interpretation and rational points

- Shimura curves are moduli spaces for abelian surfaces whose endomorphism ring contains an order in an indefinite rational quaternion algebra.
  - $\rightsquigarrow$ Studying these abelian surfaces we can describe some properties of Shimura curves.

- Shimura curves have no real points, hence no rational points.
- Over number fields, the existence of local points is well characterized, but Shimura curves are expected to fail having global points in "many cases".
  - $\rightsquigarrow$ Good candidates to counterexamples to the Hasse principle.

Definition

A rational quaternion algebra B is a central simple algebra of rank 4 over $\mathbb{Q}$. There exist $a, b \in \mathbb{Q}^{\times}$ such that

$$B = \left(\frac{a, b}{\mathbb{Q}}\right) := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = a, j^2 = b, ij = -ji.$$

Definition

A rational quaternion algebra B is a central simple algebra of rank 4 over $\mathbb{Q}$. There exist $a, b \in \mathbb{Q}^\times$ such that

$$B = \left(\frac{a, b}{\mathbb{Q}}\right) := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = a, j^2 = b, ij = -ji.$$

Canonical involution: $\beta = x + yi + zj + tij \mapsto \bar{\beta} = x - yi - zj - tij$.
Reduced norm and *reduced trace*: $\mathrm{n}(\beta) = \beta\bar{\beta}$ and $\mathrm{tr}(\beta) = \beta + \bar{\beta}$.

Definition

A rational quaternion algebra B is a central simple algebra of rank 4 over $\mathbb{Q}$. There exist $a, b \in \mathbb{Q}^\times$ such that

$$B = \left(\frac{a, b}{\mathbb{Q}}\right) := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = a, j^2 = b, ij = -ji.$$

Canonical involution: $\beta = x + yi + zj + tij \mapsto \bar{\beta} = x - yi - zj - tij$.
Reduced norm and *reduced trace*: $\mathrm{n}(\beta) = \beta\bar{\beta}$ and $\mathrm{tr}(\beta) = \beta + \bar{\beta}$.

Remark: the same definition applies over any field F, $\mathrm{char}(F) \neq 2$.

Definition

A rational quaternion algebra B is a central simple algebra of rank 4 over $\mathbb{Q}$. There exist $a, b \in \mathbb{Q}^\times$ such that

$$B = \left(\frac{a,b}{\mathbb{Q}}\right) := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = a, j^2 = b, ij = -ji.$$

Canonical involution: $\beta = x + yi + zj + tij \mapsto \bar{\beta} = x - yi - zj - tij$.
Reduced norm and *reduced trace*: $\mathrm{n}(\beta) = \beta\bar{\beta}$ and $\mathrm{tr}(\beta) = \beta + \bar{\beta}$.

Remark: the same definition applies over any field F, $\mathrm{char}(F) \neq 2$.

▷ **Fact:** Either B is a division algebra or $B \simeq \mathrm{M}_2(\mathbb{Q}) \simeq (\frac{1,b}{\mathbb{Q}})$.

Definition

A rational quaternion algebra B is a central simple algebra of rank 4 over $\mathbb{Q}$. There exist $a, b \in \mathbb{Q}^\times$ such that

$$B = \left(\frac{a, b}{\mathbb{Q}}\right) := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = a, j^2 = b, ij = -ji.$$

Canonical involution: $\beta = x + yi + zj + tij \mapsto \bar{\beta} = x - yi - zj - tij$.
Reduced norm and *reduced trace*: $\mathrm{n}(\beta) = \beta\bar{\beta}$ and $\mathrm{tr}(\beta) = \beta + \bar{\beta}$.

Remark: the same definition applies over any field F, $\mathrm{char}(F) \neq 2$.

- **Fact:** Either B is a division algebra or $B \simeq \mathrm{M}_2(\mathbb{Q}) \simeq (\frac{1,b}{\mathbb{Q}})$.
- A field $K/\mathbb{Q}$ is said to *split* B if $B \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$.

Ramified primes determine B

Fact: For any prime $p \leq \infty$, there is only one quaternion division algebra H_p over $\mathbb{Q}_p$. For $\mathbb{Q}_\infty := \mathbb{R}$, $H_\infty = \mathbb{H}$.

Ramified primes determine B

Fact: For any prime $p \leq \infty$, there is only one quaternion division algebra H_p over $\mathbb{Q}_p$. For $\mathbb{Q}_\infty := \mathbb{R}$, $H_\infty = \mathbb{H}$.

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \begin{cases} \mathrm{M}_2(\mathbb{Q}_p) & \leftarrow B \text{ is split at } p, \\ H_p & \leftarrow B \text{ is ramified at } p. \end{cases}$$

For the infinite prime, we also say B is *indefinite* or *definite*, respectively.

Ramified primes determine B

Fact: For any prime $p \leq \infty$, there is only one quaternion division algebra H_p over $\mathbb{Q}_p$. For $\mathbb{Q}_\infty := \mathbb{R}$, $H_\infty = \mathbb{H}$.

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \begin{cases} \mathrm{M}_2(\mathbb{Q}_p) & \leftarrow B \text{ is split at } p, \\ H_p & \leftarrow B \text{ is ramified at } p. \end{cases}$$

For the infinite prime, we also say B is *indefinite* or *definite*, respectively.

Theorem (Hasse)

The set $Ram(B)$ of ramified primes in B has even cardinality, and determines B (up to isom.). Conversely, for any finite set of primes S of even cardinality, there is a unique B (up to isom.) with $S = Ram(B)$.

The reduced discriminant of B is $D = \prod_{p \in S, p < \infty} p$.

Ramified primes determine B

Fact: For any prime $p \leq \infty$, there is only one quaternion division algebra H_p over $\mathbb{Q}_p$. For $\mathbb{Q}_\infty := \mathbb{R}$, $H_\infty = \mathbb{H}$.

$$B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \begin{cases} \mathrm{M}_2(\mathbb{Q}_p) & \leftarrow B \text{ is split at } p, \\ H_p & \leftarrow B \text{ is ramified at } p. \end{cases}$$

For the infinite prime, we also say B is *indefinite* or *definite*, respectively.

Theorem (Hasse)

The set $Ram(B)$ of ramified primes in B has even cardinality, and determines B (up to isom.). Conversely, for any finite set of primes S of even cardinality, there is a unique B (up to isom.) with $S = Ram(B)$.

The reduced discriminant of B is $D = \prod_{p \in S, p < \infty} p$.

- B is a division algebra if and only if $D > 1$.

Orders

Let B be a quaternion algebra over $\mathbb{Q}$. An element $\beta \in B$ is *integral* if $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in \mathbb{Z}$.

Definition

An order $\mathcal{O} \subseteq B$ is a complete $\mathbb{Z}$-lattice which is also a ring. Equivalently, it is a ring of integral elements of B, finitely generated as a $\mathbb{Z}$-module and such that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = B$.

Orders

Let B be a quaternion algebra over $\mathbb{Q}$. An element $\beta \in B$ is *integral* if $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in \mathbb{Z}$.

Definition

An order $\mathcal{O} \subseteq B$ is a complete $\mathbb{Z}$-lattice which is also a ring. Equivalently, it is a ring of integral elements of B, finitely generated as a $\mathbb{Z}$-module and such that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = B$.

- Like in the case of number fields, a theory of orders and ideals can be developed, but now in a non-commutative setting; e.g. we can consider the set of left (right) $\mathcal{O}$-ideals modulo equivalence on the right (left) $\rightsquigarrow$ class groups, class numbers, ...

Orders

Let B be a quaternion algebra over $\mathbb{Q}$. An element $\beta \in B$ is *integral* if $\mathrm{tr}(\beta), \mathrm{n}(\beta) \in \mathbb{Z}$.

Definition

An order *$\mathcal{O} \subseteq B$ is a complete $\mathbb{Z}$-lattice which is also a ring. Equivalently, it is a ring of integral elements of B, finitely generated as a $\mathbb{Z}$-module and such that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = B$.*

- Like in the case of number fields, a theory of orders and ideals can be developed, but now in a non-commutative setting; e.g. we can consider the set of left (right) $\mathcal{O}$-ideals modulo equivalence on the right (left) $\rightsquigarrow$ class groups, class numbers, ...

For our purposes, the following fact is important:

- If B is indefinite, then *all the maximal orders in B are conjugate*.

The Riemann surface V_D

- Let B_D be an indefinite rational quaternion division algebra ($D > 1$). Fix $\psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$ and a maximal order $\mathcal{O}_D \subseteq B_D$.

The Riemann surface V_D

- Let B_D be an indefinite rational quaternion division algebra ($D > 1$). Fix $\psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$ and a maximal order $\mathcal{O}_D \subseteq B_D$.
- Let $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D^\times : \mathrm{n}(\gamma) = 1\}$. The discrete subgroup $\Gamma_D = \psi(\mathcal{O}_D^1) \subseteq \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_D, z \in \mathfrak{H} \longmapsto \gamma z = \frac{az+b}{cz+d} \in \mathfrak{H}.$$

The Riemann surface V_D

- Let B_D be an indefinite rational quaternion division algebra ($D > 1$). Fix $\psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$ and a maximal order $\mathcal{O}_D \subseteq B_D$.
- Let $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D^\times : \mathrm{n}(\gamma) = 1\}$. The discrete subgroup $\Gamma_D = \psi(\mathcal{O}_D^1) \subseteq \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_D, z \in \mathfrak{H} \longmapsto \gamma z = \frac{az+b}{cz+d} \in \mathfrak{H}.$$

- $V_D := \Gamma_D \setminus \mathfrak{H}$ is a compact Riemann surface.

The Riemann surface V_D

- Let B_D be an indefinite rational quaternion division algebra ($D > 1$). Fix $\psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$ and a maximal order $\mathcal{O}_D \subseteq B_D$.
- Let $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D^\times : \mathrm{n}(\gamma) = 1\}$. The discrete subgroup $\Gamma_D = \psi(\mathcal{O}_D^1) \subseteq \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_D, z \in \mathfrak{H} \longmapsto \gamma z = \frac{az+b}{cz+d} \in \mathfrak{H}.$$

- $V_D := \Gamma_D \setminus \mathfrak{H}$ is a compact Riemann surface.
- **Shimura (1967):** There is a smooth projective algebraic curve $X_D/\mathbb{Q}$ such that $X_D(\mathbb{C})^{an} \simeq V_D$.

The Riemann surface V_D

- Let B_D be an indefinite rational quaternion division algebra ($D > 1$). Fix $\psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$ and a maximal order $\mathcal{O}_D \subseteq B_D$.
- Let $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D^\times : \mathrm{n}(\gamma) = 1\}$. The discrete subgroup $\Gamma_D = \psi(\mathcal{O}_D^1) \subseteq \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_D, z \in \mathfrak{H} \longmapsto \gamma z = \frac{az+b}{cz+d} \in \mathfrak{H}.$$

- $V_D := \Gamma_D \setminus \mathfrak{H}$ is a compact Riemann surface.
- **Shimura (1967):** There is a smooth projective algebraic curve $X_D/\mathbb{Q}$ such that $X_D(\mathbb{C})^{an} \simeq V_D$.
  - $\rightsquigarrow$ We call X_D the Shimura curve associated to B_D.

The Riemann surface V_D

- Let B_D be an indefinite rational quaternion division algebra ($D > 1$). Fix $\psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$ and a maximal order $\mathcal{O}_D \subseteq B_D$.
- Let $\mathcal{O}_D^1 = \{\gamma \in \mathcal{O}_D^\times : \mathrm{n}(\gamma) = 1\}$. The discrete subgroup $\Gamma_D = \psi(\mathcal{O}_D^1) \subseteq \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_D, z \in \mathfrak{H} \longmapsto \gamma z = \frac{az+b}{cz+d} \in \mathfrak{H}.$$

- $V_D := \Gamma_D \backslash \mathfrak{H}$ is a compact Riemann surface.
- **Shimura (1967):** There is a smooth projective algebraic curve $X_D/\mathbb{Q}$ such that $X_D(\mathbb{C})^{an} \simeq V_D$.
  - $\rightsquigarrow$ We call X_D the Shimura curve associated to B_D.

Remark: For $B_1 = \mathrm{M}_2(\mathbb{Q})$, $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})$ and we get the (affine) modular curve $Y(1)$.

X_D as a moduli space

Definition

An abelian surface with quaternionic multiplication (QM) by $\mathcal{O}_D$ *is a pair* (A, ι), *where*

- *A is an abelian surface,*
- *$\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ is a monomorphism of rings.*

X_D as a moduli space

Definition

An abelian surface with quaternionic multiplication (QM) by $\mathcal{O}_D$ *is a pair* (A, ι), *where*

- *A is an abelian surface,*
- *$\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ is a monomorphism of rings.*

▷ **Shimura**: X_D is the (coarse) moduli scheme classifying isomorphism classes of pairs (A, ι). Moreover,

$$\Gamma_D \backslash \mathfrak{H} \xrightarrow{\simeq} X_D(\mathbb{C}), \quad z \longmapsto (A_z, \iota_z), \qquad A_z := \mathbb{C}^2/\mathcal{O}_D\begin{pmatrix} z \\ 1 \end{pmatrix}.$$

X_D as a moduli space

Definition

An abelian surface with quaternionic multiplication (QM) by $\mathcal{O}_D$ is a pair (A, ι), where

- *A is an abelian surface,*
- *$\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ is a monomorphism of rings.*

▷ **Shimura**: X_D is the (coarse) moduli scheme classifying isomorphism classes of pairs (A, ι). Moreover,

$$\Gamma_D \backslash \mathfrak{H} \xrightarrow{\simeq} X_D(\mathbb{C}), \quad z \longmapsto (A_z, \iota_z), \qquad A_z := \mathbb{C}^2/\mathcal{O}_D\begin{pmatrix} z \\ 1 \end{pmatrix}.$$

▷ If $K/\mathbb{Q}$ and $P \in X_D(K)$, then
$$P = [(A, \iota)] = \{(A', \iota')/\bar{K} : (A', \iota') \simeq (A, \iota)\}, \text{ for some } (A, \iota)/\bar{K}.$$

Field of moduli vs field of definition

Definition

The field of moduli $K_P = K_{(A,\iota)}$ *of* (A,ι) *is the minimal field extension* K_P/K *such that* ${}^{\sigma}(A,\iota) \simeq (A,\iota)$ *for all* $\sigma \in \mathrm{Gal}(\bar{K}/K_P)$. *And* L/K *is* a field of definition *for* (A,ι) *if there exists* $(A',\iota')/L$ *with* $(A',\iota') \times \bar{K} \simeq (A,\iota)$. *In this case we say* (A',ι') *is a model of* (A,ι) *rational over* L.

Field of moduli vs field of definition

Definition

The field of moduli $K_P = K_{(A,\iota)}$ *of* (A,ι) *is the minimal field extension* K_P/K *such that* ${}^{\sigma}(A,\iota) \simeq (A,\iota)$ *for all* $\sigma \in \mathrm{Gal}(\bar{K}/K_P)$. *And* L/K *is* a field of definition *for* (A,ι) *if there exists* $(A',\iota')/L$ *with* $(A',\iota') \times \bar{K} \simeq (A,\iota)$. *In this case we say* (A',ι') *is a model of* (A,ι) *rational over* L.

Then the set $X_D(K)$ of K-rational points is

$$X_D(K) = \{P \in X_D(\bar{K}) : K_P \subseteq K\}.$$

Field of moduli vs field of definition

Definition

The field of moduli $K_P = K_{(A,\iota)}$ *of* (A, ι) *is the minimal field extension* K_P/K *such that* ${}^{\sigma}(A, \iota) \simeq (A, \iota)$ *for all* $\sigma \in \mathrm{Gal}\,(\bar{K}/K_P)$*. And* L/K *is* a field of definition *for* (A, ι) *if there exists* $(A', \iota')/L$ *with* $(A', \iota') \times \bar{K} \simeq (A, \iota)$*. In this case we say* (A', ι') *is a model of* (A, ι) *rational over* L*.*

Then the set $X_D(K)$ of K-rational points is

$$X_D(K) = \{P \in X_D(\bar{K}) : K_P \subseteq K\}.$$

- But it may happen that the pairs (A, ι) representing $P \in X_D(K)$ do not admit a model rational over K, i.e. K_P is not necessarily a field of definition.

Jordan's result

Theorem (Jordan, 1986)

Let $P = [(A, \iota)] \in X_D(K)$. Then (A, ι) admits a model rational over K if and only if $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$.

Jordan's result

Theorem (Jordan, 1986)

Let $P = [(A, \iota)] \in X_D(K)$. Then (A, ι) admits a model rational over K if and only if $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$.

Remark: The condition does not depend on P !

Jordan's result

Theorem (Jordan, 1986)

Let $P = [(A, \iota)] \in X_D(K)$. Then (A, ι) admits a model rational over K if and only if $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$.

Remark: The condition does not depend on P !

Example ($D = 6$)

$B_6 \simeq \left(\frac{-6,2}{\mathbb{Q}}\right) \simeq \left(\frac{-6,3}{\mathbb{Q}}\right)$. An (affine) equation for $X_6/\mathbb{Q}$ is due to Kurihara:

$$x^2 + y^2 + 3 = 0.$$

$P = (\sqrt{-7}, 2) \in X_6(\mathbb{Q}(\sqrt{-7}))$, but there is no $(A, \iota)/\mathbb{Q}(\sqrt{-7})$ representing P, because $B_6 \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-7}) \not\simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-7}))$.

Previous results concerning rational points

Let B_D be an indefinite rational quaternion division algebra ($D > 1$), and let $X_D/\mathbb{Q}$ be the associated Shimura curve.

Previous results concerning rational points

Let B_D be an indefinite rational quaternion division algebra ($D > 1$), and let $X_D/\mathbb{Q}$ be the associated Shimura curve.

- **Shimura, 1975:** $X_D(\mathbb{R}) = \emptyset$. In particular, $X_D(\mathbb{Q}) = \emptyset$.

Previous results concerning rational points

Let B_D be an indefinite rational quaternion division algebra ($D > 1$), and let $X_D/\mathbb{Q}$ be the associated Shimura curve.

- **Shimura, 1975:** $X_D(\mathbb{R}) = \emptyset$. In particular, $X_D(\mathbb{Q}) = \emptyset$.
- **Jordan-Livné, 1985:** Local points on X_D: criteria for the non-emptiness of $X_D(L)$, for $L/\mathbb{Q}_p$ finite.

Previous results concerning rational points

Let B_D be an indefinite rational quaternion division algebra ($D > 1$), and let $X_D/\mathbb{Q}$ be the associated Shimura curve.

- **Shimura, 1975:** $X_D(\mathbb{R}) = \emptyset$. In particular, $X_D(\mathbb{Q}) = \emptyset$.
- **Jordan-Livné, 1985:** Local points on X_D: criteria for the non-emptiness of $X_D(L)$, for $L/\mathbb{Q}_p$ finite.
- **Jordan, 1986:** Explicit sufficient conditions for $X_D(K) = \emptyset$, with K imaginary quadratic.

Previous results concerning rational points

Let B_D be an indefinite rational quaternion division algebra ($D > 1$), and let $X_D/\mathbb{Q}$ be the associated Shimura curve.

- ▷ **Shimura, 1975:** $X_D(\mathbb{R}) = \emptyset$. In particular, $X_D(\mathbb{Q}) = \emptyset$.
- ▷ **Jordan-Livné, 1985:** Local points on X_D: criteria for the non-emptiness of $X_D(L)$, for $L/\mathbb{Q}_p$ finite.
- ▷ **Jordan, 1986:** Explicit sufficient conditions for $X_D(K) = \emptyset$, with K imaginary quadratic.
- ▷ **Skorobogatov, 2005:** The examples given by Jordan's work are accounted for by the Brauer-Manin obstruction.

Previous results concerning rational points

Let B_D be an indefinite rational quaternion division algebra ($D > 1$), and let $X_D/\mathbb{Q}$ be the associated Shimura curve.

- ▷ **Shimura, 1975:** $X_D(\mathbb{R}) = \emptyset$. In particular, $X_D(\mathbb{Q}) = \emptyset$.
- ▷ **Jordan-Livné, 1985:** Local points on X_D: criteria for the non-emptiness of $X_D(L)$, for $L/\mathbb{Q}_p$ finite.
- ▷ **Jordan, 1986:** Explicit sufficient conditions for $X_D(K) = \emptyset$, with K imaginary quadratic.
- ▷ **Skorobogatov, 2005:** The examples given by Jordan's work are accounted for by the Brauer-Manin obstruction.

$\rightsquigarrow$ Jordan & Skorobogatov use the moduli interpretation of X_D, studying the Galois representations attached to the pairs (A, ι).

Galois representations attached to (A, ι) (I)

Assume $(A, \iota)/K$, and let p be a prime.

- The p^n-torsion subgroups of A form a projective limit, the p-adic Tate module $T_p(A) = \varprojlim A[p^n]$ of A. It is a free $\mathbb{Z}_p$-module of rank 4.

Galois representations attached to (A, ι) (I)

Assume $(A, \iota)/K$, and let p be a prime.

- The p^n-torsion subgroups of A form a projective limit, the p-adic Tate module $T_p(A) = \varprojlim A[p^n]$ of A. It is a free $\mathbb{Z}_p$-module of rank 4.
- $\mathrm{Gal}\,(\bar{K}/K)$ acts on $T_p(A) = \varprojlim A[p^n]$, and gives rise to a Galois representation

  $$\rho_{(A,\iota),p} : \mathrm{Gal}\,(\bar{K}/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \subseteq (B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times,$$

  where $(B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times \subseteq \mathrm{GL}_2(L_p)$, with $L_p/\mathbb{Q}_p$ the unique unramified quadratic extension.

Galois representations attached to (A, ι) (I)

Assume $(A,\iota)/K$, and let p be a prime.

- The p^n-torsion subgroups of A form a projective limit, the p-adic Tate module $T_p(A) = \varprojlim A[p^n]$ of A. It is a free $\mathbb{Z}_p$-module of rank 4.
- $\mathrm{Gal}(\bar{K}/K)$ acts on $T_p(A) = \varprojlim A[p^n]$, and gives rise to a Galois representation

$$\rho_{(A,\iota),p} : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \subseteq (B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times,$$

  where $(B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times \subseteq \mathrm{GL}_2(L_p)$, with $L_p/\mathbb{Q}_p$ the unique unramified quadratic extension.
- By reducing modulo p, we get the action on $A[p]$:

$$\bar{\rho}_{(A,\iota),p} : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A[p]) \simeq (\mathcal{O}_D/p\mathcal{O}_D)^\times \subseteq \mathrm{GL}_2(\mathbb{F}_{p^2}).$$

Galois representations attached to (A, ι) (II)

We assume now that $p \mid D$.

- There exists a unique $\mathcal{O}_D$-submodule C_p of $A[p]$. If $I(p)$ is the unique $\mathcal{O}_D$-ideal of norm p, then

$$C_p = A[I(p)] = \{x \in A : \iota(\beta)(x) = 0 \ \forall \beta \in I(p)\} \simeq \mathcal{O}_D / I(p) \simeq \mathbb{F}_{p^2}.$$

Galois representations attached to (A, ι) (II)

We assume now that $p \mid D$.

- There exists a unique $\mathcal{O}_D$-submodule C_p of $A[p]$. If $I(p)$ is the unique $\mathcal{O}_D$-ideal of norm p, then

$$C_p = A[I(p)] = \{x \in A : \iota(\beta)(x) = 0 \ \forall \beta \in I(p)\} \simeq \mathcal{O}_D / I(p) \simeq \mathbb{F}_{p^2}.$$

- $\mathrm{Gal}\,(\bar{K}/K)$ acts on C_p, and yields a representation

$$\alpha_{(A,\iota),p} : \mathrm{Gal}\,(\bar{K}/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times},$$

which is a subrepresentation of $\bar{\rho}_{(A,\iota),p}$.

Galois representations attached to (A, ι) (II)

We assume now that $p \mid D$.

- There exists a unique $\mathcal{O}_D$-submodule C_p of $A[p]$. If $I(p)$ is the unique $\mathcal{O}_D$-ideal of norm p, then

$$C_p = A[I(p)] = \{x \in A : \iota(\beta)(x) = 0 \ \forall \beta \in I(p)\} \simeq \mathcal{O}_D/I(p) \simeq \mathbb{F}_{p^2}.$$

- $\mathrm{Gal}\,(\bar{K}/K)$ acts on C_p, and yields a representation

$$\alpha_{(A,\iota),p} : \mathrm{Gal}\,(\bar{K}/K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^{\times},$$

  which is a subrepresentation of $\bar{\rho}_{(A,\iota),p}$.

$\rightsquigarrow$ By studying these representations with K imaginary quadratic, Jordan found explicit conditions on B_D and K that imply $X_D(K) = \emptyset$.

$X_D(K)$ with K imaginary quadratic

Let q be a prime. Define $\mathcal{P}(q)$ as the (finite) set of prime factors of the non-zero integers in

$$\{a, a \pm q, a \pm 2q, a^2 - 3q^2\}_{|a| \leq 2q}.$$

$X_D(K)$ with K imaginary quadratic

Let q be a prime. Define $\mathcal{P}(q)$ as the (finite) set of prime factors of the non-zero integers in

$$\{a, a \pm q, a \pm 2q, a^2 - 3q^2\}_{|a| \leq 2q}.$$

Let also

$$\mathcal{B}(q) = \{\text{indef. } B_D : B_D \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))\} \ (q \neq 2),$$
$$\mathcal{B}(2) = \{\text{indef. } B_D : B_D \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-d}) \not\simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-d})), d = 1, 2\}.$$

$X_D(K)$ with K imaginary quadratic

Let q be a prime. Define $\mathcal{P}(q)$ as the (finite) set of prime factors of the non-zero integers in

$$\{a, a \pm q, a \pm 2q, a^2 - 3q^2\}_{|a| \leq 2q}.$$

Let also

$$\mathcal{B}(q) = \{\text{indef. } B_D : B_D \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))\} \; (q \neq 2),$$
$$\mathcal{B}(2) = \{\text{indef. } B_D : B_D \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-d}) \not\simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-d})), d = 1, 2\}.$$

Theorem (Jordan, 1986)

Assume $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$ with K imaginary quadratic, and let q be a prime ramifying in K. If $B_D \in \mathcal{B}(q)$ and there is a prime $p \mid D$, $p \notin \mathcal{P}(q)$, then $X_D(K) = \emptyset$.

Counterexamples to the Hasse principle

Example ($D = 39$)

B_{39} is split by $K = \mathbb{Q}(\sqrt{-13})$, but not by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$; $q = 2$ is ramified in K and $p = 13 \notin \mathcal{P}(2)$. Then $X_{39}(K) = \emptyset$.
But one can check that $X_{39}(K_v) \neq \emptyset$ for every place v of K.

Counterexamples to the Hasse principle

Example ($D = 39$)

B_{39} is split by $K = \mathbb{Q}(\sqrt{-13})$, but not by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$; $q = 2$ is ramified in K and $p = 13 \notin \mathcal{P}(2)$. Then $X_{39}(K) = \emptyset$.
But one can check that $X_{39}(K_v) \neq \emptyset$ for every place v of K.

Given a projective algebraic curve X defined over a global field K, clearly

$$X(K) \neq \emptyset \Rightarrow X(K_v) \neq \emptyset \text{ for every place } v \text{ of } K.$$

If the converse holds, we say that the Hasse principle over K holds for X. Otherwise, X is said to be a *counterexample to the Hasse principle over K*.

Counterexamples to the Hasse principle

Example ($D = 39$)

B_{39} is split by $K = \mathbb{Q}(\sqrt{-13})$, but not by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$; $q = 2$ is ramified in K and $p = 13 \notin \mathcal{P}(2)$. Then $X_{39}(K) = \emptyset$.
But one can check that $X_{39}(K_v) \neq \emptyset$ for every place v of K.

Given a projective algebraic curve X defined over a global field K, clearly

$$X(K) \neq \emptyset \Rightarrow X(K_v) \neq \emptyset \text{ for every place } v \text{ of } K.$$

If the converse holds, we say that the Hasse principle over K holds for X. Otherwise, X is said to be a *counterexample to the Hasse principle over K*.

- Jordan's theorem (combined with Jordan-Livné (1985)) provides several counterexamples to the Hasse principle over imaginary quadratic fields.

Exceptional pairs and the hypothesis $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$

- It is expected that $X_D(K) = \emptyset$ for $D, \mathrm{disc}(K) \gg 0$, so the hypothesis $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$ does not seem "natural".

Exceptional pairs and the hypothesis $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$

- It is expected that $X_D(K) = \emptyset$ for $D, \mathrm{disc}(K) \gg 0$, so the hypothesis $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$ does not seem "natural".
- Jordan calls a pair (B_D, K) exceptional if $B_D \otimes_{\mathbb{Q}} K \not\simeq \mathrm{M}_2(K)$, $X_D(K) = \emptyset$ but $X_D(K_v) \neq \emptyset$ for every place v of K. His theorem cannot cover these counterexamples to the Hasse principle.

Exceptional pairs and the hypothesis $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$

- It is expected that $X_D(K) = \emptyset$ for $D, \mathrm{disc}(K) \gg 0$, so the hypothesis $B_D \otimes_{\mathbb{Q}} K \simeq \mathrm{M}_2(K)$ does not seem "natural".
- Jordan calls a pair (B_D, K) exceptional if $B_D \otimes_{\mathbb{Q}} K \not\simeq \mathrm{M}_2(K)$, $X_D(K) = \emptyset$ but $X_D(K_v) \neq \emptyset$ for every place v of K. His theorem cannot cover these counterexamples to the Hasse principle.

In joint work with V. Rotger, we can avoid this hypothesis.

$\rightsquigarrow$ We attach analogous Galois representations to the points $P \in X_D(K)$ rather than to the pairs (A, ι), following an idea of Ellenberg and Skinner for elliptic $\mathbb{Q}$-curves.

$X_D(K)$ with K imaginary quadratic (again)

For any prime q, we define a finite set of primes $\mathcal{P}'(q)$ similar to $\mathcal{P}(q)$. Consider also the same family $\mathcal{B}(q)$ of quaternion algebras.

Theorem (de V. - Rotger)

Let $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field, and q a prime ramifying in K. If $B_D \in \mathcal{B}(q)$ and there is a prime $p \mid D$ not split in K, $p \notin \mathcal{P}'(q)$, then $X_D(K) = \emptyset$.

$X_D(K)$ with K imaginary quadratic (again)

For any prime q, we define a finite set of primes $\mathcal{P}'(q)$ similar to $\mathcal{P}(q)$. Consider also the same family $\mathcal{B}(q)$ of quaternion algebras.

Theorem (de V. - Rotger)

Let $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field, and q a prime ramifying in K. If $B_D \in \mathcal{B}(q)$ and there is a prime $p \mid D$ not split in K, $p \notin \mathcal{P}'(q)$, then $X_D(K) = \emptyset$.

- Actually, we can prove that $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

$X_D(K)$ with K imaginary quadratic (again)

For any prime q, we define a finite set of primes $\mathcal{P}'(q)$ similar to $\mathcal{P}(q)$. Consider also the same family $\mathcal{B}(q)$ of quaternion algebras.

Theorem (de V. - Rotger)

Let $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field, and q a prime ramifying in K. If $B_D \in \mathcal{B}(q)$ and there is a prime $p \mid D$ not split in K, $p \notin \mathcal{P}'(q)$, then $X_D(K) = \emptyset$.

- Actually, we can prove that $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.
- For $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, $X_D(K)$ contains only CM points.

Some exceptional pairs

Combining the previous theorem with Jordan-Livné (1985), we can produce several exceptional pairs:

$D = 2 \cdot p$	K
$2 \cdot 23$	$\mathbb{Q}(\sqrt{-55})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-119})$, ...
$2 \cdot 31$	$\mathbb{Q}(\sqrt{-39})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, ...
$2 \cdot 43$	$\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-95})$, $\mathbb{Q}(\sqrt{-111})$, ...
$2 \cdot 59$	$\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-119})$, ...
$2 \cdot 67$	$\mathbb{Q}(\sqrt{-55})$, ...
$2 \cdot 71$	$\mathbb{Q}(\sqrt{-119})$, $\mathbb{Q}(\sqrt{-143})$, ...
$2 \cdot 79$	$\mathbb{Q}(\sqrt{-87})$, $\mathbb{Q}(\sqrt{-111})$, $\mathbb{Q}(\sqrt{-159})$, ...

For all the pairs (D, K) in the table, $B_D \otimes_{\mathbb{Q}} K \not\simeq \mathrm{M}_2(K)$ and X_D is a counterexample to the Hasse principle over K.

Final comments

- X_D is supplied with a group $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$ of involutions ω_m, indexed by the positive divisors m of D: the Atkin-Lehner involutions.

Final comments

- X_D is supplied with a group $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$ of involutions ω_m, indexed by the positive divisors m of D: the Atkin-Lehner involutions.
- Although $X_D(\mathbb{Q}) = \emptyset$, it can be $X_D/\langle\omega_m\rangle(\mathbb{Q}) \neq \emptyset$.

Final comments

- X_D is supplied with a group $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$ of involutions ω_m, indexed by the positive divisors m of D: the Atkin-Lehner involutions.
- Although $X_D(\mathbb{Q}) = \emptyset$, it can be $X_D/\langle\omega_m\rangle(\mathbb{Q}) \neq \emptyset$.
- Using the same ideas, we find explicit sufficient conditions for $X_D/\langle\omega_m\rangle(\mathbb{Q}) = \emptyset$, and using a criterion for the existence of local points due to Rotger-Skorobogatov-Yafaev (2005) we can provide several counterexamples to the Hasse principle over $\mathbb{Q}$.

Final comments

- X_D is supplied with a group $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$ of involutions ω_m, indexed by the positive divisors m of D: the Atkin-Lehner involutions.
- Although $X_D(\mathbb{Q}) = \emptyset$, it can be $X_D/\langle\omega_m\rangle(\mathbb{Q}) \neq \emptyset$.
- Using the same ideas, we find explicit sufficient conditions for $X_D/\langle\omega_m\rangle(\mathbb{Q}) = \emptyset$, and using a criterion for the existence of local points due to Rotger-Skorobogatov-Yafaev (2005) we can provide several counterexamples to the Hasse principle over $\mathbb{Q}$.

- We can attach Galois representations to points in more general moduli spaces for abelian varieties, and hope they can be used to study rational points over number fields.

Thank you for your attention!