THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Experiments with the transcendental Brauer-Manin obstruction

Andreas-Stephan Elsenhans and Jörg Jahnel

msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.369

msp

Experiments with the transcendental Brauer-Manin obstruction

Andreas-Stephan Elsenhans and Jörg Jahnel

We report on some experiments and theoretical investigations concerning weak approximation and the transcendental Brauer-Manin obstruction for Kummer surfaces of certain products of elliptic curves.

1. Introduction

Weak approximation. Consider a geometrically integral, projective variety S over the field $\mathbb{Q}$ of rational numbers. We say that *S fulfills weak approximation* when the following is true: For every finite set $\{p_1, \ldots, p_l\}$ of prime numbers and every vector

$$(x_0, x_1, \ldots, x_l) \in S(\mathbb{R}) \times S(\mathbb{Q}_{p_1}) \times \cdots \times S(\mathbb{Q}_{p_l}),$$

there exists a sequence of $\mathbb{Q}$-rational points that simultaneously converges to x_i in the p_i-adic topology for $i = 1, \ldots, l$ and to x_0 with respect to the real topology. In a more formal language, this means that the set $S(\mathbb{Q})$ of the rational points on S is dense in the set $S(\mathbb{A}_{\mathbb{Q}})$ of all adelic points.

Even for Fano varieties, which are generally expected to have many rational points, weak approximation is not always fulfilled. Well-known counterexamples are due to Sir Peter Swinnerton-Dyer [26], L. J. Mordell [20], J. W. S. Cassels and M. J. T. Guy [4], and many others.

For varieties of intermediate type — K3 surfaces, for example — the situation is yet more obscure. In fact, proving the much weaker statement that $\#S(\mathbb{Q}) = \infty$ is usually a formidable task in its own [18; 17]. It seems therefore that proving weak approximation, even for a single K3 surface, is presently out of reach and that experiments are asked for.

MSC2010: primary 11D41; secondary 11Y50, 11G35, 14J28.
Keywords: Kummer surface, weak approximation, transcendental Brauer-Manin obstruction, multivariate paging.

Obstructions and colorings. To test weak approximation experimentally is, however, an ill-posed problem, at least from the strictly formal point of view. The reason is that weak approximation is not a finite phenomenon. It is strongly infinite in nature.

An interesting situation occurs when a certain "obstruction" is responsible for the failure of weak approximation. This means that $S(\mathbb{Q}_p)$ breaks somehow regularly into open-closed subsets, each of which behaves uniformly as far as approximation by $\mathbb{Q}$-rational points is concerned. As $S(\mathbb{Q}_p)$ is compact, it is clear that finitely many subsets $U_1, \ldots, U_k \subset S(\mathbb{Q}_p)$ will suffice. When such a behavior appears, we speak of a *coloring* and call the subsets the *colors* of $S(\mathbb{Q}_p)$.

The Brauer-Manin obstructions. It is well-known that a class $\alpha \in \mathrm{Br}(S)$ in the Grothendieck-Brauer group of S induces such a coloring. For a point $x \in S(\mathbb{Q}_p)$, its color is obtained as $\mathrm{inv}_{\mathbb{Q}_p}(\alpha|x) \in \mathbb{Q}/\mathbb{Z}$. If α is of order N then not more than N colors may occur.

As a result, a failure of weak approximation may appear. Indeed, for a $\mathbb{Q}$-rational point x one must have $\sum_p \mathrm{inv}_{\mathbb{Q}_p}(\alpha|x) = 0$, but the same need not be true for an adelic point. This phenomenon is called the Brauer-Manin obstruction [19].

There is a canonical filtration on $\mathrm{Br}(S)$, which gives rise to a distinction between *algebraic* and *transcendental* Brauer classes. Correspondingly, there are the algebraic and the transcendental Brauer-Manin obstructions.

The algebraic Brauer-Manin obstruction is rather well understood. At least on $S(\mathbb{Q}_p)_{\mathrm{good}} \subseteq S(\mathbb{Q}_p)$, the p-adic points with good reduction, it yields extremely regular colorings [5; 6; 11]. For example, a coloring by two colors is possible only when there is an unramified two-sheeted covering $\pi : X \to S(\mathbb{Q}_p)_{\mathrm{good}}$. The two colors are then given by the subsets

$$\{x \in S(\mathbb{Q}_p) \mid \pi^{-1}(x) = \varnothing\} \quad \text{and} \quad \{x \in S(\mathbb{Q}_p) \mid \#\pi^{-1}(x) = 2\}.$$

Explicit computations of the algebraic Brauer-Manin obstruction have been done for many classes of varieties. Most of the examples were Fano. For instance, we gave a systematic treatment of the (algebraic) Brauer-Manin obstruction for cubic surfaces in [9; 10]. Concerning K3 surfaces, computations for diagonal quartic surfaces are provided by M. Bright [3]. Furthermore, it is known that there is no algebraic Brauer-Manin obstruction on a generic Kummer surface, or in the generic case of a Kummer surface associated to the product of two elliptic curves [25, Proposition 1.4(ii)].

The transcendental Brauer-Manin obstruction. The transcendental Brauer-Manin obstruction is much less understood and seems to be by far more difficult, at least at present. Historically, the first example of a variety where weak approximation is violated due to a transcendental Brauer class was constructed by D. Harari [12].

Concerning K3 surfaces, the available literature is still rather small. The interested reader is encouraged to consult the articles [13; 14; 15; 16; 22; 24; 27], at least in order to recognize the enormous efforts made by the authors. For example, the entire Ph.D. thesis of Th. Preu is devoted to the computation of the transcendental Brauer-Manin obstruction for single diagonal quartic surface.

An exceptional case, which seems to be a bit more accessible, is provided by the Kummer surfaces $S := \mathrm{Kum}(E \times E')$ for two elliptic curves E and E'. Here the Brauer group, which is typically purely transcendental, was described in detail by A. N. Skorobogatov and Yu. G. Zarhin in [25].

The present article. For this reason, in the present article we will deal with Kummer surfaces, defined over $\mathbb{Q}$, of the type described in the preceding paragraph. To keep the theory simple, we will restrict ourselves to the case that both curves have their full 2-torsion defined over the base field. We may start with equations for the elliptic curves of the form

$$E : y^2 = x(x-a)(x-b) \quad \text{and} \quad E' : y^2 = x(x-a')(x-b'),$$

for $a, b, a', b' \in \mathbb{Q}$. Then $S := \mathrm{Kum}(E \times E')$ is a double cover of $\mathbf{P}^1 \times \mathbf{P}^1$, an affine chart of which is given by the equation

$$z^2 = x(x-a)(x-b)u(u-a')(u-b'). \tag{1}$$

The goal of the article is to report on our experiments and theoretical investigations concerning weak approximation and the transcendental Brauer-Manin obstruction for Kummer surfaces of this particular type.

Remark 1.1. To be precise, Equation (1) defines a model of the Kummer surface with 16 singular points of type A_1. In the minimal regular model, the singularities are replaced by projective lines. As $\mathrm{Br}(\mathbf{P}^1_k) = \mathrm{Br}(k)$, the evaluation of a Brauer class on a projective line is automatically constant. Thus, we may work as well with the singular model.

The results. Among the Kummer surfaces of type (1) for integers a, b, a', b' of absolute value at most 200, we determined all those for which there is a transcendental Brauer-Manin obstruction arising from a 2-torsion Brauer class.

We found that there are exactly 3418 such surfaces having a nontrivial 2-torsion Brauer class. In three cases, this class was algebraic. Moreover, we identified the adelic subsets of the surfaces where the Brauer class gives no obstruction. On only six of the surfaces, it happened that no adelic point was excluded.

On the other hand, we developed a memory-friendly point searching algorithm for Kummer surfaces of the form above. The sets of $\mathbb{Q}$-rational points found turned out to be compatible with the idea that the Brauer-Manin obstruction might be the only obstruction to weak approximation.

2. The transcendental Brauer group

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

(i) $\mathrm{Br}_0(S) \subseteq \mathrm{Br}(S)$ is the image of $\mathrm{Br}(k)$ under the natural map. When S has a k-rational point, we have $\mathrm{Br}_0(S) \cong \mathrm{Br}(k)$; when k is a number field, the existence of an adelic point suffices. The group $\mathrm{Br}_0(S)$ does not contribute to the Brauer-Manin obstruction.

(ii) The quotient $\mathrm{Br}_1(S)/\mathrm{Br}_0(S)$ is isomorphic to $H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), \mathrm{Pic}(S_{k^{\mathrm{sep}}}))$. This subquotient is called the *algebraic* part of the Brauer group. For k a number field, it is responsible for the algebraic Brauer-Manin obstruction.

(iii) 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. Nevertheless, every Brauer class that is not algebraic is usually said to be transcendental. For k a number field, the corresponding obstruction is a transcendental Brauer-Manin obstruction.

When S is the Kummer surface corresponding to the product of two elliptic curves, the Brauer group of S is well understood due to the work of A. N. Skorobogatov and Yu. G. Zarhin [25]. For us, the proposition below will be sufficient.

Notation. We will denote the 2-torsion part of an abelian group A by A_2.

Proposition 2.1 (Skorobogatov and Zarhin). *Let*

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

be elliptic curves over a field k of characteristic zero, and let $S := \mathrm{Kum}(E \times E')$ be the corresponding Kummer surface. Suppose that the 2-torsion points of E and E' are defined over k and that $E_{\bar{k}}$ and $E'_{\bar{k}}$ are not isogenous to one another. Then

$$\mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = \mathrm{im}\big(\mathrm{Br}(S)_2 \to \mathrm{Br}(S_{\bar{k}})_2\big) \cong \ker(\mu : \mathbb{F}_2^4 \to (k^*/k^{*2})^4),$$

where μ is given by the matrix

$$M_{aba'b'} := \begin{pmatrix} 1 & ab & a'b' & -aa' \\ ab & 1 & aa' & a'(a'-b') \\ a'b' & aa' & 1 & a(a-b) \\ -aa' & a'(a'-b') & a(a-b) & 1 \end{pmatrix}. \tag{2}$$

Remark 2.2. The reader should keep in mind that the matrix in Equation (2) is supposed to be giving a linear map from $\mathbb{F}_2^4$ to $(k^*/k^{*2})^4$. Thus, the entries of the matrix (although written as elements of k) represent classes of k^*/k^{*2}, and the null space of the matrix is a subspace of $\mathbb{F}_2^4$.

Proof of Proposition 2.1. The equality on the left hand side expresses the absence of algebraic Brauer classes, which is shown in [25, Proposition 3.5.i]. The isomorphism on the right is established by combining [25, Propositions 3.5.ii and 3.5.iii] with [25, Lemma 3.6]. The reader might want to compare [25, Proposition 3.7]. □

Consider the case where k is algebraically closed. Then the Kummer sequence induces a short exact sequence

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

We have $\dim_{\mathbb{F}_2} \mathrm{Pic}(S)/2\,\mathrm{Pic}(S) = 16 + \dim_{\mathbb{F}_2} \mathrm{NS}(E \times E')/2\,\mathrm{NS}(E \times E') = 18$ and $\dim_{\mathbb{F}_2} H^2_{\text{ét}}(S, \mu_2) = 22$. This explains why $\mathrm{Br}(S)_2 \cong \mathbb{F}_2^4$. More canonically, there are isomorphisms

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

Remark 2.3. If k is a field of characteristic zero, the assumption that the 2-torsion points are defined over k implies that $\mathrm{Gal}(\bar{k}/k)$ operates trivially on $\mathrm{Br}(S_{\bar{k}})_2$. We see explicitly that

$$\mathrm{Br}(S)_2/\,\mathrm{Br}(k)_2 \subsetneqq \mathrm{Br}(S_{\bar{k}})_2^{\mathrm{Gal}(\bar{k}/k)} \cong \mathbb{F}_2^4,$$

in general.

Assume that k is algebraically closed. For two rational functions $f, g \in k(S)$, we denote by (f, g) the quaternion algebra

$$k(S)\{I, J\}/(I^2 - f, J^2 - g, IJ + JI)$$

over $k(S)$. Cohomologically, f and g define classes in $H^1(\mathrm{Gal}(\overline{k(S)}/k(S)), \mu_2)$ via the Kummer sequence. The Brauer class of (f, g) is the cup product of these two classes in

$$\begin{aligned} H^2(\mathrm{Gal}(\overline{k(S)}/k(S)), \mu_2^{\otimes 2}) &= H^2(\mathrm{Gal}(\overline{k(S)}/k(S)), \mu_2) \\ &\subseteq H^2(\mathrm{Gal}(\overline{k(S)}/k(S)), \overline{k(S)}^*). \end{aligned}$$

The symbol $(\cdot, \cdot)$ is thus bilinear and symmetric.

Fact 2.4. *Let k be an algebraically closed field of characteristic 0, let a, b, a', b' be elements of k, and let S be as in Proposition 2.1. Then, in terms of the canonical injection $\mathrm{Br}(S) \hookrightarrow \mathrm{Br}(k(S))$, a basis of $\mathrm{Br}(S)_2$ is given by the four quaternion algebras*

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

for $\mu \in \{0, a\}$ and $\nu \in \{0, a'\}$. Here the standard vectors in $\mathbb{F}_2^4$ correspond to these four algebras. More precisely, e_1 corresponds to $A_{a,a'}$, e_2 to $A_{a,0}$, e_3 to $A_{0,a'}$, and e_4 to $A_{0,0}$.

Proof. This is [25, Lemma 3.6] together with [25, formula (20)]. □

Remark 2.5. Using bilinearity, we find for nine of the 15 nontrivial classes a description as a single quaternion algebra, similar to the type above. For the six classes corresponding to the vectors $(1,0,0,1)$, $(0,1,1,0)$, $(1,1,1,0)$, $(1,1,0,1)$, $(1,0,1,1)$, and $(0,1,1,1)$, we need at least two such algebras.

Observations 2.6 (Isomorphy, twisting).

(i) We may replace (a,b) by $(-a,b-a)$ or $(-b,a-b)$ without changing S, and similarly for (a',b'). Indeed, these substitutions simply come from applying the translations $\mathbf{A}^1_k \to \mathbf{A}^1_k$ given by $x \mapsto x-\mu$, for $\mu = a,b$.

(ii) It is also possible to replace (a,b,a',b') with the vector $(\lambda^2 a, \lambda^2 b, a', b')$ or the vector $(\lambda a, \lambda b, \lambda a', \lambda b')$, for $\lambda \in k$. The reason is that the twist

$$E^{(\lambda)} : \lambda y^2 = x(x-a)(x-b)$$

is isomorphic to the elliptic curve given by $Y^2 = X(X-\lambda a)(X-\lambda b)$.

One hypothesis of Proposition 2.1 is that $E_{\bar{k}}$ and $E'_{\bar{k}}$ are not isogenous. Only minor modifications to the proposition are necessary to deal with the case when these curves *are* isogenous. The isogeny causes $\mathrm{NS}(E_{\bar{k}} \times E'_{\bar{k}})/2\,\mathrm{NS}(E_{\bar{k}} \times E'_{\bar{k}})$ to have dimension higher than two, so the homomorphism $\mathbb{F}_2^4 \cong \mathrm{Hom}(E[2], E'[2]) \to \mathrm{Br}(S_{\bar{k}})_2$ is only a surjection, not a bijection.

Over a non-algebraically closed field, the situation is as follows. If E and E' are isogenous over k then $\dim_{\mathbb{F}_2} \mathrm{Pic}(S)/2\,\mathrm{Pic}(S) > 16+2 = 18$. As the additional generator evaluates trivially, it will be found in $\ker M_{aba'b'}$ [25, Lemma 3.6]. Thus, the homomorphism $\ker M_{aba'b'} \twoheadrightarrow \mathrm{Br}(S)_2/\mathrm{Br}(k)_2$ has a nontrivial kernel.

An isogeny defined over a proper field extension l/k causes the same effect over l, but not over k. As $\mathrm{Pic}(S)/2\,\mathrm{Pic}(S) \subsetneq \mathrm{Pic}(S_l)/2\,\mathrm{Pic}(S_l)$, it may, however, happen that a Brauer class is annihilated by the extension l/k; that is, that a vector in $\ker M_{aba'b'}$ describes an *algebraic* Brauer class. By the Hochschild-Serre spectral sequence, we have $H^2_{\text{ét}}(S,\mu_2)/\mathrm{Br}(k)_2 \subseteq H^2_{\text{ét}}(S_{\bar{k}},\mu_2)$. Hence, there are no other algebraic 2-torsion Brauer classes than these.

The transcendental Brauer-Manin obstruction.

Lemma 2.7. *Let k be a local field of characteristic zero, let $E : y^2 = x(x-a)(x-b)$ and $E' : v^2 = u(u-a')(u-b')$ be elliptic curves over k with all 2-torsion points defined over k, and let $S := \mathrm{Kum}(E \times E')$, given explicitly by*

$$z^2 = x(x-a)(x-b)u(u-a')(u-b'). \tag{3}$$

Let $\alpha \in \mathrm{Br}(S)_2$ be a Brauer class, represented by an Azumaya algebra over $k(S)$ of the type $\bigotimes_i A_{\mu_i,\nu_i}$. Then the local evaluation map $\mathrm{ev}_\alpha : S(k) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is given

by

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

Here $(\cdot,\cdot)_k$ *denotes the* k*-Hilbert symbol* [2, Chapter 1, §6].

Proof. By definition, $\mathrm{ev}_\alpha((x,u;z))=\mathrm{inv}(\alpha|_{(x,u;z)})$. Further, $\alpha|_{(x,u;z)}$ is the Azumaya algebra $\bigotimes_i((x-\mu_i)(x-b),(u-\nu_i)(u-b'))$ over k. Now observe that the quaternion algebra (s,t) splits if and only if t is a norm from $k(\sqrt{s})$. This is tested by the norm residue symbol $(t,k(\sqrt{s})/k)$, which agrees with the classical Hilbert symbol $(s,t)_k$. □

Remarks 2.8.

(i) For us, the Hilbert symbol takes values in $(\frac{1}{2}\mathbb{Z}/\mathbb{Z},+)$. This differs from the classical setting, where the values are taken in $(\{\pm1\},\cdot)$.

(ii) According to Proposition 2.1, $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2\subseteq\mathbb{F}_2^4$. Further, by Fact 2.4, we have an explicit basis, which is given by Azumaya algebras; that is, for each class in $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2$, we chose a lift to $\mathrm{Br}(S)_2$. For k a local field, this lift is normalized such that $\mathrm{ev}_\alpha((\infty,\infty;\cdot))=0$. Indeed, for x close to ∞ in k, $(x-\mu)(x-b)$ is automatically a square.

The next lemma shows that the evaluation map is constant near the singular points.

Lemma 2.9. *Let* $p>2$ *be a prime number, and let* a,b,a',b' *be elements of* $\mathbb{Z}_p$ *such that* $E:y^2=x(x-a)(x-b)$ *and* $E':v^2=u(u-a')(u-b')$ *are elliptic curves that are not isogenous to each other. Suppose that*

$$\min(v_p(a),v_p(b))=\min(v_p(a'),v_p(b'))=0$$

and put

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

Consider the surface S *over* $\mathbb{Q}_p$ *defined 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*

$$T:=\big\{(x,u;z)\in S(\mathbb{Q}_p)\;\big|\;v_p(x)<0\text{ or }v_p(u)<0\big\}\cup\bigcup_{\substack{\mu\in\{0,a,b\}\\ \nu\in\{0,a',b'\}}}\big\{(x,u;z)\in S(\mathbb{Q}_p)\;\big|\;x\equiv\mu,u\equiv\nu\pmod{p^{l+1}}\big\}$$

depicted in Figure 1.

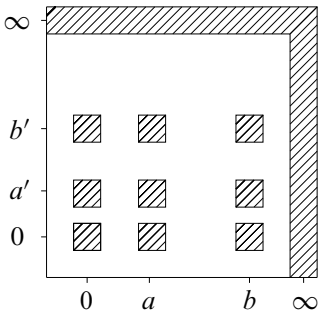

Figure 1. The set T.

Proof. It suffices to prove the lemma for α ranging over a lift to $\mathrm{Br}(S)_2$ of a basis for $\mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q}_p)_2$; we will use the basis given in Fact 2.4. We first consider the basis element e_1, corresponding to the Hilbert symbol $((x-a)(x-b),(u-a')(u-b'))_p$. We will show that if ab and $a'b'$ and $-aa'$ are all squares, then the Hilbert symbol will be 0 on the set T.

Using the equation of the surface, we see that

$$\begin{aligned}((x-a)(x-b),(u-a')(u-b'))_p &= ((x-a)(x-b),-xu)_p \\ &= (-xu,(u-a')(u-b'))_p.\end{aligned} \tag{4}$$

Let us distinguish three cases. In all cases, we observe that a Hilbert symbol is zero when at least one of its arguments is a square.

First case. Suppose that either $v_p(x)<0$ or $v_p(u)<0$. If the first condition holds, then $(x-a)(x-b)$ is a square, while if the second condition holds, then $(u-a')(u-b')$ is a square. Thus the Hilbert symbol is 0 in this case.

Second case. Suppose that $x\equiv 0$ or $u\equiv 0 \pmod{p^{l+1}}$.

If $x\equiv 0 \pmod{p^{l+1}}$ then $(x-a)(x-b)\equiv ab \pmod{p^{l+1}}$. Since

$$v_p(ab)=v_p(a)+v_p(b)=\max(v_p(a),v_p(b))\le l,$$

the numbers $(x-a)(x-b)$ and ab belong to the same square class. Thus, if ab is a square, the Hilbert symbol will be 0.

Analogously, if $u\equiv 0 \pmod{p^{l+1}}$ then $(u-a')(u-b')\equiv a'b' \pmod{p^{l+1}}$, so that $(u-a')(u-b')$ is in the square class of $a'b'$. It follows that if $a'b'$ is a square, the Hilbert symbol will be 0.

Third case. Suppose that $x\equiv\mu$ and $u\equiv\nu \pmod{p^{l+1}}$ where $\mu\in\{a,b\}$ and $\nu\in\{a',b'\}$.

Suppose, for example that $x\equiv a \pmod{p^{l+1}}$ and $u\equiv a' \pmod{p^{l+1}}$. Then, in particular, $x\equiv a \pmod{p^{v(a)+1}}$ and $u\equiv a' \pmod{p^{v(a')+1}}$. This implies that $-xu\equiv -aa' \pmod{p^{v(a)+v(a')+1}}$ so that $-xu$ is in the square class of $-aa'$. In

particular, if $-aa'$ is a square then the Hilbert symbol is 0. The other possibilities for the residue classes of x and u yield the square classes of $-ab'$, $-ba'$, and $-bb'$, which are all trivial when ab, $a'b'$, and $-aa'$ are squares.

We see that the evaluation map is constant on the set T if and only if the vector

$$(1, ab, a'b', -aa')^t \in (\mathbb{Q}_p^*/\mathbb{Q}_p^{*2})^4$$

is zero. This is exactly the first column of the matrix $M_{aba'b'}$ given in Equation (2).

For the Hilbert symbols $((x-a)(x-b), u(u-b'))_p$, $(x(x-b), (u-a')(u-b'))_p$, and $(x(x-b), u(u-b'))_p$, the calculations are completely analogous. They lead to the second, third, and fourth columns of $M_{aba'b'}$.

Hence we see that, for a combination of Hilbert symbols, the evaluation map is constant on the set T if and only if it represents a Brauer class. □

Remarks 2.10.

(i) In Lemma 2.9, the assumption that

$$\min(v_p(a), v_p(b)) = \min(v_p(a'), v_p(b')) = 0$$

is not a restriction in view of Remark 2.16(i), below.

(ii) A result similar to Lemma 2.9 holds for $p = 2$ as well; however, the condition in the first set in the definition of T must be strengthened to $v_2(x) < -2$ or $v_2(u) < -2$, and the congruences in the other sets in the definition of T must be taken modulo 2^{l+3}. The proof is essentially the same.

Proposition 2.11. *Let k be either $\mathbb{R}$ or the field $\mathbb{Q}_p$ for a prime p. Let $E : y^2 = x(x-a)(x-b)$ and $E' : v^2 = u(u-a')(u-b')$ be elliptic curves over k with all 2-torsion points defined over k, and let $S := \mathrm{Kum}(E \times E')$ be the corresponding Kummer surface. Suppose that E and E' are not isogenous to one another, and that both E and E' have good reduction if $k = \mathbb{Q}_p$. Then for every $\alpha \in \mathrm{Br}(S)_2$, the evaluation map $\mathrm{ev}_\alpha : S(k) \to \mathbb{Q}/\mathbb{Z}$ is constant.*

Proof. First suppose that $k = \mathbb{Q}_p$. Then the assertion of the lemma is a particular case of a very general result [6, Proposition 2.4] due to J.-L. Colliot-Thélène and A. N. Skorobogatov. (Using Lemma 2.9 and elementary properties of the Hilbert symbol, one could also provide an elementary argument that is specific for the present situation.)

Next, suppose that $k = \mathbb{R}$. Without loss of generality, we may assume that $a > b > 0$ and $a' > b' > 0$. Then it will suffice to prove the assertion for representatives of e_2 and e_3, that is, for $((x-a)(x-b), u(u-b'))_{\mathbb{R}}$ and $(x(x-b), (u-a')(u-b'))_{\mathbb{R}}$.

Consider e_2. Suppose $(x, u; z)$ is an $\mathbb{R}$-rational point on the model of S given by Equation (3). If $((x-a)(x-b), u(u-b'))_{\mathbb{R}} = \frac{1}{2}$ then $(x-a)(x-b) < 0$ and

$u(u-b') < 0$. Hence, $b < x < a$ and $0 < u < b'$. But then

$$z^2 = x(x-a)(x-b)u(u-a')(u-b') < 0,$$

a contradiction. Thus, the evaluation map is constant.

For e_3, the argument is analogous. □

Algorithm 2.12.

Input: Integers a, b, a', and b'; a prime number p; and a Brauer class $\alpha \in \mathrm{Br}(S)_2$ for the surface

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

given as a combination of Hilbert symbols.

Output: The coloring of $S(\mathbb{Q}_p)$ defined by $\mathrm{ev}_\alpha : S(\mathbb{Q}_p) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

1. Calculate $l := \max(v_p(a), v_p(b), v_p(a-b), v_p(a'), v_p(b'), v_p(a'-b'))$, the bound established in Lemma 2.9.
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
$$\{(x, u; z) \in S(\mathbb{Q}_p) \mid v_p(x - x_0) \geq e, v_p(u - u_0) \geq e\}.$$
3. Run through S_2. For each element (x_0, u_0, p^e), execute the following operations.
   (a) Test whether the corresponding set is nonempty. If not, delete the element (x_0, u_0, p^e).
   (b) If $e \geq l+1$ and $v_p(x-\mu) \geq l+1$ for some $\mu \in \{0, a, b\}$, and $v_p(u-\nu) \geq l+1$ for a $\nu \in \{0, a', b'\}$, then move (x_0, u_0, p^e) to S_0.
   (c) Test naïvely, 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, depending on whether the value is 0 or $\frac{1}{2}$.
   (d) Otherwise, replace (x_0, u_0, p^e) by the p^2 triples $(x_0 + i p^e, u_0 + j p^e, p^{e+1})$ 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.

Example 2.13. Consider the Kummer surface S over $\mathbb{Q}$ given by

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

Then weak approximation is violated on S.

Proof. This is caused by a transcendental Brauer-Manin obstruction. In fact, the matrix (2) is

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

and its kernel is $\langle e_1 \rangle$. Hence there is a transcendental Brauer class on S, represented by the quaternion algebra $((x-1)(x-25), (u+25)(u+36))$.

Now the argument is completely elementary. For every $(x, u; z) \in S(\mathbb{Q}_p)$ with $z \neq 0$, one has

$$\sum_p ((x-1)(x-25), (u+25)(u+36))_p = 0,$$

according to the sum formula for the Hilbert symbol. The bad primes of the elliptic curves $y^2 = x(x-1)(x-25)$ and $y^2 = x(x+25)(x+36)$ are 2, 3, 5, and 11. Hence, the sum is actually only over these four primes.

Our implementation of Algorithm 2.12 shows that the local evaluation map is constant at the primes 2, 3, and 11, but not at 5. Hence, 5-adic points such that $((x-1)(x-25), (u+25)(u+36))_5 = \frac{1}{2}$ may not be approximated by $\mathbb{Q}$-rational ones.

Examples of such 5-adic points include those with $(x, u) = (2, 5)$. Indeed,

$$2 \cdot (2-1) \cdot (2-25) \cdot 5 \cdot (5+25) \cdot (5+36) = -11316 \cdot 5^2$$

is a 5-adic square, but $(2-1) \cdot (2-25) = -23$ is a nonsquare and $v_5((5+25) \cdot (5+36)) = 1$ is odd. □

Remarks 2.14.

(i) The constancy of the local evaluation maps at 3 and 11 and the nonconstancy at 5 also follow from the criterion formulated as Theorem 2.19 below.

(ii) In the coloring obtained on $S(\mathbb{Q}_5)$, all the points such that $x, u \not\equiv 0 \pmod 5$ have color zero. This is rather different from the colorings typically obtained from an algebraic Brauer class. The reader should compare the situation described in [5], where, on the cone over an elliptic curve, three sets of equal sizes appear.

Normal form, ranks, asymptotics. Let k be a field, let a, b, a', and b' be elements of k^* with $a \neq b$ and $a' \neq b'$, and let S be the Kummer surface

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

There are two types of nontrivial 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 $M_{aba'b'}$. As seen in Observations 2.6(i), a suitable translation of $\mathbf{A}^1 \times \mathbf{A}^1$ transforms the surface into an isomorphic one with kernel vector e_1. Then ab, $a'b'$, and $-aa'$ are squares in k. Note that this implies that $-ba'$, $-ab'$, and $-bb'$ are squares as well.

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 an isomorphic one with kernel vector $e_2 + e_3$. Then aa', bb', and $(a-b)(a'-b')$ are squares.

Corollary 2.15. *Let p be a prime number, let a, b, a', and b' be elements of $\mathbb{Q}_p^*$ with $a \neq b$ and $a' \neq b'$, and let S be the Kummer surface*

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

Suppose that $\nu_p(a) \leq \nu_p(b)$, that $\nu_p(a') \leq \nu_p(b')$, and that $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \neq 0$. Then $\nu_p(aa')$ is even.

Proof. The assertion is that the expression

$$m := \min(\nu_p(a), \nu_p(b), \nu_p(a-b)) + \min(\nu_p(a'), \nu_p(b'), \nu_p(a'-b'))$$

is even as soon as $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \neq 0$. As m is invariant under translations as described in Observations 2.6(i), we may suppose that either e_1 or $e_2 + e_3$ lies in $\ker M_{aba'b'}$. In both cases the assertion is easily checked. Note that either minimum is adopted by at least two of the three valuations. □

Remarks 2.16.

(i) Suppose $k = \mathbb{Q}_p$. Then, by Observations 2.6(ii), we may assume without loss of generality that $a, b, a', b' \in \mathbb{Z}_p$, that $\min(\nu_p(a), \nu_p(b)) = 0$, and that $\min(\nu_p(a'), \nu_p(b')) = 0, 1$. By Corollary 2.15, the assumption that $M_{aba'b'}$ has a nontrivial kernel ensures that $\min(\nu_p(a'), \nu_p(b')) = 0$, too.

(ii) Suppose that $k = \mathbb{Q}$ and that there is a Brauer class of type 1. Reasoning as in the preceding remark, we see that we may suppose that a, b, a', and b' are integers with $\gcd(a, b) = \gcd(a', b') = 1$. Hence there is a normal form with $a > b$, with $a' < b'$, and with $a, b, -a', -b' \in \mathbb{Z} \cap \mathbb{Q}^{*2}$. Up to the involution $(a, b, a', b') \mapsto (-a', -b', -a, -b)$, this normal form is unique. The geometric interpretation of this involution is that it interchanges the two elliptic curves and twists them both by -1.

Proposition 2.17. *Let k be a field of characteristic zero, let $E : y^2 = x(x-a)(x-b)$ and $E' : v^2 = u(u-a')(u-b')$ be elliptic curves over k with all 2-torsion points defined over k, and let $S := \mathrm{Kum}(E \times E')$ be the corresponding Kummer surface. Suppose that E and E' are not isogenous to each other.*

(i) *We have* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \le 4$ *and* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \ne 3$. *Further*, $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = 4$ *is possible only when* -1 *is a square in* k.

(ii) *Suppose* $k = \mathbb{Q}_p$ *for a prime* p. *If both* E *and* E' *have potential good reduction then* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2$ *is even.*

(iii) *If* $k = \mathbb{R}$ *then* $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = 2$.

Proof. All of these assertions will follow from Proposition 2.1. Recall that $M_{aba'b'}$ is a matrix with entries in the $\mathbb{F}_2$-vector space k^*/k^{*2}.

Statement (i): The inequality $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \le 4$ is clear. If the vector space had dimension three, the matrix $M_{aba'b'}$ would have column rank one. But this is impossible for a symmetric matrix having zeroes on the diagonal. Further, $\dim \mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = 4$ requires $M_{aba'b'}$ to be the zero matrix. In particular, aa' and $-aa'$ both have to be squares in k. This implies that -1 is a square, too.

Statement (ii): Standard considerations (see [23, Proposition VII.5.5], for example) show that the elliptic curve given by $y^2 = x(x-\mu)(x-\nu)$ has potential good reduction if and only if $\mu/\nu \in \mathbb{Z}_p^*$ and $\mu/\nu \not\equiv 1 \pmod p$. This implies, in particular, that $p > 2$.

If $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2 = 0$ the assertion is trivially true, so let us assume that $\mathrm{Br}(S)_2/\mathrm{Br}(k)_2 \ne 0$. Then, by Remark 2.16(i), we may assume that the elements $a, b, a-b, a', b', a'-b'$ all lie in $\mathbb{Z}_p^*$. But for p-adic units, being a square in $\mathbb{Q}_p$ or not is tested by the Legendre symbol. Thus $M_{aba'b'}$ is essentially an alternating matrix with entries in $\mathbb{F}_2$. Such matrices have even rank.

Statement (iii): After applying one of the translations $\mathbf{A}^1 \times \mathbf{A}^1 \to \mathbf{A}^1 \times \mathbf{A}^1$ given by $(x,u) \mapsto (x-\mu, u-\nu)$ for $\mu \in \{0,a,b\}$ and $\nu \in \{0,a',b'\}$, we may assume that $a > b > 0$ and $a' > b' > 0$. Then

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

has kernel $\langle e_2, e_3 \rangle$. □

Remarks 2.18. We discuss some asymptotic estimates for the number of surfaces with Brauer groups of various types.

(i) Let $N > 0$. Then the number of pairs (a,b) such that a and b are perfect squares, $a < b$, and $a, b-a < N$ is asymptotically CN for

$$C := \tfrac{1}{2}\big(\log(\sqrt{2}+1) + \sqrt{2} - 1\big).$$

Indeed, the Stieltjes integral

$$\int_1^N \big(\sqrt{x+N} - \sqrt{x}\big)\, d\sqrt{x}$$

has exactly this behavior. Assuming that isogenies are rare, we find that the number of surfaces over $\mathbb{Q}$ with integer parameters of absolute value at most N and a 2-torsion Brauer class of type 1 is asymptotically

$$\frac{1}{2}\left(\frac{6}{\pi^2}\right)^2 C^2 N^2 \approx 0.077544 N^2.$$

(ii) On the other hand, a 2-torsion Brauer class of type 2 yields a $\mathbb{Q}$-rational point on the intersection of three quadrics in $\mathbf{P}^6$. The Manin conjecture leads to the naïve expectation of growth of the type $cN\log^d N$ for some integer $d \geq 0$.

(iii) The number of all Kummer surfaces of the form considered and with parameters up to N is $O(N^4)$. Thus, only a very small fraction have a nontrivial 2-torsion Brauer class.

Even fewer surfaces should have odd torsion in their Brauer group. Indeed, for l-torsion, one must have

$$\mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(E[l], E'[l]) \neq 0$$

(see [25, Proposition 3.3]). Consequently, $\#E(\mathbb{F}_p) \equiv \#E'(\mathbb{F}_p) \pmod{l}$ for every prime $p \neq l$ that is good for both E and E'. Based on this, our computations show that, up to $N = 200$, no surface has an l-torsion Brauer class for $l \geq 5$. Further, at most eight pairs of j-invariants allow a 3-torsion Brauer class.

(iv) It is possible over $\mathbb{Q}$ to have a 2-dimensional 2-torsion Brauer group. For this, in the normal form of Remark 2.16(ii), one needs that $a-b$ and $b'-a'$ are perfect squares. Further, these surfaces have four normal forms instead of two, as there are two Brauer classes of type 1. These examples correspond to pairs of Pythagorean triples, and we therefore have two Kummer surfaces, differing from each other by a twist by (-1). The asymptotics of Pythagorean triples [1] shows that there are asymptotically

$$\frac{4}{\pi^4}\log^2(1+\sqrt{2})N \approx 0.031899 N$$

surfaces over $\mathbb{Q}$ with integer parameters of absolute value at most N and a Brauer group of dimension two.

(v) Some actual numbers are listed in Table 1. For a precise description of the sample, see Section 4B below.

Trivial evaluation.

Theorem 2.19. *Let $p > 2$ be a prime number and let a, b, a', b' be nonzero elements of $\mathbb{Z}_p$ such that $a \neq b$ and $a' \neq b'$. Let S be the Kummer surface given*

Bound	Dimension 2	Dimension 1, type 1		Dimension 1, type 2	
		Total	Algebraic	Total	Algebraic
50	0	183	1	38	0
100	0	766	2	98	0
200	2	3049	3	367	0
500	12	18825	4	1457	0
1000	20	77249	8	4398	0
2000	42	305812	11	12052	0

Table 1. Number of surfaces with bounded parameters whose Brauer groups have 2-torsion of various types. The first column gives the bound N on the parameters of the surfaces we computed; see Section 4B for a precise description of the parameters allowed. The remaining columns give the number of such surfaces whose Brauer groups have 2-torsion subgroups of dimension 2, of dimension 1 and type 1, and of dimension 1 and type 2. For the 1-dimensional cases, the number of algebraic classes is listed as well.

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.*

(i) *Suppose that either* $a \equiv b \not\equiv 0 \pmod p$ *or* $a' \equiv b' \not\equiv 0 \pmod p$. *Then the evaluation map* $\mathrm{ev}_\alpha : S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ *is constant.*

(ii) *If* $a \not\equiv b \pmod p$ *and* $a' \not\equiv b' \pmod p$, *and if not all four numbers are* p*-adic units, then the evaluation map* $\mathrm{ev}_\alpha : S(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ *is nonconstant.*

Proof. First step: *Preparations.* We are interested in the Hilbert symbol

$$((x-a)(x-b), (u-a')(u-b'))_p.$$

Recall that a/b, a'/b', and $-bb'$ are all squares in $\mathbb{Q}_p$.

A $\mathbb{Q}_p$-rational point on S corresponds to a pair of points on the elliptic curves $\lambda y^2 = x(x-a)(x-b)$ and $\lambda v^2 = u(u-a')(u-b')$ for a common value of λ. The Hilbert symbol then simplifies to $(\lambda x, \lambda u)_p$.

Second step: 2*-descent.* By 2-descent (see for example [23, Proposition X.1.4]), the elliptic curve $E : Y^2 = X(X-a)(X-b)$ has a point in the square class of x if and only if the system

$$xz_1^2 - tz_2^2 = a$$
$$xz_1^2 - xtz_3^2 = b$$

is solvable. Eliminating t, we obtain $x^2 z_1^2 z_3^2 - xz_1^2 z_2^2 = axz_3^2 - bz_2^2$, which gives

$$(xz_3^2 - z_2^2)(xz_1^2 - b) = (a-b)xz_3^2.$$

Dividing by $-bxz_3^2$ yields

$$\left(1-\frac{z_2^2}{z_3^2}\frac{1}{x}\right)\left(1-\frac{z_1^2}{b}x\right)=1-\frac{a}{b}.$$

In other words, E has a point in the square class of x if and only if the equation $(1-v^2x)(1-w^2x/b)=1-a/b$ is solvable.

Third step: *Application to the Kummer surface* S. As $\lambda y^2=x(x-a)(x-b)$ is equivalent to $y'^2=\lambda x(\lambda x-\lambda a)(\lambda x-\lambda b)$ and b and $-b'$ are squares, we see that S has a point with coordinates in the square classes of x and u if and only if

$$(1-v^2\lambda x)(1-w^2x/b)=1-a/b$$
$$(1-v'^2\lambda u)(1-w'^2x/b')=1-a'/b'$$

has a solution $(v,w,v',w',\lambda)\in(\mathbb{Q}_p^*)^5$.

Proof of (i): Without loss of generality, assume that $a\equiv b\not\equiv 0 \pmod p$ and $a'/b'\in\mathbb{Z}_p$. Let $(x,u;z)\in S(\mathbb{Q}_p)$ be any point such that $z\neq 0$.

Then Lemma 2.21(i) (below) shows that $(u/b',\lambda u)_p=0$. Furthermore, by Lemma 2.21(iii), at least one of x/b and λx is a square in $\mathbb{Q}_p$. In the case $\lambda x\in\mathbb{Q}_p^{*2}$, the assertion $(\lambda x,\lambda u)_p=0$ is clearly true. If $x/b\in\mathbb{Q}_p^{*2}$ then

$$0=(u/b',\lambda u)_p=(-\lambda/b',\lambda u)_p=((\lambda x)/(-bb'),\lambda u)_p=(\lambda x,\lambda u)_p.$$

Proof of (ii): Again without loss of generality, assume that $p^2\mid a$, that b is a unit, and that $a'/b'\in\mathbb{Z}_p$. We claim that, for $\lambda=-b$, there is a point on S such that $x=p$ and $2\mid v_p(u)$, so that $\lambda u=-bu$ is a nonsquare.

Indeed, it is obvious that $-bp(p-a)(p-b)\in\mathbb{Q}_p^{*2}$. Further, by Hensel's Lemma, it suffices to find a pair $(U_1,U_2)\in\mathbb{F}_p^*\times\mathbb{F}_p^*$ of nonsquares such that $(1-U_1)(1-U_2)=1-\overline{a}'/\overline{b}'$. For this, a counting argument applies. In fact, each $U_1\in\mathbb{F}_p\setminus\{0,1,\overline{a}'/\overline{b}'\}$ uniquely determines its partner. As this set contains $(p-1)/2$ nonsquares and only $(p-5)/2$ squares, the assertion follows. □

Remarks 2.20.

(i) It might seem strange to use a descent argument over a local field. It seems to us, however, that a direct argument is neither more elegant nor shorter.

(ii) Using the descent argument above, we also recover the constancy of the evaluation map in the case of good reduction. Indeed, Lemma 2.21(ii) implies that either at least one of x/b and λx is a square, or both have even valuation. The first two cases are dealt with as above. Otherwise, λb is a square, hence $-\lambda/b'$ is a square, too, and one has to show that $2\mid v_p(\lambda u)$. But this is implied by Lemma 2.21(ii) when looking at the second equation.

Lemma 2.21. *Let $p > 2$ be a prime number, let A and B be nonzero elements of $\mathbb{Q}_p$, and let $Q \in \mathbb{Q}_p^*$ be a square. Suppose that the equation $(1-Av^2)(1-Bw^2) = 1-Q$ is solvable in $\mathbb{Q}_p^* \times \mathbb{Q}_p^*$.*

(i) *We have $(A, B)_p = 0$.*

(ii) *If $Q \in \mathbb{Z}_p^*$ then either $A \in \mathbb{Q}_p^{*2}$, or $B \in \mathbb{Q}_p^{*2}$, or both A and B are of even valuation.*

(iii) *If $Q \in \mathbb{Z}_p^*$ and $Q \equiv 1 \pmod{p}$ then either $A \in \mathbb{Q}_p^{*2}$ or $B \in \mathbb{Q}_p^{*2}$.*

Proof. Statement (i): We have that $Av^2 + Bw^2 - AB(vw)^2$ is a square. When all three summands are of the same valuation, they must be units. The assertion is then clearly true. Otherwise, at most two of the three summands have minimal valuation. Then their sum is a square, too. According to the definition of the Hilbert symbol [2, p. 55], we have either $(A, B)_p = 0$ or $(A, -AB)_p = 0$ or $(B, -AB)_p = 0$. These three statements are equivalent to each other.

Statement (ii): We have $\nu_p(1 - Q) \geq 0$. On the other hand, if both A and B are nonsquares then $\nu_p(1 - Av^2), \nu_p(1 - Bw^2) \leq 0$. This implies equality, hence $Av^2, Bw^2 \in \mathbb{Z}_p$. Both must be units as $Av^2 + Bw^2 - AB(vw)^2$ is, by assumption, a square in $\mathbb{Z}_p^*$.

Statement (iii): If A and B were both nonsquares then $\nu_p(1 - Av^2) \leq 0$ and $\nu_p(1 - Bw^2) \leq 0$. As $\nu_p(1 - Q) > 0$, this is a contradiction. □

Experiments with Algorithm 2.12 show that surprisingly often there are nontrivial Brauer classes with trivial p-adic evaluation. This is partially explained by the following result.

Theorem 2.22. *Let $p > 2$ be a prime number and let $a, b, a', b' \in \mathbb{Q}_p$ be such that $E : y^2 = x(x-a)(x-b)$ and $E' : v^2 = u(u-a')(u-b')$ are elliptic curves. Suppose that E and E' are not isogenous to each other, and let S be the corresponding Kummer surface.*

(i) *If $\dim \mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q}_p)_2 \geq 2$ then there is a nonzero $\alpha \in \mathrm{Br}(S)_2$ such that ev_α is the zero map.*

(ii) *If $\dim \mathrm{Br}(S)_2/\mathrm{Br}(\mathbb{Q}_p)_2 = 4$ then the subspace of classes with constant evaluation map is of dimension 4 when both E and E' have potential good reduction. The dimension is 3 when neither curve has potential good reduction and 2 in the mixed case.*

Proof. By Remark 2.16(i), we may assume without loss of generality that a and b lie in $\mathbb{Z}_p$ and are not both divisible by p, and that the same holds for a' and b'. The case in which both E and E' have potential good reduction has already been treated in Proposition 2.11.

Statement (ii). If neither curve has potential good reduction, we can apply a translation of $\mathbf{A}^1 \times \mathbf{A}^1$, as in Observations 2.6(i), to reduce to the case $a \equiv b \not\equiv 0 \pmod{p}$ and $a' \equiv b' \not\equiv 0 \pmod{p}$. Then, by virtue of Theorem 2.19(ii), the Brauer classes corresponding to $\langle e_1, e_2, e_3 \rangle$ have constant evaluation maps, but ev_{e_4} is nonconstant.

Further, when only E' has potential good reduction, the same arguments show that the Brauer classes corresponding to $\langle e_1, e_2 \rangle$ have constant evaluation maps, while those of e_3, e_4, and $e_3 + e_4$ are nonconstant.

Statement (i). Only the case that at least one of the curves E and E' does not have potential good reduction requires a proof. Hence, we may assume that $a, b \in \mathbb{Z}_p$ and $a \equiv b \not\equiv 0 \pmod{p}$. Then $ab \in \mathbb{Q}_p^{*2}$.

The upper left 2×2-block of $M_{aba'b'}$ is zero. If the block $\left(\begin{smallmatrix} a'b' & aa' \\ -aa' & a'(a'-b') \end{smallmatrix}\right)$ occurring in the lower left has trivial kernel then the 2×2-block in the upper right is certainly not the zero matrix. Therefore $\dim \ker M_{aba'b'} \leq 1$, a contradiction. Thus, there is a Brauer class represented by a vector from $\langle e_1, e_2 \rangle$. By Theorem 2.19(i), its evaluation map is constant. □

3. A point search algorithm for special Kummer surfaces

The surfaces we are studying are double covers of $\mathbf{P}^1 \times \mathbf{P}^1$, given by equations of the form

$$w^2 = f_{ab}(x, y) f_{a'b'}(u, v).$$

Here, f_{ab} is the binary quartic form $f_{ab}(x, y) := xy(x - ay)(x - by)$. Thus, a point $([x : y], [u : v]) \in (\mathbf{P}^1 \times \mathbf{P}^1)(\mathbb{Q})$ leads to a point on the surface if and only if the square classes of $f_{ab}(x, y)$ and $f_{a'b'}(u, v)$ coincide, or one of them is zero.

We will call the solutions with $f_{ab}(x, y)$ or $f_{a'b'}(u, v)$ zero the *trivial* solutions of the equation. Obviously, there is a huge number of trivial solutions. Our aim is to describe an efficient algorithm that searches for nontrivial solutions and does not care about the trivial ones. In its simplest version, our algorithm works as follows.

Algorithm 3.1 (Point search).

Input: Two sequences $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ of integers and a search bound $B > 0$.

Output: All solutions of the equations

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

for which x, y, u, and v are integers 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 squarefree 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 $x, y \in \mathbb{Z}$, $|x|, |y| \le B$, and $x, y \neq 0$.
4. For each point $[x : y]$ enumerated, execute the operations below.
   (a) 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}.
   (b) Store the squarefree parts of the factors in $m_1, \dots, m_4$. (Use the table T to compute the squarefree parts.)
   (c) Put
   $$p_1 := \frac{m_1}{\gcd(m_1, m_2)} \frac{m_2}{\gcd(m_1, m_2)}$$
   $$p_2 := \frac{m_3}{\gcd(m_3, m_4)} \frac{m_4}{\gcd(m_3, m_4)}$$
   $$p_3 := \frac{p_1}{\gcd(p_1, p_2)} \frac{p_2}{\gcd(p_1, p_2)}.$$
   Thus, p_3 is a representative of the square class of $f_{a_i b_i}(x, y)$.
   (d) Store the quadruple $(x, y, i, h(p_3))$ in a list. Here, h is a hash function.
5. Sort the list by the last component.
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 3.2.

(i) For practical search bounds B, the first integer overflow occurs when we multiply $p_1/\gcd(p_1, p_2)$ and $p_2/\gcd(p_1, p_2)$. But we can think of this reduction modulo 2^{64} as being a part of our hash function. Note that the final check of $f_{a_i b_i}(x, y) f_{a_{i'} b_{i'}}(x', y')$ being a square can be done without multiprecision integers by inspecting the gcd's of the eight factors.

(ii) One disadvantage of Algorithm 3.1 is obvious. It requires more memory than is reasonably available by present standards. We solved this problem by the

introduction of what we call a *multiplicative paging*. This is an approach motivated by the simple additive paging as described in [8]. In addition, our memory-optimized point search algorithm is based on the following observation.

Lemma 3.3. *Let p be a good prime. Then, for each pair (x, y) with $\gcd(x, y) = 1$, at most one of the factors x, y, $(x - ay)$, and $(x - by)$ is divisible by p.* □

Algorithm 3.4 (Point search using multivariate paging).

Input: The same as in Algorithm 3.1.

Output: The same as in Algorithm 3.1.

1. Compute the bound L and the square-class representatives as in Algorithm 3.1.
2. Compute the upper bound
$$C := 2 \max\{|a_i|, |b_i| \mid i = 1, \ldots, k\}$$
for the possible bad primes.
3. Initialize an array of boolean variables of length L. Use the value `false` for the initialization. We will call this array the *markers* of the factors already treated.
4. In a loop, run over all good primes below L. Start with the biggest prime and stop when the upper bound C is reached; that is, work in *decreasing* order. For each prime p_p, execute the steps below. We call p_p the *page prime*.
   (a) Run over all multiples m of p_p not exceeding L and such that the p_p-adic valuation is odd. For each m, do the following.
      i. Check whether m is marked as already treated. In this case, continue with the next m.
      ii. Test whether x, y, $x - a_i y$, or $x - b_i y$ can represent this value. Here, use the constraints $|x|, |y| \leq B$ and $i \in \{1, \ldots, k\}$.
      iii. For each possible representation with $\gcd(x, y) = 1$, check to see whether x, y, $x - a_i y$, or $x - b_i y$ is marked as already treated. Otherwise, store the quadruples $(x, y, i, h(p_3))$ into a list.
      iv. Mark the value of m as treated and continue with the next m.
   (b) As in Algorithm 3.1, construct all solutions by inspecting the collisions of the hash function.
5. Up to now, all solutions were found such that w has at least one prime factor bigger than the bad primes bound. To get the remaining ones, use Algorithm 3.1 but skip all values of x, y that are marked as treated factors. Further, break step 4 of Algorithm 3.1 early if m_3 or m_4 is marked as treated.

Remark 3.5. The last step computes all solutions in smooth numbers — that is, points such that the square classes of $f_{ab}(x, y)$ and $f_{a'b'}(u, v)$ are smooth with respect to the bad primes bound C defined in step 2. It is an experimental observation that this step takes only a small fraction of the running time, but gives a large percentage of the solutions. The algorithm may easily be modified such that only the solutions in smooth numbers are found. For this, the markers for treated factors have to be initialized in an appropriate way.

4. Some experiments

4A. ***Coloring by covering — a search for regular colorings.*** As noted in the introduction, on various types of surfaces [3; 11], the (algebraic) Brauer-Manin obstruction leads to very regular colorings. Carrying this knowledge over to the special Kummer surfaces given by

$$S: \ w^2 = f_4(x, y)g_4(u, v),$$

one is led to test the following: For a $\mathbb{Q}$-rational point with $w \neq 0$, write $\lambda w_1^2 = f_4(x, y)$ and $\lambda w_2^2 = g_4(u, v)$ and expect the color to be given by the square class of λ.

For p-adic points, this defines a coloring with four or eight colors, depending on whether $p > 2$ or $p = 2$. At the infinite place, the color is given by the sign of λ. Motivated by [3; 11], we assume that the p-adic color of a rational point has a meaning only when p divides the conductor of one of the elliptic curves used to construct S. Further, we restricted ourselves to the square classes of even p-adic valuation (for the primes of bad reduction). This does not exclude all rational points reducing to the singular locus at a bad prime.

Thus, we get a coloring of the $\mathbb{Q}$-rational points with 2^{k+1} colors for a surface with k relevant odd primes. Weak approximation would imply that the color map is a surjection. In the case of a visible obstruction, we would expect that at most half of the possible colors are in the image of the color map.

For a systematic test, we used the 184 elliptic curves with odd conductor and $|a|, |b| < 100$. This led to 16,836 surfaces. Table 2 gives an overview of the number of colors that occurred. The table indicates that our result is negative: It seems that there is no obstruction factoring over such a coloring. We expect that one would find $\mathbb{Q}$-rational points of all colors for a sufficiently large search bound.

On one core of an Intel Core 2 Duo E8300 processor, the running times were 18.5 hours for search bound 30,000 and 275 hours for search bound 100,000, but only 51 minutes for smooth solutions with respect to a bad prime bound of 200 and bound 100,000.

#Bad primes	2	3	4	5	6	7	8
#Surfaces	4	182	1678	5777	7409	1726	60
#Colors	8	16	32	64	128	256	512
$B = 1000$	8	15–16	26–32	32–64	33–127	31–157	27– 81
$B = 3000$	8	16	30–32	49–64	67–128	81–226	92–192
$B = 10000$	8	16	32	57–64	93–128	142–254	207–352
$B = 30000$	8	16	32	62–64	109–128	196–256	303–474
$B = 100000$	8	16	32	64	121–128	232–256	387–505
$B = 10000$, smooth	8	16	31–32	54–64	79–128	99–236	113–197
$B = 30000$, smooth	8	16	32	59–64	92–128	146–253	161–300
$B = 100000$, smooth	8	16	32	61–64	108–128	185–256	230–381

Table 2. Number of colors attained by $\mathbb{Q}$-rational points of bounded height on Kummer surfaces of products of elliptic curves, classified by the number of bad primes and the search bound B. The second row of the table indicates the number of surfaces we analyzed with the given number of bad primes. For each number of bad primes and each search bound B, we list the lowest and highest number of colors attained by $\mathbb{Q}$-rational points of height at most B, ranging over the surfaces with the given number of bad primes. For the rows in which the search bound is annotated with the word "smooth", we consider only rational points that are smooth in the sense of Remark 3.5.

4B. ***Investigating the Brauer-Manin obstruction — a sample.*** We determined all Kummer surfaces of the form

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

with integer parameters of absolute value at most 200, that have a transcendental 2-torsion Brauer class.

More precisely, we determined all $(a, b, a', b') \in \mathbb{Z}^4$ such that

$$\begin{array}{llll} \gcd(a,b) = 1, & a > b > 0, & a - b \le 200, & b \le 200, \\ \gcd(a',b') = 1, & a' < b' < 0, & a' - b' \ge -200, & b' \ge -200, \end{array}$$

and such that the matrix $M_{aba'b'}$ has nonzero kernel. We made sure that only one of the four equivalent quadruples

$$(a,b,a',b'), \quad (-a',-b',-a,-b), \quad (a,a-b,a',a'-b'), \quad (-a',b'-a',-a,b-a)$$

was on the list, and we ignored the quadruples where (a, b) and (a', b') define geometrically isomorphic elliptic curves.

This led to 3075 surfaces with a kernel vector of type 1 and 367 surfaces with a kernel vector of type 2, together with two surfaces with $\mathrm{Br}(S)_2$ of dimension two. The latter correspond to the quadruples $(25, 9, -169, -25)$ and $(25, 16, -169, -25)$.

#Relevant primes	0	1	2	3	4	5	6
#Surfaces	6	428	1577	1119	276	9	1

Table 3. Number of surfaces with a given number of relevant primes.

Among the 3075 surfaces, 26 actually have $\mathrm{Br}(S)_2 = 0$, due to a $\mathbb{Q}$-isogeny between the corresponding elliptic curves.

The complete list of these surfaces, the exact equations we worked with, and more details are available on both author's web pages in the file `ants_X_data.txt`.

4C. ***The BM-relevant primes — the p-adic point of view.*** 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 nonconstant. For every surface in the sample described in Section 4B, we used Algorithm 2.12 and Theorem 2.19 to determine all of the *BM-relevant primes* p — that is, those for which there is a Brauer class working at p.

For the two surfaces with $\mathrm{Br}(S)_2$ of dimension two, the situation is as follows: In the case of the parameter vector $(25, 9, -169, -25)$, one Brauer class works at 2 and 13, another at 5 and 13, and the third at all three. For the surface corresponding to $(25, 16, -169, -25)$, one Brauer class works at 3 and 13, another at 5 and 13, and the last at all three.

Table 3 lists the number of surfaces in our sample set having a given number of relevant primes. The one example with six relevant primes is $(196, 75, -361, -169)$, for which the Brauer class works at 2, 5, 7, 11, 13, and 19.

For three surfaces, it happened that the corresponding elliptic curves were isogenous over a proper extension of $\mathbb{Q}$. In these cases, the Brauer-Manin obstruction is algebraic. For two of the surfaces, it worked at one prime, while for the third it worked at two.

4D. ***The BM-relevant primes — $\mathbb{Q}$-rational points.*** When the Brauer class α works at l primes $p_1, \ldots, p_l$, there are 2^l vectors with entries in $\{0, \frac{1}{2}\}$. By the Brauer-Manin obstruction, half of these vectors cannot be obtained as values of $(\mathrm{ev}_{\alpha,p_1}(x), \ldots, \mathrm{ev}_{\alpha,p_l}(x))$ for $\mathbb{Q}$-rational points $x \in S(\mathbb{Q})$. For every surface in our sample set, and for every vector not forbidden by the Brauer-Manin obstruction, we used Algorithm 3.4 to test whether there is a rational point giving rise to the vector.

It turned out that this was indeed the case. Thus, no further obstruction becomes visible via this coloring. However, in some of the cases rather high search bounds were necessary. Table 4 shows, for the extreme case of six relevant primes, the number of vectors hit for several search bounds. Somewhat surprisingly, the smallest solution for each color was smooth with respect to a bad prime bound of 800.

For the other surfaces in the sample, lower search bounds were sufficient, but the differences were enormous. We summarize our observations in Table 5.

Bound	50	100	200	400	800	1600	3200	6400	12800	25600	50000
#Vecs	5	10	14	20	24	26	28	30	31	31	32

Table 4. Numbers of evaluation vectors obtained from rational points of bounded height for the surface with parameters $(196, 75, -361, -169)$.

		Search bound B								
#Primes	#Surfaces	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 5. Search bounds required to obtain all possible evaluation vectors from rational points. For each entry in the first column, we list in the second column the number of surfaces in our sample having that number of relevant primes. For each search bound B in columns 3 through 11, we list the number of these surfaces for which the rational points of height at most B do *not* account for all valuations vectors not forbidden by the Brauer-Manin obstruction.

Remark 4.1. There is the expectation that the behavior of the evaluation map $\mathrm{ev}_{\alpha,p}$ is strongly connected to the type of bad reduction at the prime p. For algebraic Brauer classes, such a connection is well known; for example, see [11]. In the transcendental case, there are only partial results; see for example [13, §4].

For our examples, the reductions S_p are rational surfaces having one or two double lines. Further, $\mathrm{ev}_{\alpha,p}$ is necessarily constant on the set of $\mathbb{Q}$-rational points reducing to a smooth point. The finer structure seems to be complicated; compare Lemma 2.9.

References

[1] Manuel Benito and Juan L. Varona, *Pythagorean triangles with legs less than n*, J. Comput. Appl. Math. **143** (2002), no. 1, 117–126. MR 2003b:11027

[2] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics, no. 20, Academic Press, New York, 1966. MR 33 #4001

[3] Martin Bright, *The Brauer-Manin obstruction on a general diagonal quartic surface*, Acta Arith. **147** (2011), no. 3, 291–302. MR 2012f:11118

[4] J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika **13** (1966), 111–120. MR 35 #2841

[5] Jean-Louis Colliot-Thélène, Dimitri Kanevsky, and Jean-Jacques Sansuc, *Arithmétique des surfaces cubiques diagonales*, in Wüstholz [28], 1987, pp. 1–108. MR 89g:11051

[6] Jean-Louis Colliot-Thélène and Alexei N. Skorobogatov, *Good reduction of the Brauer–Manin obstruction*, Trans. Amer. Math. Soc. **365** (2013), no. 2, 579–590. MR 2995366

[7] Sinnou David (ed.), *Number theory*: *Papers from the Séminaire de Théorie des Nombres de Paris*, 1993–94, London Mathematical Society Lecture Note Series, no. 235, Cambridge University Press, 1996. MR 99b:11003

[8] Andreas-Stephan Elsenhans and Jörg Jahnel, *The Diophantine equation* $x^4 + 2y^4 = z^4 + 4w^4$, Math. Comp. **75** (2006), no. 254, 935–940. MR 2007e:11143

[9] ———, *On the Brauer-Manin obstruction for cubic surfaces*, J. Comb. Number Theory **2** (2010), no. 2, 107–128. MR 2907786

[10] ———, *On the order three Brauer classes for cubic surfaces*, Cent. Eur. J. Math. **10** (2012), no. 3, 903–926. MR 2902222

[11] ———, *On the quasi-group of a cubic surface over a finite field*, J. Number Theory **132** (2012), no. 7, 1554–1571. MR 2903170

[12] David Harari, *Obstructions de Manin transcendantes*, in David [7], 1996, pp. 75–87. MR 99e: 14025

[13] Brendan Hassett and Anthony Várilly-Alvarado, *Failure of the Hasse principle on general K*3 *surfaces*, 2011. arXiv 1110.1738 [math.NT]

[14] Brendan Hassett, Anthony Várilly-Alvarado, and Patrick Varilly, *Transcendental obstructions to weak approximation on general K*3 *surfaces*, Adv. Math. **228** (2011), no. 3, 1377–1404. MR 2012i:14025

[15] Evis Ieronymou, *Diagonal quartic surfaces and transcendental elements of the Brauer groups*, J. Inst. Math. Jussieu **9** (2010), no. 4, 769–798. MR 2011g:14053

[16] Evis Ieronymou, Alexei N. Skorobogatov, and Yuri G. Zarhin, *On the Brauer group of diagonal quartic surfaces*, J. Lond. Math. Soc. (2) **83** (2011), no. 3, 659–672. MR 2012e:14046

[17] Ilya Karzhemanov, *One construction of a K*3 *surface with the dense set of rational points*, 2011. arXiv 1102.1873 [math.AG]

[18] Adam Logan, David McKinnon, and Ronald van Luijk, *Density of rational points on diagonal quartic surfaces*, Algebra Number Theory **4** (2010), no. 1, 1–20. MR 2011a:11126

[19] Yu. I. Manin, *Cubic forms*: *algebra*, *geometry*, *arithmetic*, North-Holland Mathematical Library, no. 4, North-Holland Publishing Co., Amsterdam, 1974. MR 57 #343

[20] L. J. Mordell, *On the conjecture for the rational points on a cubic surface*, J. London Math. Soc. **40** (1965), 149–158. MR 30 #58

[21] Bjorn Poonen and Yuri Tschinkel (eds.), *Arithmetic of higher-dimensional algebraic varieties*: *Proceedings of the Workshop on Rational and Integral Points of Higher-Dimensional Varieties held in Palo Alto*, *CA*, *December* 11–20, 2002, Progress in Mathematics, no. 226, Boston, Birkhäuser, 2004. MR 2004h:11001

[22] Thomas Preu, *Transcendental Brauer-Manin obstruction for a diagonal quartic surface*, Ph.D. thesis, Universität Zürich, 2011. http://www.math.uzh.ch/fileadmin/user/preu/publikation/preuThesis.pdf

[23] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, no. 106, Springer, Dordrecht, 2009. MR 2010i:11005

[24] Alexei Skorobogatov and Peter Swinnerton-Dyer, 2*-descent on elliptic curves and rational points on certain Kummer surfaces*, Adv. Math. **198** (2005), no. 2, 448–483. MR 2006g:11129

[25] Alexei N. Skorobogatov and Yuri G. Zarhin, *The Brauer group of Kummer surfaces and torsion of elliptic curves*, J. Reine Angew. Math. **666** (2012), 115–140. MR 2920883

[26] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika **9** (1962), 54–56. MR 25 #3413

[27] Olivier Wittenberg, *Transcendental Brauer-Manin obstruction on a pencil of elliptic curves*, in Poonen and Tschinkel [21], 2004, pp. 259–267. MR 2005c:11082

[28] G. Wüstholz (ed.), *Diophantine approximation and transcendence theory*: *Papers from the seminar on number theory held in Bonn*, *May–June* 1985, Lecture Notes in Mathematics, no. 1290, Springer, Berlin, 1987. MR 88j:11036

ANDREAS-STEPHAN ELSENHANS: stephan@maths.usyd.edu.au
School of Mathematics and Statistics F07, University of Sydney, NSW 2006, Sydney, Australia

JÖRG JAHNEL: jahnel@mathematik.uni-siegen.de
Department Mathematik, Universität Siegen, Walter-Flex-Straße 3, D-57068 Siegen, Germany

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS