Brauer-Manin obstructions on K3 surfaces and Ш for genus-2 Jacobians

Patrick Corn

St. Mary's College of Maryland

January 7, 2009

Introduction

Let C be a genus-2 curve over a number field k, and let J be its Jacobian.

Introduction

Let C be a genus-2 curve over a number field k, and let J be its Jacobian.

General goal: Compute the (finite) set $C(k)$.

Introduction

Let C be a genus-2 curve over a number field k, and let J be its Jacobian.

General goal: Compute the (finite) set $C(k)$.
General idea: Understand $J(k)$ instead; use the embedding $C \hookrightarrow J$.

Introduction

Let C be a genus-2 curve over a number field k, and let J be its Jacobian.

General goal: Compute the (finite) set $C(k)$.
General idea: Understand $J(k)$ instead; use the embedding $C \hookrightarrow J$.

Various methods use this general idea (Chabauty-Coleman, Mordell-Weil sieve, covering techniques). We will focus here on the computation of $J(k)$.

Introduction

Let C be a genus-2 curve over a number field k, and let J be its Jacobian.

General goal: Compute the (finite) set $C(k)$.
General idea: Understand $J(k)$ instead; use the embedding $C \hookrightarrow J$.

Various methods use this general idea (Chabauty-Coleman, Mordell-Weil sieve, covering techniques). We will focus here on the computation of $J(k)$.

In particular, $J(k)$ is a finitely generated abelian group of some rank r. What can we say about r?

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to Ш(k, J)[2] \to 0$$

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to \text{Ш}(k, J)[2] \to 0$$

Here $\mathrm{Sel}^{(2)}(J/k)$ has the following properties:

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to \text{Ш}(k, J)[2] \to 0$$

Here $\mathrm{Sel}^{(2)}(J/k)$ has the following properties:

- It is the subgroup of $H^1(k, J[2])$ consisting of classes which restrict to zero in $H^1(k_v, J[2])$, for all places v of k

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to Ш(k, J)[2] \to 0$$

Here $\mathrm{Sel}^{(2)}(J/k)$ has the following properties:

- It is the subgroup of $H^1(k, J[2])$ consisting of classes which restrict to zero in $H^1(k_v, J[2])$, for all places v of k
- Its elements can be represented as 2-coverings of J with points everywhere locally

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to Ш(k, J)[2] \to 0$$

Here $\mathrm{Sel}^{(2)}(J/k)$ has the following properties:

- It is the subgroup of $H^1(k, J[2])$ consisting of classes which restrict to zero in $H^1(k_v, J[2])$, for all places v of k
- Its elements can be represented as 2-coverings of J with points everywhere locally
- It is finite, and effectively computable (Stoll–implementation in MAGMA).

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to Ш(k, J)[2] \to 0$$

Here $\mathrm{Sel}^{(2)}(J/k)$ has the following properties:

- It is the subgroup of $H^1(k, J[2])$ consisting of classes which restrict to zero in $H^1(k_v, J[2])$, for all places v of k
- Its elements can be represented as 2-coverings of J with points everywhere locally
- It is finite, and effectively computable (Stoll–implementation in MAGMA).

The Tate-Shafarevich group $Ш(k, J)$ has the following properties:

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to Ш(k, J)[2] \to 0$$

Here $\mathrm{Sel}^{(2)}(J/k)$ has the following properties:

- It is the subgroup of $H^1(k, J[2])$ consisting of classes which restrict to zero in $H^1(k_v, J[2])$, for all places v of k
- Its elements can be represented as 2-coverings of J with points everywhere locally
- It is finite, and effectively computable (Stoll–implementation in MAGMA).

The Tate-Shafarevich group $Ш(k, J)$ has the following properties:

- It is the subgroup of $H^1(k, J)$ consisting of classes which restrict to zero in $H^1(k_v, J)$, for all places v of k

Fundamental exact sequence

$$0 \to J(k)/2J(k) \to \mathrm{Sel}^{(2)}(J/k) \to Ш(k, J)[2] \to 0$$

Here $\mathrm{Sel}^{(2)}(J/k)$ has the following properties:

- It is the subgroup of $H^1(k, J[2])$ consisting of classes which restrict to zero in $H^1(k_v, J[2])$, for all places v of k
- Its elements can be represented as 2-coverings of J with points everywhere locally
- It is finite, and effectively computable (Stoll–implementation in MAGMA).

The Tate-Shafarevich group $Ш(k, J)$ has the following properties:

- It is the subgroup of $H^1(k, J)$ consisting of classes which restrict to zero in $H^1(k_v, J)$, for all places v of k
- An element of $Ш(k, J)$ represented by a principal homogeneous space X of J is trivial if and only if X has a k-rational point

The Kummer surface

Our goal is to exhibit examples of C and J such that $Ш(\mathbb{Q}, J)[2]$ is nonzero.

The Kummer surface

Our goal is to exhibit examples of C and J such that $\text{Ш}(\mathbb{Q}, J)[2]$ is nonzero.

Idea: Find an explicit 2-covering X of J with points everywhere locally but no k-rational points. ("The Hasse principle fails.")

The Kummer surface

Our goal is to exhibit examples of C and J such that $\text{Ш}(\mathbb{Q}, J)[2]$ is nonzero.

Idea: Find an explicit 2-covering X of J with points everywhere locally but no k-rational points. ("The Hasse principle fails.")
Problem: The best-known explicit description of X is as the intersection of 72 quadric hypersurfaces in $\mathbb{P}^{15}$!

The Kummer surface

Our goal is to exhibit examples of C and J such that $Ш(\mathbb{Q}, J)[2]$ is nonzero.

Idea: Find an explicit 2-covering X of J with points everywhere locally but no k-rational points. ("The Hasse principle fails.")
Problem: The best-known explicit description of X is as the intersection of 72 quadric hypersurfaces in $\mathbb{P}^{15}$!

Better idea: (Logan, van Luijk) Look instead at the desingularization V of the quotient X/ι, where ι corresponds to $[-1]$ on J.
This is a Kummer K3 surface, which can be written down explicitly as the smooth intersection of three quadrics in $\mathbb{P}^5$.
If there are no points on V, then there are no points on X.

Brauer-Manin obstruction

But how do we find counterexamples to the Hasse principle?

Brauer-Manin obstruction

But how do we find counterexamples to the Hasse principle?
Idea: (Manin, 1971) Use the Brauer group $\mathrm{Br}\, V$, together with the following exact sequence from local class field theory:

$$0 \to \mathrm{Br}\, k \to \oplus_v \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z} \to 0 \tag{1}$$

(The right map comes from maps $\mathrm{inv}_v \colon \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z}$.) Elements of $\mathrm{Br}\, V$ are equivalence classes of *Azumaya algebras* (generalizations of central simple algebras).

Brauer-Manin obstruction

But how do we find counterexamples to the Hasse principle?
Idea: (Manin, 1971) Use the Brauer group $\mathrm{Br}\, V$, together with the following exact sequence from local class field theory:

$$0 \to \mathrm{Br}\, k \to \oplus_v \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z} \to 0 \tag{1}$$

(The right map comes from maps $\mathrm{inv}_v \colon \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z}$.) Elements of $\mathrm{Br}\, V$ are equivalence classes of *Azumaya algebras* (generalizations of central simple algebras).
By functoriality, every point $x_v \in V(k_v)$ gives an evaluation map $\mathrm{Br}\, V \to \mathrm{Br}\, k_v$ sending an algebra $\mathcal{A}$ to some algebra $\mathcal{A}(x_v)$.

Brauer-Manin obstruction

But how do we find counterexamples to the Hasse principle?
Idea: (Manin, 1971) Use the Brauer group $\mathrm{Br}\, V$, together with the following exact sequence from local class field theory:

$$0 \to \mathrm{Br}\, k \to \oplus_v \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z} \to 0 \qquad (1)$$

(The right map comes from maps $\mathrm{inv}_v \colon \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z}$.) Elements of $\mathrm{Br}\, V$ are equivalence classes of *Azumaya algebras* (generalizations of central simple algebras).
By functoriality, every point $x_v \in V(k_v)$ gives an evaluation map $\mathrm{Br}\, V \to \mathrm{Br}\, k_v$ sending an algebra $\mathcal{A}$ to some algebra $\mathcal{A}(x_v)$.
Let $V(\mathbb{A}_k) = \prod_v V(k_v)$. Consider the set

$$V(\mathbb{A}_k)^{\mathrm{Br}} := \{(x_v) \in V(\mathbb{A}_k) | \sum_v \mathrm{inv}_v \mathcal{A}(x_v) = 0 \text{ for all } \mathcal{A} \in \mathrm{Br}\, V\}.$$

Brauer-Manin obstruction

But how do we find counterexamples to the Hasse principle?

Idea: (Manin, 1971) Use the Brauer group $\mathrm{Br}\, V$, together with the following exact sequence from local class field theory:

$$0 \to \mathrm{Br}\, k \to \oplus_v \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z} \to 0 \tag{1}$$

(The right map comes from maps $\mathrm{inv}_v \colon \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z}$.) Elements of $\mathrm{Br}\, V$ are equivalence classes of *Azumaya algebras* (generalizations of central simple algebras).

By functoriality, every point $x_v \in V(k_v)$ gives an evaluation map $\mathrm{Br}\, V \to \mathrm{Br}\, k_v$ sending an algebra $\mathcal{A}$ to some algebra $\mathcal{A}(x_v)$.

Let $V(\mathbb{A}_k) = \prod_v V(k_v)$. Consider the set

$$V(\mathbb{A}_k)^{\mathrm{Br}} := \{(x_v) \in V(\mathbb{A}_k) | \sum_v \mathrm{inv}_v \mathcal{A}(x_v) = 0 \text{ for all } \mathcal{A} \in \mathrm{Br}\, V\}.$$

Then the exactness of (1) implies that

$$V(k) \subseteq V(\mathbb{A}_k)^{\mathrm{Br}} \subseteq V(\mathbb{A}_k).$$

Constructing Azumaya algebras

Since V has points everywhere locally, the natural map $\mathrm{Br}\, k \to \mathrm{Br}\, V$ is injective. The following key isomorphism is fundamental in the construction of explicit Azumaya algebras:

$$\phi\colon \frac{\mathrm{Br}\, V}{\mathrm{Br}\, k} \to H^1(k, \mathrm{Pic}\, \overline{V})$$

Constructing Azumaya algebras

Since V has points everywhere locally, the natural map $\mathrm{Br}\, k \to \mathrm{Br}\, V$ is injective. The following key isomorphism is fundamental in the construction of explicit Azumaya algebras:

$$\phi\colon \frac{\mathrm{Br}\, V}{\mathrm{Br}\, k} \to H^1(k, \mathrm{Pic}\, \overline{V})$$

In principle, we can construct elements on the left side if we can understand the right side. But there is the added difficulty that ϕ is not particularly explicit and can be difficult to invert (it is only surjective because $H^3(k, \overline{k}^*) = 0$).

Constructing Azumaya algebras

Since V has points everywhere locally, the natural map $\mathrm{Br}\, k \to \mathrm{Br}\, V$ is injective. The following key isomorphism is fundamental in the construction of explicit Azumaya algebras:

$$\phi\colon \frac{\mathrm{Br}\, V}{\mathrm{Br}\, k} \to H^1(k, \mathrm{Pic}\, \overline{V})$$

In principle, we can construct elements on the left side if we can understand the right side. But there is the added difficulty that ϕ is not particularly explicit and can be difficult to invert (it is only surjective because $H^3(k, \overline{k}^*) = 0$).

As an abelian group, $\mathrm{Pic} \overline{V} \cong \mathbb{Z}^\rho$ for some ρ. Inflation-restriction shows that

$$H^1(k, \mathrm{Pic}\, \overline{V}) \cong H^1(G, \mathbb{Z}^\rho),$$

where G is the Galois group of the field of definition of the divisor classes generating $\mathrm{Pic}\, \overline{V}$.

The geometry of V

Proposition

(Logan, van Luijk) Generically $\rho = 17$, and G is the semi-direct product of $(\mathbb{Z}/2)^6/\langle(1,1,1,1,1,1)\rangle$ with S_6 (with the natural action of S_6 on $(\mathbb{Z}/2)^6$).

The geometry of V

Proposition

(Logan, van Luijk) Generically $\rho = 17$, and G is the semi-direct product of $(\mathbb{Z}/2)^6/\langle(1,1,1,1,1,1)\rangle$ with S_6 (with the natural action of S_6 on $(\mathbb{Z}/2)^6$).

(The curve C has the equation $y^2 = f(x)$, where $f(x)$ is a sextic; the subgroup of S_6 in G corresponds to the Galois group of f.)

The geometry of V

Proposition

(Logan, van Luijk) Generically $\rho = 17$, and G is the semi-direct product of $(\mathbb{Z}/2)^6/\langle(1,1,1,1,1,1)\rangle$ with S_6 (with the natural action of S_6 on $(\mathbb{Z}/2)^6$).

(The curve C has the equation $y^2 = f(x)$, where $f(x)$ is a sextic; the subgroup of S_6 in G corresponds to the Galois group of f.)
We can analyze subgroups H of G using MAGMA to try to discover (non-generic) examples of nontrivial elements in $H^1(H, \mathbb{Z}^{17})$. Then we construct examples of V such that the Galois group of the generating set of $\mathrm{Pic}\,\overline{V}$ is H.

The geometry of V

Proposition

(Logan, van Luijk) Generically $\rho = 17$, and G is the semi-direct product of $(\mathbb{Z}/2)^6/\langle(1,1,1,1,1,1)\rangle$ with S_6 (with the natural action of S_6 on $(\mathbb{Z}/2)^6$).

(The curve C has the equation $y^2 = f(x)$, where $f(x)$ is a sextic; the subgroup of S_6 in G corresponds to the Galois group of f.)

We can analyze subgroups H of G using MAGMA to try to discover (non-generic) examples of nontrivial elements in $H^1(H, \mathbb{Z}^{17})$. Then we construct examples of V such that the Galois group of the generating set of $\operatorname{Pic} \overline{V}$ is H.

Logan and van Luijk find a certain subgroup H of order 32 in G such that the corresponding V has an elliptic fibration, and use that fibration to construct explicit Azumaya algebras corresponding to nontrivial elements of $H^1(H, \operatorname{Pic} \overline{V})$.

The geometry of V

Proposition

(Logan, van Luijk) Generically $\rho = 17$, and G is the semi-direct product of $(\mathbb{Z}/2)^6/\langle(1,1,1,1,1,1)\rangle$ with S_6 (with the natural action of S_6 on $(\mathbb{Z}/2)^6$).

(The curve C has the equation $y^2 = f(x)$, where $f(x)$ is a sextic; the subgroup of S_6 in G corresponds to the Galois group of f.)

We can analyze subgroups H of G using MAGMA to try to discover (non-generic) examples of nontrivial elements in $H^1(H, \mathbb{Z}^{17})$. Then we construct examples of V such that the Galois group of the generating set of $\operatorname{Pic} \overline{V}$ is H.

Logan and van Luijk find a certain subgroup H of order 32 in G such that the corresponding V has an elliptic fibration, and use that fibration to construct explicit Azumaya algebras corresponding to nontrivial elements of $H^1(H, \operatorname{Pic} \overline{V})$.

Our method; the main result

We search G and find a subgroup H of order 96 such that, given a corresponding V, we can construct a *quaternion algebra* giving rise to nonconstant elements of Br V.

Our method; the main result

We search G and find a subgroup H of order 96 such that, given a corresponding V, we can construct a *quaternion algebra* giving rise to nonconstant elements of Br V.

After a lengthy computer search and involved invariant computations, we obtain our main result:

Theorem

Let C be the genus-2 curve $y^2 = (x^2 - 5x + 1)(x^3 - 7x + 10)(x + 1)$. Then $\text{Ш}(\mathbb{Q}, \mathrm{Jac}(C))[2] \neq 0$.

In fact, we find infinitely many quadratic twists of C with the same property. The three quadrics in $\mathbb{P}^5$ cutting out the associated K3 surface V are available upon request

Our method; the main result

We search G and find a subgroup H of order 96 such that, given a corresponding V, we can construct a *quaternion algebra* giving rise to nonconstant elements of Br V.

After a lengthy computer search and involved invariant computations, we obtain our main result:

Theorem

Let C be the genus-2 curve $y^2 = (x^2 - 5x + 1)(x^3 - 7x + 10)(x + 1)$. Then $\text{Ш}(\mathbb{Q}, \mathrm{Jac}(C))[2] \neq 0$.

In fact, we find infinitely many quadratic twists of C with the same property. The three quadrics in $\mathbb{P}^5$ cutting out the associated K3 surface V are available upon request (but the equations are too large to fit in the margin of this slide).