Experiments with the transcendental Brauer-Manin obstruction

Jörg Jahnel

University of Siegen

Intense collaboration workshop on
Rational points

MSRI, Berkeley
October 12, 2012

joint work with
Andreas-Stephan Elsenhans (University of Bayreuth)

A Diophantine equation

Example

Consider the Diophantine equation

$$z^2 = x(x-1)(x-25)u(u+25)(u+36)\,.$$

A Diophantine equation

Example

Consider the Diophantine equation

$$z^2 = x(x-1)(x-25)u(u+25)(u+36)\,.$$

Trivial solutions: $x \in \{0, 1, 25\}$ or $u \in \{0, -25, -36\}$.

Observation

There are 64 non-trivial solutions of height <100:

$(-2, -24; \pm 216)$, $(9, -24; \pm 576)$, $(-2, -3; \pm 594)$, $(4, -18; \pm 756)$, $(5, -20; \pm 800)$, $(4, -14; \pm 924)$, $(-5, -20; \pm 1200)$, $(9, -3; \pm 1584)$, $(29, -29; \pm 1624)$, $(10, -40; \pm 1800)$, $(5, -45; \pm 1800)$, $(8, -8; \pm 1904)$, $(-7, -18; \pm 2016)$, $(4, -50; \pm 2100)$, $(22, -11; \pm 2310)$, $(-7, -14; \pm 2464)$, $(-5, -45; \pm 2700)$, $(18, -8; \pm 2856)$, $(-10, -11; \pm 3850)$, $(-15, -40; \pm 4800)$, $(-7, -50; \pm 5600)$, $(-24, -40; \pm 8400)$, $(5, -80; \pm 8800)$, $(-5, -80; \pm 13200)$, $(-32, -44; \pm 20064)$, $(14, -88; \pm 24024)$, $(-55, -11; \pm 30800)$, $(-63, -11; \pm 36960)$, $(-27, -64; \pm 52416)$, $(64, 14; \pm 65520)$, $(64, 27; \pm 117936)$ $(-56, -63; \pm 129276)$,

A Diophantine equation II

Fact

There are no solutions $(x, u, z) \in \mathbb{Z}^3$ *such that* $x \equiv 2 \pmod 5$ *and* $u \equiv 5 \pmod{25}$.
Thus, weak approximation *is violated.*

Observe that $x = 2$ and $u = 5$ lead to a solution in 5-adic integers. Indeed, $2 \cdot (2-1) \cdot (2-25) \cdot 5 \cdot (5+25) \cdot (5+36) = -11\,316 \cdot 5^2$ is a 5-adic square.

A Diophantine equation II

Fact

There are no solutions $(x, u, z) \in \mathbb{Z}^3$ *such that* $x \equiv 2 \pmod 5$ *and* $u \equiv 5 \pmod{25}$.
Thus, weak approximation *is violated.*

Observe that $x = 2$ and $u = 5$ lead to a solution in 5-adic integers. Indeed, $2 \cdot (2-1) \cdot (2-25) \cdot 5 \cdot (5+25) \cdot (5+36) = -11\,316 \cdot 5^2$ is a 5-adic square.

Remark

From the geometric point of view, $z^2 = x(x-1)(x-25)u(u+25)(u+36)$ defines a $K3$ surface, more precisely a Kummer surface.
It is obtained form the product $E \times E'$ of the elliptic curves

$$E\colon y^2 = x(x-1)(x-25) \text{ and } E'\colon y'^2 = u(u+25)(u+36)$$

by identifying (x, y, u, y') with $(x, -y, u, -y')$.

The Hilbert symbol

Definition

For k a local field and $0 \neq \alpha, \beta \in k$ define $(\alpha, \beta)_k \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ by

$$(\alpha, \beta)_k := \begin{cases} 0 & \text{if } \alpha X^2 + \beta Y^2 - Z^2 \text{ non-trivially represents } 0 \text{ over } k\,, \\ \frac{1}{2} & \text{otherwise}\,. \end{cases}$$

This is called the *Hilbert symbol* of α and β.

The Hilbert symbol

Definition

For k a local field and $0 \neq \alpha, \beta \in k$ define $(\alpha, \beta)_k \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ by

$$(\alpha, \beta)_k := \begin{cases} 0 & \text{if } \alpha X^2 + \beta Y^2 - Z^2 \text{ non-trivially represents 0 over } k\,, \\ \frac{1}{2} & \text{otherwise}\,. \end{cases}$$

This is called the *Hilbert symbol* of α and β.

Fact

For $0 \neq \alpha, \beta \in \mathbb{Q}$*, there is the* sum formula $\sum\limits_{p \in \{2,3,5,\ldots;\infty\}} (\alpha, \beta)_p = 0.$

The Hilbert symbol II

For the equation $z^2 = x(x-1)(x-25)u(u+25)(u+36)$, we may show the following

- For every non-trivial real or p-adic solution ($p \neq 5$), one automatically has $((x-1)(x-25), (u+25)(u+36))_p = 0$.
- There are, however non-trivial 5-adic solutions such that $((x-1)(x-25), (u+25)(u+36))_5 = \frac{1}{2}$.

The Hilbert symbol II

For the equation $z^2 = x(x-1)(x-25)u(u+25)(u+36)$, we may show the following

- For every non-trivial real or p-adic solution ($p \neq 5$), one automatically has $((x-1)(x-25), (u+25)(u+36))_p = 0$.
- There are, however non-trivial 5-adic solutions such that $((x-1)(x-25), (u+25)(u+36))_5 = \frac{1}{2}$.

Thus, $S(\mathbb{Q}_5)$ splits into two sorts of points (*red* and *green* points), we have a *colouring*. Only one sort may be approximated by $\mathbb{Q}$-rational points.

The Hilbert symbol II

For the equation $z^2 = x(x-1)(x-25)u(u+25)(u+36)$, we may show the following

- For every non-trivial real or p-adic solution ($p \neq 5$), one automatically has $((x-1)(x-25), (u+25)(u+36))_p = 0$.
- There are, however non-trivial 5-adic solutions such that $((x-1)(x-25), (u+25)(u+36))_5 = \frac{1}{2}$.

Thus, $S(\mathbb{Q}_5)$ splits into two sorts of points (*red* and *green* points), we have a *colouring*. Only one sort may be approximated by $\mathbb{Q}$-rational points.

One might try to search for such colourings experimentally. We had no success, found only those, which are known. These are related to the Brauer group.

The Brauer group

Definition

Let S be any scheme. Then the (cohomological) *Brauer group* of S is defined by $\mathrm{Br}(S) := H^2_{\acute{e}t}(S, \mathbb{G}_m)$.

The Brauer group

Definition

Let S be any scheme. Then the (cohomological) *Brauer group* of S is defined by $\text{Br}(S) := H^2_{\text{ét}}(S, \mathbb{G}_m)$.

Remarks

1. This definition is not very explicit. In general, Brauer groups are not easily computable.

The Brauer group

Definition

Let S be any scheme. Then the (cohomological) *Brauer group* of S is defined by $\mathrm{Br}(S) := H^2_{\text{ét}}(S, \mathbb{G}_m)$.

Remarks

1. This definition is not very explicit. In general, Brauer groups are not easily computable.
2. One has $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and

$$\mathrm{Br}(\mathbb{Q}) = \ker(\mathrm{sum}\colon \bigoplus_{p \in \{2,3,5,\dots\}} \mathrm{Br}(\mathbb{Q}_p) \oplus \bigoplus_{\nu\colon K \to \mathbb{R}} \mathrm{Br}(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z}).$$

The Brauer group

Definition

Let S be any scheme. Then the (cohomological) *Brauer group* of S is defined by $\mathrm{Br}(S) := H^2_{\text{ét}}(S, \mathbb{G}_m)$.

Remarks

1. This definition is not very explicit. In general, Brauer groups are not easily computable.
2. One has $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and
$$\mathrm{Br}(\mathbb{Q}) = \ker(\mathrm{sum}\colon \bigoplus_{p \in \{2,3,5,\ldots\}} \mathrm{Br}(\mathbb{Q}_p) \oplus \bigoplus_{\nu\colon K \to \mathbb{R}} \mathrm{Br}(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z})\,.$$
3. Let $\alpha \in \mathrm{Br}(S)$ be any Brauer class. Then, for every K-rational point $p \in S(K)$, there is $\alpha|_p \in \mathrm{Br}(\operatorname{Spec} K)$.
Hence, an adelic point *not* fulfilling the condition that the sum zero cannot be approximated by $\mathbb{Q}$-rational points.
This is called the *Brauer-Manin obstruction* to weak approximation.

The Brauer group II

The cohomological Brauer group of a variety S over a field k is equipped with a canonical filtration, defined by the Hochschild-Serre spectral sequence.

1. $\mathrm{Br}_0(S) \subseteq \mathrm{Br}(S)$ is the image of $\mathrm{Br}(k)$ under the natural map. At least when S has a k-rational point, $\mathrm{Br}_0(S) \cong \mathrm{Br}(k)$. $\mathrm{Br}_0(S)$ does not contribute to the Brauer-Manin obstruction.

The Brauer group II

The cohomological Brauer group of a variety S over a field k is equipped with a canonical filtration, defined by the Hochschild-Serre spectral sequence.

1. $\mathrm{Br}_0(S) \subseteq \mathrm{Br}(S)$ is the image of $\mathrm{Br}(k)$ under the natural map. At least when S has a k-rational point, $\mathrm{Br}_0(S) \cong \mathrm{Br}(k)$. $\mathrm{Br}_0(S)$ does not contribute to the Brauer-Manin obstruction.
2. One has

$$\mathrm{Br}_1(S)/\,\mathrm{Br}_0(S) \cong H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), \mathrm{Pic}(S_{k^{\mathrm{sep}}}))\,.$$

   This subquotient is called the algebraic part of the Brauer group. For k a number field, it is responsible for the so-called *algebraic* Brauer-Manin obstruction.

The Brauer group II

The cohomological Brauer group of a variety S over a field k is equipped with a canonical filtration, defined by the Hochschild-Serre spectral sequence.

1. $\mathrm{Br}_0(S) \subseteq \mathrm{Br}(S)$ is the image of $\mathrm{Br}(k)$ under the natural map. At least when S has a k-rational point, $\mathrm{Br}_0(S) \cong \mathrm{Br}(k)$. $\mathrm{Br}_0(S)$ does not contribute to the Brauer-Manin obstruction.

2. One has

$$\mathrm{Br}_1(S)/\,\mathrm{Br}_0(S) \cong H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), \mathrm{Pic}(S_{k^{\mathrm{sep}}}))\,.$$

   This subquotient is called the algebraic part of the Brauer group. For k a number field, it is responsible for the so-called *algebraic* Brauer-Manin obstruction.

3. Finally, $\mathrm{Br}(S)/\,\mathrm{Br}_1(S)$ injects into $\mathrm{Br}(S_{k^{\mathrm{sep}}})$. This quotient is called the transcendental part of the Brauer group. For k a number field, the corresponding obstruction is called a *transcendental* Brauer-Manin obstruction.

Proposition (Skorobogatov/Zarhin)

Let $E\colon y^2 = x(x-a)(x-b)$ *and* $E'\colon v^2 = u(u-a')(u-b')$ *be two elliptic curves over a field* k, $\operatorname{char} k = 0$. *Suppose that their 2-torsion points are defined over* k *and that* $E_{\overline{k}}$ *and* $E'_{\overline{k}}$ *are not isogenous to each other.*

Further, let $S := \operatorname{Kum}(E \times E')$ *be the corresponding Kummer surface. Then*

$$\operatorname{Br}(S)_2/\operatorname{Br}(k)_2 = \operatorname{im}(\operatorname{Br}(S)_2 \to \operatorname{Br}(S_{\overline{k}})_2) \cong \ker(\mu\colon \mathbb{F}_2^4 \to (k^*/k^{*2})^4)\,,$$

where μ *is given by the matrix*

$$M_{aba'b'} := \begin{pmatrix} 1 & ab & a'b' & -aa' \\ ab & 1 & aa' & a'(a'-b') \\ a'b' & aa' & 1 & a(a-b) \\ -aa' & a'(a'-b') & a(a-b) & 1 \end{pmatrix}.$$

Remarks

1. In general, there is the short exact sequence

$$0 \to \mathrm{Pic}(S)/2\,\mathrm{Pic}(S) \to H^2_{\text{ét}}(S, \mu_2) \to \mathrm{Br}(S)_2 \to 0\,.$$

The Brauer group of particular Kummer surfaces II

Remarks

1. In general, there is the short exact sequence

$$0 \to \mathrm{Pic}(S)/2\,\mathrm{Pic}(S) \to H^2_{\text{ét}}(S, \mu_2) \to \mathrm{Br}(S)_2 \to 0\,.$$

2. $S := \mathrm{Kum}(E \times E')$ over algebraically closed field k. Then $\mathrm{Br}(S)_2 \cong \mathbb{F}_2^4$. More canonically,

$$\mathrm{Br}(S)_2 \cong H^2_{\text{ét}}(E \times E', \mu_2)/(H^2_{\text{ét}}(E, \mu_2) \oplus H^2_{\text{ét}}(E', \mu_2)) \cong \mathrm{Hom}(E[2], E'[2]).$$

Remarks

1. In general, there is the short exact sequence

$$0 \to \operatorname{Pic}(S)/2\operatorname{Pic}(S) \to H^2_{\text{ét}}(S, \mu_2) \to \operatorname{Br}(S)_2 \to 0\,.$$

2. $S := \operatorname{Kum}(E \times E')$ over algebraically closed field k. Then $\operatorname{Br}(S)_2 \cong \mathbb{F}_2^4$. More canonically,

$$\operatorname{Br}(S)_2 \cong H^2_{\text{ét}}(E \times E', \mu_2)/(H^2_{\text{ét}}(E, \mu_2) \oplus H^2_{\text{ét}}(E', \mu_2)) \cong \operatorname{Hom}(E[2], E'[2]).$$

3. $S := \operatorname{Kum}(E \times E')$ over an arbitrary field k, $\operatorname{char} k = 0$. Then the assumption that the 2-torsion points are defined over k implies that $\operatorname{Gal}(\overline{k}/k)$ operates trivially on $\operatorname{Br}(S_{\overline{k}})_2$. Nevertheless, in general,

$$\operatorname{Br}(S)_2/\operatorname{Br}(k)_2 \subsetneq \operatorname{Br}(S_{\overline{k}})_2^{\operatorname{Gal}(\overline{k}/k)} \cong \mathbb{F}_2^4\,.$$

Algebraic versus transcendental Brauer-Manin obstruction

- Algebraic Brauer-Manin obstruction:

  Explicit computations have been done for many classes of varieties. Most examples were Fano.

  Cubic surfaces:

  Classical counterexamples to the Hasse principle (Mordell and Cassels/ Guy) are in fact algebraic BM (Manin),
  $\mathrm{Br}(S)/\mathrm{Br}(\mathbb{Q}) \cong 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/3\mathbb{Z})^2$ (Swinnerton-Dyer),
  Order-2 (3) Brauer class only if Galois invariant double-six (triplet, E.&J.)

  Computations for diagonal quartic surfaces, by M. Bright.

Algebraic versus transcendental Brauer-Manin obstruction

- Algebraic Brauer-Manin obstruction:

  Explicit computations have been done for many classes of varieties. Most examples were Fano.

  Cubic surfaces:
  Classical counterexamples to the Hasse principle (Mordell and Cassels/ Guy) are in fact algebraic BM (Manin),
  $\mathrm{Br}(S)/\mathrm{Br}(\mathbb{Q}) \cong 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/3\mathbb{Z})^2$ (Swinnerton-Dyer),
  Order-2 (3) Brauer class only if Galois invariant double-six (triplet, E.&J.)

  Computations for diagonal quartic surfaces, by M. Bright.

- Transcendental Brauer-Manin obstruction:

  Much less understood, seemingly more difficult.
  First explicit example: Harari 1993.
  Literature still very small. Often enormous efforts.
  E.g., a whole Ph.D. thesis on one diagonal quartic surface, by Th. Preu.

The local evaluation map

Remark

The result of Skorobogatov/Zarhin gives us a class of varieties, for which the transcendental Brauer group is exceptionally well accessible. The same is true for the local evaluation map.

The local evaluation map

Remark

The result of Skorobogatov/Zarhin gives us a class of varieties, for which the transcendental Brauer group is exceptionally well accessible. The same is true for the local evaluation map.

Fact

Over the function field $k(S)$, each of the 16 vectors in $\mathbb{F}_2^4$ defines a Brauer class. Consider the four quaternion algebras

$$A_{\mu,\nu} := ((x-\mu)(x-b), (u-\nu)(u-b')), \qquad \mu = 0, a,\ \nu = 0, a'.$$

Then e_1 corresponds to $A_{a,a'}$, e_2 to $A_{a,0}$, e_3 to $A_{0,a'}$, and e_4 to $A_{0,0}$.

The local evaluation map II

Lemma

Let k be a local field, $\operatorname{char} k = 0$*, $a, b, a', b' \in k$ be such that*

$$E\colon y^2 = x(x-a)(x-b) \quad \textit{and} \quad E'\colon v^2 = u(u-a')(u-b')$$

are elliptic curves. Consider $S := \operatorname{Kum}(E \times E')$, given explicitly by

$$z^2 = x(x-a)(x-b)u(u-a')(u-b')\,.$$

Let $\alpha \in \operatorname{Br}(S)$ be a Brauer class, represented over $k(S)$ by the central simple algebra $\bigotimes_i A_{\mu_i,\nu_i}$.
Then the local evaluation map $\operatorname{ev}_\alpha\colon S(k) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is given by

$$(x,u;z) \mapsto \operatorname{ev}_\alpha((x,u;z)) = \sum_i ((x-\mu_i)(x-b),(u-\nu_i)(u-b'))_k\,.$$

Constancy near the singular points

Lemma

Let $p > 2$ be a prime number and $a, b, a', b' \in \mathbb{Z}_p$ be such that $E\colon y^2 = x(x-a)(x-b)$ and $E'\colon v^2 = u(u-a')(u-b')$ are elliptic curves, not isogenous to each other. Put

$$l := \max(\nu_p(a), \nu_p(b), \nu_p(a-b), \nu_p(a'), \nu_p(b'), \nu_p(a'-b')) .$$

Consider the surface S over $\mathbb{Q}_p$, given by

$$z^2 = x(x-a)(x-b)u(u-a')(u-b') .$$

Then, for every $\alpha \in \mathrm{Br}(S)_2$, the evaluation map $S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is constant on the subset

$$T := \{(x, u; z) \in S(\mathbb{Q}_p) \mid \nu_p(x) < 0 \text{ or } \nu_p(u) < 0 \text{ or } x \equiv \mu, u \equiv \nu \pmod{p^{l+1}}, \mu = 0, a, b,\ \nu = 0, a', b'\} .$$

The case of good reduction

Proposition

Let $E\colon y^2 = x(x-a)(x-b)$ *and* $E'\colon v^2 = u(u-a')(u-b')$ *be two elliptic curves over a local field* k*, not isogenous to each other. Suppose that* $a, b, a', b' \in k$*. Further, let* $S := \mathrm{Kum}(E \times E')$ *be the corresponding Kummer surface.*

Suppose that either $k = \mathbb{R}$ *or* k *is a p-adic field and both* E *and* E' *have good reduction. Then, for every* $\alpha \in \mathrm{Br}(S)_2$*, the evaluation map* $\mathrm{ev}_\alpha\colon S(k) \to \mathbb{Q}/\mathbb{Z}$ *is constant.*

The case of good reduction

Proposition

Let $E\colon y^2 = x(x-a)(x-b)$ *and* $E'\colon v^2 = u(u-a')(u-b')$ *be two elliptic curves over a local field* k*, not isogenous to each other. Suppose that* $a, b, a', b' \in k$*. Further, let* $S := \mathrm{Kum}(E \times E')$ *be the corresponding Kummer surface.*

Suppose that either $k = \mathbb{R}$ *or* k *is a* p*-adic field and both* E *and* E' *have good reduction. Then, for every* $\alpha \in \mathrm{Br}(S)_2$*, the evaluation map* $\mathrm{ev}_\alpha\colon S(k) \to \mathbb{Q}/\mathbb{Z}$ *is constant.*

- The case $k = \mathbb{Q}_p$ is a particular case of a very general result, due to J.-L. Colliot-Thélène and A. N. Skorobogatov. It also follows from the lemma above.

The case of good reduction II

- $k = \mathbb{R}$: Without loss of generality, suppose $a > b > 0$ and $a' > b' > 0$. Then

$$M_{aba'b'} = \begin{pmatrix} + & + & + & - \\ + & + & + & + \\ + & + & + & + \\ - & + & + & + \end{pmatrix}$$

has kernel $\langle e_2, e_3 \rangle$. Representatives for e_2 and e_3 are $((x-a)(x-b), u(u-b'))_{\mathbb{R}}$ and $(x(x-b), (u-a')(u-b'))_{\mathbb{R}}$.

e_2: $((x-a)(x-b), u(u-b'))_{\mathbb{R}} = \frac{1}{2}$ would mean $(x-a)(x-b) < 0$ and $u(u-b') < 0$. Hence, $b < x < a$ and $0 < u < b'$. But then $x(x-a)(x-b)u(u-a')(u-b') < 0$. There is no real point on S corresponding to (x, u).

For e_3, the argument is analogous.

An algorithm determining the local evaluation map

Algorithm

Let the parameters $a, b, a', b' \in \mathbb{Z}$, a Brauer class $\alpha \in \mathrm{Br}(S)_2$ as a combination of Hilbert symbols, and a prime number p be given.

1. Calculate $l := \max(\nu_p(a), \nu_p(b), \nu_p(a-b), \nu_p(a'), \nu_p(b'), \nu_p(a'-b'))$.

An algorithm determining the local evaluation map

Algorithm

Let the parameters $a, b, a', b' \in \mathbb{Z}$, a Brauer class $\alpha \in \mathrm{Br}(S)_2$ as a combination of Hilbert symbols, and a prime number p be given.

1. Calculate $l := \max(\nu_p(a), \nu_p(b), \nu_p(a-b), \nu_p(a'), \nu_p(b'), \nu_p(a'-b'))$.
2. Initialize three lists S_0, S_1, and S_2, the first two being empty, the third containing all triples (x_0, u_0, p) for $x_0, u_0 \in \{0, \ldots, p-1\}$. A triple (x_0, u_0, p^e) shall represent the subset

$$\{(x, u; z) \in S(\mathbb{Q}_p) \mid \nu_p(x - x_0) \geq e, \nu_p(u - u_0) \geq e\} \; .$$

An algorithm determining the local evaluation map

Algorithm

Let the parameters $a, b, a', b' \in \mathbb{Z}$, a Brauer class $\alpha \in \mathrm{Br}(S)_2$ as a combination of Hilbert symbols, and a prime number p be given.

1. Calculate $l := \max(\nu_p(a), \nu_p(b), \nu_p(a-b), \nu_p(a'), \nu_p(b'), \nu_p(a'-b'))$.
2. Initialize three lists S_0, S_1, and S_2, the first two being empty, the third containing all triples (x_0, u_0, p) for $x_0, u_0 \in \{0, \dots, p-1\}$. A triple (x_0, u_0, p^e) shall represent the subset

$$\{(x, u; z) \in S(\mathbb{Q}_p) \mid \nu_p(x - x_0) \geq e, \nu_p(u - u_0) \geq e\} \, .$$

3. Run through S_2. For each element (x_0, u_0, p^e), execute, in this order, the following operations.

- Test whether the corresponding set is non-empty. Otherwise, delete it.
- If $e \geq l + 1$, $\nu_p(x - \mu) \geq l + 1$ and $\nu_p(u - \nu) \geq l + 1$ for some $\mu \in \{0, a, b\}$ and $\nu \in \{0, a', b'\}$ then move (x_0, u_0, p^e) to S_0.

An algorithm determining the local evaluation map II

- Test naively, using the elementary properties of the Hilbert symbol, whether the elements in the corresponding set all have the same evaluation. If this test succeeds then move (x_0, u_0, p^e) to S_0 or S_1, accordingly.
- Otherwise, replace (x_0, u_0, p^e) by the p^2 triples $(x_0 + ip^e, u_0 + jp^e, p^{e+1})$ for $i, j \in \{0, \ldots, p-1\}$.

An algorithm determining the local evaluation map II

- Test naively, using the elementary properties of the Hilbert symbol, whether the elements in the corresponding set all have the same evaluation. If this test succeeds then move (x_0, u_0, p^e) to S_0 or S_1, accordingly.
- Otherwise, replace (x_0, u_0, p^e) by the p^2 triples $(x_0 + ip^e, u_0 + jp^e, p^{e+1})$ for $i, j \in \{0, \ldots, p-1\}$.

4. If S_2 is empty then output S_0 and S_1 and terminate. Otherwise, go back to step 3.

An algorithm determining the local evaluation map II

- Test naively, using the elementary properties of the Hilbert symbol, whether the elements in the corresponding set all have the same evaluation. If this test succeeds then move (x_0, u_0, p^e) to S_0 or S_1, accordingly.
- Otherwise, replace (x_0, u_0, p^e) by the p^2 triples $(x_0 + ip^e, u_0 + jp^e, p^{e+1})$ for $i, j \in \{0, \ldots, p-1\}$.

4. If S_2 is empty then output S_0 and S_1 and terminate. Otherwise, go back to step 3.

Remark

This algorithm terminates after finitely many steps only because constancy near the singular points is known.

Back to the introductory example

The introductory example $S\colon z^2 = x(x-1)(x-25)u(u+25)(u+36)$ has the Skorobogatov-Zarhin matrix

$$M = \begin{pmatrix} 1 & 25 & 900 & 25 \\ 25 & 1 & -25 & -275 \\ 900 & -25 & 1 & -24 \\ 25 & -275 & -24 & 1 \end{pmatrix} \mathrel{\widehat{=}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -11 \\ 1 & -1 & 1 & -6 \\ 1 & -11 & -6 & 1 \end{pmatrix},$$

with $\ker M = \langle e_1 \rangle$. Thus, there is a non-trivial Brauer class.

Furthermore, S has bad reduction at $2, 3, 5$, and 11. Running the algorithm for these four primes, one sees that the local evaluation maps at $2, 3$, and 11 are constant, while that at 5 is not.

Some kind of normal form

Observation

Let k be a field, $a, b, a', b' \in k^*$, $a \neq b$, $a' \neq b'$, and S be the Kummer surface $z^2 = x(x-a)(x-b)u(u-a')(u-b')$. There are two types of non-trivial Brauer classes $\alpha \in \operatorname{Br}(S)_2 / \operatorname{Br}(k)_2$.

Some kind of normal form

Observation

Let k be a field, $a, b, a', b' \in k^*$, $a \neq b$, $a' \neq b'$, and S be the Kummer surface $z^2 = x(x-a)(x-b)u(u-a')(u-b')$. There are two types of non-trivial Brauer classes $\alpha \in \operatorname{Br}(S)_2/\operatorname{Br}(k)_2$.

Type 1. α may be expressed by a single Hilbert symbol.
There are nine cases for the kernel vector of $M_{aba'b'}$. A suitable translation of $\mathbf{A}^1 \times \mathbf{A}^1$ transforms the surface into one with kernel vector e_1.
Then $ab, a'b', (-aa') \in k^{*2}$.
This implies $(-ba'), (-ab'), (-bb') \in k^{*2}$, too.

Some kind of normal form

Observation

Let k be a field, $a, b, a', b' \in k^*$, $a \neq b$, $a' \neq b'$, and S be the Kummer surface $z^2 = x(x-a)(x-b)u(u-a')(u-b')$. There are two types of non-trivial Brauer classes $\alpha \in \mathrm{Br}(S)_2 / \mathrm{Br}(k)_2$.

Type 1. α may be expressed by a single Hilbert symbol.
There are nine cases for the kernel vector of $M_{aba'b'}$. A suitable translation of $\mathbf{A}^1 \times \mathbf{A}^1$ transforms the surface into one with kernel vector e_1. Then $ab, a'b', (-aa') \in k^{*2}$.
This implies $(-ba'), (-ab'), (-bb') \in k^{*2}$, too.

Type 2. To express α, two Hilbert symbols are necessary.
There are six cases for the kernel vector of $M_{aba'b'}$. A suitable translation of $\mathbf{A}^1 \times \mathbf{A}^1$ transforms the surface into one with kernel vector $e_2 + e_3$. Then $aa', bb', (a-b)(a'-b') \in k^{*2}$.

A criterion for trivial evaluation

Theorem

Let $p > 2$ be a prime number and $0 \neq a, b, a', b' \in \mathbb{Z}_p$ such that $a \neq b$ and $a' \neq b'$. Let S be the Kummer surface, given by $z^2 = x(x-a)(x-b)u(u-a')(u-b')$.

Assume that e_1 is a kernel vector of the matrix $M_{aba'b'}$ and let $\alpha \in \mathrm{Br}(S)_2$ be the corresponding Brauer class.

1. *Suppose $a \equiv b \not\equiv 0 \pmod{p}$ or $a' \equiv b' \not\equiv 0 \pmod{p}$. Then the evaluation map $\mathrm{ev}_\alpha \colon S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is constant.*
2. *If $a \not\equiv b \pmod{p}$, $a' \not\equiv b' \pmod{p}$, and not all four numbers are p-adic units then the evaluation map $\mathrm{ev}_\alpha \colon S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is non-constant.*

A criterion for trivial evaluation

Theorem

Let $p > 2$ be a prime number and $0 \neq a, b, a', b' \in \mathbb{Z}_p$ such that $a \neq b$ and $a' \neq b'$. Let S be the Kummer surface, given by $z^2 = x(x-a)(x-b)u(u-a')(u-b')$.

Assume that e_1 is a kernel vector of the matrix $M_{aba'b'}$ and let $\alpha \in \mathrm{Br}(S)_2$ be the corresponding Brauer class.

1. *Suppose $a \equiv b \not\equiv 0 \pmod{p}$ or $a' \equiv b' \not\equiv 0 \pmod{p}$. Then the evaluation map $\mathrm{ev}_\alpha \colon S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is constant.*
2. *If $a \not\equiv b \pmod{p}$, $a' \not\equiv b' \pmod{p}$, and not all four numbers are p-adic units then the evaluation map $\mathrm{ev}_\alpha \colon S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is non-constant.*

Remark

Consider $a = 1, b = 25, a' = -25, b' = -36$.
By 1, we have constancy at $2, 3, 11$. By 2, there is non-constancy at 5.

A sample

Determined all Kummer surfaces of the form

$$z^2 = x(x-a)(x-b)u(u-a')(u-b')$$

allowing coefficients of absolute value ≤ 200 and having a transcendental 2-torsion Brauer class.

More precisely,

- we determined all $(a, b, a', b') \in \mathbb{Z}^4$ such that $\gcd(a, b) = 1$, $\gcd(a', b') = 1$, $a > b > 0$, $a - b, b \leq 200$, as well as $a' < b' < 0$, $a' - b', b' \geq -200$ and the matrix $M_{aba'b'}$ has a non-zero kernel.
- We made sure that (a, b, a', b') was not listed when $(-a', -b', -a, -b)$, $(a, a-b, a', a'-b')$, or $(-a', b'-a', -a, b-a)$ was already in the list. We ignored the quadruples where (a, b) and (a', b') define geometrically isomorphic elliptic curves.

A sample II

This led to

- 3075 surfaces with a kernel vector of type 1, among them 26 have $\mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q})_2 = 0$, due to a $\mathbb{Q}$-isogeny.
- 367 surfaces with a kernel vector of type 2
- two surfaces with $\dim \mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q})_2 = 2$, $(25, 9, -169, -25)$ and $(25, 16, -169, -25)$.

The generic case is that $\dim \mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q})_2 = 0$.

A sample II

This led to

- 3075 surfaces with a kernel vector of type 1, among them 26 have $\mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q})_2 = 0$, due to a $\mathbb{Q}$-isogeny.
- 367 surfaces with a kernel vector of type 2
- two surfaces with $\dim \mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q})_2 = 2$, $(25, 9, -169, -25)$ and $(25, 16, -169, -25)$.

The generic case is that $\dim \mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q})_2 = 0$.

Definition

1. We say that a Brauer class $\alpha \in \mathrm{Br}(S)$ *works* at a prime p if the local evaluation map $\mathrm{ev}_{\alpha,p}$ is non-constant.
2. A prime number p is *BM-relevant* for S if there is a Brauer class working at p.

BM-relevant primes

$(25, 9, -169, -25)$:
One Brauer class works at 2 and 13, another at 5 and 13, and the third at all three.

$(25, 16, -169, -25)$:
One Brauer class works at 3 and 13, another at 5 and 13, and the last at all three.

Remaining surfaces:

# relevant primes	# surfaces
-	6
1	428
2	1577
3	1119
4	276
5	9
6	1

For $(196, 75, -361, -169)$, the Brauer class works at 2, 5, 7, 11, 13, and 19.

$\mathbb{Q}$-rational points

Assume $\alpha \in \mathrm{Br}(S)$ works at l primes $p_1, \dots, p_l$. There are 2^l vectors consisting only of zeroes and $\frac{1}{2}$'s. By the Brauer-Manin obstruction, half of them are forbidden as values of

$$(\mathrm{ev}_{\alpha,p_1}(x), \dots, \mathrm{ev}_{\alpha,p_l}(x))$$

for $\mathbb{Q}$-rational points $x \in S(\mathbb{Q})$.

$\mathbb{Q}$-rational points

Assume $\alpha \in \mathrm{Br}(S)$ works at l primes $p_1, \dots, p_l$. There are 2^l vectors consisting only of zeroes and $\frac{1}{2}$'s. By the Brauer-Manin obstruction, half of them are forbidden as values of

$$(\mathrm{ev}_{\alpha,p_1}(x), \dots, \mathrm{ev}_{\alpha,p_l}(x))$$

for $\mathbb{Q}$-rational points $x \in S(\mathbb{Q})$.

Table: Search bounds to get all vectors by rational points

		bound N insufficient for								
#primes	#surfaces	$N = 50$	100	200	400	800	1600	3200	6400	12800
2	1577	190	56	22	-					
3	1119	555	187	48	1	-				
4	262	262	200	127	67	36	24	13	4	-
5	9	9	9	8	8	8	5	3	1	-

Table: Numbers of vectors in the case $(196, 75, -361, -169)$

bound	50	100	200	400	800	1600	3200	6400	12 800	25 600	50 000
vectors	5	10	14	20	24	26	28	30	31	31	32

$\mathbb{Q}$-rational points II

Algorithm (Point search)

Given two lists $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ and a search bound B, this algorithm will simultaneously search for the solutions of all equations of the form

$$w^2 = f_{a_i b_i}(x, y) f_{a_j b_j}(u, v) \, .$$

Here, f_{ab} is the binary quartic form $f_{ab}(x, y) := xy(x - ay)(x - by)$. It will find those with $|x|, |y|, |u|, |v| \leq B$.

1. Compute the bound $L := B(1 + \max\{|a_i|, |b_i| \mid i = 1, \ldots, k\})$ for the linear factors.

$\mathbb{Q}$-rational points II

Algorithm (Point search)

Given two lists $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ and a search bound B, this algorithm will simultaneously search for the solutions of all equations of the form

$$w^2 = f_{a_i b_i}(x, y) f_{a_j b_j}(u, v)\,.$$

Here, f_{ab} is the binary quartic form $f_{ab}(x, y) := xy(x - ay)(x - by)$.
It will find those with $|x|, |y|, |u|, |v| \leq B$.

1. Compute the bound $L := B(1 + \max\{|a_i|, |b_i| \mid i = 1, \ldots, k\})$ for the linear factors.
2. Store the square-free parts of the integers in $[1, \ldots, L]$ in an array T.

$\mathbb{Q}$-rational points II

Algorithm (Point search)

Given two lists $a_1, \dots, a_k$ and $b_1, \dots, b_k$ and a search bound B, this algorithm will simultaneously search for the solutions of all equations of the form

$$w^2 = f_{a_i b_i}(x, y) f_{a_j b_j}(u, v) \,.$$

Here, f_{ab} is the binary quartic form $f_{ab}(x, y) := xy(x - ay)(x - by)$.
It will find those with $|x|, |y|, |u|, |v| \leq B$.

1. Compute the bound $L := B(1 + \max\{|a_i|, |b_i| \mid i = 1, \dots, k\})$ for the linear factors.
2. Store the square-free parts of the integers in $[1, \dots, L]$ in an array T.
3. Enumerate in an iterated loop representatives for all points $[x : y] \in \mathbf{P}^1(\mathbb{Q})$ with $x, y \in \mathbb{Z}$, $|x|, |y| \leq B$, and $x, y \neq 0$.

$\mathbb{Q}$-rational points III

4. For each point $[x : y]$ enumerated, execute the operations below.

- Run a loop over $i = 1, \ldots, k$ to compute the four linear factors x, y, $x - a_i y$, and $x - b_i y$ of f_{a_i,b_i}.
- Store the square-free parts of the factors in $m_1, \ldots, m_4$. Use the table T here.
- Put $p_1 := \frac{m_1}{\gcd(m_1,m_2)} \frac{m_2}{\gcd(m_1,m_2)}$, $p_2 := \frac{m_3}{\gcd(m_3,m_4)} \frac{m_4}{\gcd(m_3,m_4)}$, and

$$p_3 := \frac{p_1}{\gcd(p_1,p_2)} \frac{p_2}{\gcd(p_1,p_2)} \,.$$

  Thus, p_3 is a representative of the square class of $f_{a_i b_i}(x, y)$.
- Store the quadruple $(x, y, i, h(p_3))$ into a list. Here, h is a hash-function.

$\mathbb{Q}$-rational points III

4. For each point $[x : y]$ enumerated, execute the operations below.

- Run a loop over $i = 1, \dots, k$ to compute the four linear factors x, y, $x - a_i y$, and $x - b_i y$ of f_{a_i,b_i}.
- Store the square-free parts of the factors in $m_1, \dots, m_4$. Use the table T here.
- Put $p_1 := \frac{m_1}{\gcd(m_1,m_2)} \frac{m_2}{\gcd(m_1,m_2)}$, $p_2 := \frac{m_3}{\gcd(m_3,m_4)} \frac{m_4}{\gcd(m_3,m_4)}$, and

$$p_3 := \frac{p_1}{\gcd(p_1,p_2)} \frac{p_2}{\gcd(p_1,p_2)} .$$

  Thus, p_3 is a representative of the square class of $f_{a_i b_i}(x, y)$.
- Store the quadruple $(x, y, i, h(p_3))$ into a list. Here, h is a hash-function.

5. Sort the list by the last component.

$\mathbb{Q}$-rational points III

6. Split the list into parts. Each part corresponds to a single value of $h(p_3)$. (At this point, we have detected all collisions of the hash-function.)

$\mathbb{Q}$-rational points III

6. Split the list into parts. Each part corresponds to a single value of $h(p_3)$. (At this point, we have detected all collisions of the hash-function.)
7. Run in an iterated loop over all the collisions and check whether $((x, y, i, h(p_3)), (x', y', i', h(p'_3)))$ corresponds to a solution $([x : y], [x' : y'])$ of the equation $w^2 = f_{a_i b_i}(x, y) f_{a_{i'} b_{i'}}(x', y')$. Output all the solutions found.

$\mathbb{Q}$-rational points III

6. Split the list into parts. Each part corresponds to a single value of $h(p_3)$. (At this point, we have detected all collisions of the hash-function.)
7. Run in an iterated loop over all the collisions and check whether $((x, y, i, h(p_3)), (x', y', i', h(p_3')))$ corresponds to a solution $([x : y], [x' : y'])$ of the equation $w^2 = f_{a_i b_i}(x, y) f_{a_{i'} b_{i'}}(x', y')$. Output all the solutions found.

Remarks

- For practical search bounds B, the first integer overflow occurs when we multiply $\frac{p_1}{\gcd(p_1,p_2)}$ and $\frac{p_2}{\gcd(p_1,p_2)}$. But we can think of this reduction modulo 2^{64} as being a part of our hash-function.
- In practice, some modification of this algorithm is necessary as it would require more memory than reasonably available. We introduced a *multiplicative paging*.

Summary

Summary

- We investigated the transcendental Brauer-Manin obstruction for a sample of particular Kummer surfaces.
  Actually, most of the surfaces had $\operatorname{Br}(S)/\operatorname{Br}(\mathbb{Q}) = 0$, but there was a 2-torsion Brauer class on more than 3000 of the surfaces.
- In our situation, the Brauer classes never works at the infinite place. As is known, they do not work at good places, either.

Summary

Summary

- We investigated the transcendental Brauer-Manin obstruction for a sample of particular Kummer surfaces.
  Actually, most of the surfaces had $\mathrm{Br}(S)/\mathrm{Br}(\mathbb{Q}) = 0$, but there was a 2-torsion Brauer class on more than 3000 of the surfaces.
- In our situation, the Brauer classes never works at the infinite place. As is known, they do not work at good places, either.
- We tested at which (bad) primes the Brauer classes actually work. There were form zero (in six cases) to six BM-relevant primes.
- We carried out a relatively extensive point search, but no other exceptional phenomena showed up. Our results are perfectly compatible with the idea that there are no further obstructions.

Summary

Summary

- We investigated the transcendental Brauer-Manin obstruction for a sample of particular Kummer surfaces.
  Actually, most of the surfaces had $\mathrm{Br}(S)/\mathrm{Br}(\mathbb{Q}) = 0$, but there was a 2-torsion Brauer class on more than 3000 of the surfaces.
- In our situation, the Brauer classes never works at the infinite place. As is known, they do not work at good places, either.
- We tested at which (bad) primes the Brauer classes actually work. There were form zero (in six cases) to six BM-relevant primes.
- We carried out a relatively extensive point search, but no other exceptional phenomena showed up. Our results are perfectly compatible with the idea that there are no further obstructions.

Thank you!!