The Brauer–Manin obstruction

David Kurniadi Angdinata

Tuesday, 5 December 2023

Abstract

A Diophantine equation with a rational solution always has a real solution and a p-adic solution for every prime number p, but the converse is not always true — why?

1 Diophantine equations

Number theorists have been fascinated with solving Diophantine equations for millennia. To this end, Hilbert asked if there is a deterministic algorithm that decides whether any Diophantine equation has an integral solution, and this was answered in the negative by Matiyasevich–Robinson–Davis–Putnam. The analogous problem is trivial over an archimedean local field or a finite field, and is well-understood over a non-archimedean local field via Hensel's lemma, but is completely open for a number field.

A natural first step is to search for rational solutions with small height in a bounded box. If the Diophantine equation does have a solution, this procedure will eventually terminate, albeit possibly taking longer than the heat death of the universe. If it does not have solutions in the first place, this procedure will never terminate, so a more systematic approach is necessary. One approach is to understand the local solutions of the Diophantine equation, and apply a local-global principle to get a global rational solution.

2 The Hasse principle

Throughout, let K be a number field, and let $\mathbb{A}_K$ denote its ring of adèles. For any place $v \in \Omega_K$, let K_v denote its completion at v, let K_v^{nr} denote its maximal unramified extension, let $\mathcal{O}_v$ denote its valuation ring, and let $\mathbb{F}_v$ denote its residue field. Furthermore, let X be a smooth projective geometrically integral variety over K, and let X_L and $X(L)$ be its base change and rational points over an extension L of K respectively.

For any place $v \in \Omega_K$, the embedding $K \hookrightarrow K_v$ induces an inclusion $\iota_{K_v} : X(K) \hookrightarrow X(K_v)$, so clearly $X(K_v) = \emptyset$ implies that $X(K) = \emptyset$. In fancier terminology, this says that there is a **local obstruction** to existence of rational points on X. In fact, checking that $X(\mathbb{F}_v) = \emptyset$ is often enough by Hensel's lemma.

Example. *Let X be given by $x^2 + y^2 - 3z^2 = 0$. Then $(\frac{-1}{3}) = -1$, so $X(\mathbb{F}_3) = X(\mathbb{Q}_3) = X(\mathbb{Q}) = \emptyset$.*

By considering all places simultaneously, the diagonal embedding $K \hookrightarrow \mathbb{A}_K$ induces an inclusion $\iota_{\mathbb{A}_K} : X(K) \hookrightarrow X(\mathbb{A}_K)$, which by the valuative criterion for properness is equal to $\prod_{v \in \Omega_K} X(K_v)$ since X is projective. Although this is an infinite product, checking for local obstructions is a finite process.

Proposition. *There is an effectively computable finite set of places $v \in \Omega_K$ such that $X(K_v) = \emptyset$.*

Sketch of proof. Let C be a smooth geometrically integral curve on X, which has finitely many places of bad reduction. For any place $v \in \Omega_K$ of good reduction, there is some smooth point in $C(\mathbb{F}_v)$ for sufficiently large $\#\mathbb{F}_v$ by the Hasse–Weil bound, so Hensel's lemma lifts this to some smooth point in $C(\mathbb{Q}_v)$. □

If one's luck depletes, it may be the case that $X(\mathbb{A}_K) \neq \emptyset$ but $X(K) = \emptyset$ in a box with bounded height. It begs the question of whether $X(\mathbb{A}_K) \neq \emptyset$ is sufficient for $X(K) \neq \emptyset$, but this is not true in general.

Example (Lind–Reichardt)**.** *Let X be given by the genus one curve $2y^2 = x^4 - 17z^4$, which has bad reduction at 2 and 17. Clearly $(\sqrt{2} : \sqrt{2} : 0) \in X(\mathbb{R})$. For any prime p of good reduction, the Hasse–Weil bound gives $\#X(\mathbb{F}_p) \geq p + 1 - 2\sqrt{p} > 0$, which lifts by Hensel's lemma to give $X(\mathbb{Q}_p) \neq \emptyset$. Furthermore, $(\sqrt{2} : \sqrt{2} : 0) \in X(\mathbb{Q}_{17})$ since $2 \equiv 6^2 \mod 17$ and $(\sqrt[4]{17} : 0 : 1) \in X(\mathbb{Q}_2)$ since $17 \equiv 3^4 \mod 64$. On the other hand, if $(x : y : z) \in X(\mathbb{Q})$, then without loss of generality $x, y, z \in \mathbb{Z}$ such that $\gcd(x, z) = 1$ and $y > 0$. For any odd prime $p \mid y$, reducing modulo p gives $x^4 \equiv 17z^4 \mod p$, so quadratic reciprocity says that p is a square modulo 17. Since ± 2 are also squares modulo 17, in fact y is itself a square modulo 17, so let $y = y'^2$ for some $y' \in \mathbb{Z}$. Then $2y'^4 \equiv x^4 \mod 17$, but 2 is not a fourth power modulo 17.*

In fact, this represents an element of the Tate–Shafarevich group of the elliptic curve $y^2 = x^3 + 17x$. In a strange stroke of luck, if the converse were to hold for X, say that **the Hasse principle** holds for X.

Example. *The Hasse principle is known to hold for many families of varieties:*

- *(Hasse–Minkowski) quadric hypersurfaces*
- *Severi–Brauer varieties*
- *del Pezzo surfaces of degree at least five*

On the other hand, there are many individual varieties where the Hasse principle fails:

- *(Selmer) a cubic curve given by $3x^3 + 4y^3 + 5z^3 = 0$*
- *(Cassels–Guy) a cubic surface given by $5x^3 + 12y^3 + 9z^3 + 10t^3 = 0$*
- *(Birch–Swinnerton-Dyer) a del Pezzo surface given by $uv = x^2 - 5y^2$ and $(u + v)(u + 2v) = x^2 - 5z^2$*

Counter-examples to the Hasse principle have also been constructed for a few families of varieties:

- *curves of arbitrary genus at least one*
- *del Pezzo surfaces of degree between two and four, such as cubic surfaces*
- *K3 surfaces, such as quartics*

In the examples where the Hasse principle fails, there is no local obstruction, so a more refined obstruction is necessary to explain these counter-examples. The idea is to construct an obstruction set S sandwiched in

$$X(K) \subseteq S \subseteq X(\mathbb{A}_K),$$

such that $X(\mathbb{A}_K) \neq \emptyset$ but $S = \emptyset$, and this will be defined in terms of the Brauer group of X.

3 Brauer groups

Let X be the spectrum $\mathrm{Spec}(F)$ of a field F. A **central simple algebra** over F is a finite-dimensional algebra over F with centre F and with no non-trivial two-sided ideals. For instance, any matrix algebra $\mathrm{Mat}_n(F)$ over F is a central simple algebra over F, and the tensor product $A \otimes_F B$ of two central simple algebras A and B over F is also central simple algebra over F. Two central simple algebras over F are **Brauer equivalent** if there are $m, n \in \mathbb{N}$ such that $A \otimes_F \mathrm{Mat}_m(F) \cong B \otimes_F \mathrm{Mat}_n(F)$ as algebras over F.

Proposition. *The Brauer equivalence classes of central simple algebras over F forms a torsion abelian group under $\otimes_F$ with identity $\mathrm{Mat}_n(F)$, and is isomorphic to the Galois cohomology group $H^2(\mathrm{Gal}(\overline{F}/F), \overline{F}^\times)$.*

Sketch of proof. The inverse of a central simple algebra is its opposite algebra, and the group axioms can be checked individually. The final statement follows from the parameterisation of central simple algebras over F of degree n by $H^1(F, \mathrm{PGL}_n)$ and considering the long exact sequence of $1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1$. □

This group is called the **Brauer group** $\mathrm{Br}(F)$ of F.

Example. *Here are some examples of Brauer groups of fields.*

- $\mathrm{Br}(\mathbb{F}_p) = \mathrm{Br}(\mathbb{C}) = \mathrm{Br}(\mathbb{C}(X)) = 0$.
- *There are two central simple algebras over* $\mathbb{R}$ *given by itself and* $\mathbb{H}$*, so* $\mathrm{Br}(\mathbb{R}) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.
- *For any finite place* $v \in \Omega_K$*, there is a map* $\mathrm{inv}_v : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$*, given by the composition*

$$\mathrm{Br}(K_v) \hookleftarrow H^2(\mathrm{Gal}(K_v^{\mathrm{nr}}/K_v), K_v^{\mathrm{nr}\times}) \xleftarrow{\phi_p^v \leftarrow\!\shortmid v} H^2(\widehat{\mathbb{Z}}, \mathbb{Z}) \xleftarrow{\delta} H^1(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\phi \mapsto \phi(1)} \mathbb{Q}/\mathbb{Z},$$

which is an isomorphism by the proof of local class field theory.

Theorem (Albert–Brauer–Hasse–Noether)**.** *There is a short exact sequence*

$$0 \to \mathrm{Br}(K) \to \bigoplus_{v \in \Omega_K} \mathrm{Br}(K_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0.$$

Sketch of proof. The maps are induced covariant functorially, and injectivity follows from the vanishing of the first Galois cohomology of the idéle class group associated to K in the proof of global class field theory. □

In general, the Brauer group of a scheme X generalises that of F in two different ways. One way is to replace central simple algebras with **Azumaya algebras**, which are locally free $\mathcal{O}_X$-algebras such that every scheme-theoretic fibre $X \otimes \kappa(x)$ is a central simple algebra over the residue field $\kappa(x)$, and the resulting quotient group is the **Brauer–Azumaya group** $\mathrm{Br}'(X)$. This interpretation is amenable to realising explicit elements in $\mathrm{Br}'(X)[2]$ called quaternion algebras to get explicit obstructions.

Another way is to replace Galois cohomology with étale cohomology to get the **Brauer–Grothendieck group** $\mathrm{Br}(X) := H^2_{\text{ét}}(X, \mathbb{G}_m)$. For a general scheme X, there is merely an injection $\mathrm{Br}'(X) \hookrightarrow \mathrm{Br}(X)$, but in the relevant case of a quasi-projective variety over an affine scheme, this is an isomorphism of torsion abelian groups. This interpretation is amenable to abstractly computing $\mathrm{Br}(X)$ via the **Leray spectral sequence**

$$H^p(\mathrm{Gal}(\overline{K}/K), H^q_{\text{ét}}(X_{\overline{K}}, \mathbb{G}_m)) \implies H^{p+q}_{\text{ét}}(X, \mathbb{G}_m),$$

whose first few terms form an exact sequence

$$0 \to \mathrm{Pic}(X) \to \mathrm{Pic}(X_{\overline{K}})^{\mathrm{Gal}(\overline{K}/K)} \to \mathrm{Br}(K) \to \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}})) \to H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Pic}(X_{\overline{K}})) \to 0.$$

The kernel $\mathrm{Br}_1(X) := \ker(\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}}))$ is called the **algebraic Brauer group**, whose quotient $\mathrm{Br}(X)/\mathrm{Br}_1(X)$ is called the **transcendental Brauer group**. The latter is still rather mysterious, but can be computed by an exact sequence arising from higher terms in the Leray spectral sequence, given by

$$0 \to \mathrm{Br}(X)/\mathrm{Br}_1(X) \to \mathrm{Br}(X_{\overline{K}}) \to H^2(\mathrm{Gal}(\overline{K}/K), \mathrm{Pic}(X_{\overline{K}})).$$

Example. *Here are some examples of Brauer groups of schemes.*

- *If* X *is the spectrum of a field* F*, then* $\mathrm{Br}(X) = \mathrm{Br}(\mathrm{Spec}(F))$.
- *If* X *is the projective line, then* $\mathrm{Br}(X) \cong \mathrm{Br}(K)$.
- *If* X *is an elliptic curve, then* $\mathrm{Br}(X) \cong \mathrm{Br}(K) \oplus H^1(\mathrm{Gal}(\overline{K}/K), X)$.

4 The Brauer–Manin obstruction

In general, Brauer groups are difficult to compute, but their cohomological description proves to be useful in explaining the failure of the Hasse principle. The point is that Br defines a contravariant functor, in the sense that a morphism $f : X \to Y$ of smooth projective geometrically integral varieties induces a homomorphism $f^* : \mathrm{Br}(Y) \to \mathrm{Br}(X)$ of torsion abelian groups. In particular, a point $x \in X(L)$ over an extension L of K is just a map $x : \mathrm{Spec}(L) \to X$, which induces a map $x^* : \mathrm{Br}(X) \to \mathrm{Br}(L)$, and hence a pairing

$$\begin{array}{rccc} \langle -, - \rangle_L & : & \mathrm{Br}(X) \times X(L) & \longrightarrow & \mathrm{Br}(L) \\ & & (A, x) & \longmapsto & x^*A \end{array}.$$

When $L = \mathbb{A}_K$, this is called the **Brauer–Manin pairing**. Turning this around, an Azumaya algebra $A \in \mathrm{Br}(X)$ induces maps $\langle A, - \rangle_K : X(K) \to \mathrm{Br}(K)$ and $\langle A, - \rangle_{K_v} : X(K_v) \to \mathrm{Br}(K_v)$ for each place $v \in \Omega_K$, and it turns out that the local maps are trivial for all but finitely many places $v \in \Omega_K$, giving a map $\langle A, - \rangle_{\mathbb{A}_K} : X(\mathbb{A}_K) \to \bigoplus_{v \in \Omega_K} \mathrm{Br}(K_v)$. Combining this with the short exact sequence yields a diagram

$$\begin{array}{ccccccccc} & & & & X(K) & \xrightarrow{\iota_{\mathbb{A}_K}} & X(\mathbb{A}_K) & & \\ & & & & \downarrow & & \downarrow{\scriptstyle \langle A, - \rangle_{\mathbb{A}_K}} & & \\ 0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & \bigoplus_{v \in \Omega_K} \mathrm{Br}(K_v) & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0. \end{array}$$

Since the bottom row is exact, for any $A \in \mathrm{Br}(X)$, the map

$$\begin{array}{rccc} \langle A, - \rangle_K & : & X(K) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & & x & \longmapsto & \sum_{v \in \Omega_K} \mathrm{inv}_v \langle A, \iota_{K_v}(x) \rangle_{K_v} \end{array}$$

is trivial, so $X(K)$ lies in the subset of $X(\mathbb{A}_K)$ orthogonal to A with respect to $\langle A, - \rangle_K$, namely

$$X(\mathbb{A}_K)^A := \{x \in X(\mathbb{A}_K) : \langle A, x \rangle_K = 0\}.$$

The **Brauer–Manin set** is then defined to be the intersection of $X(\mathbb{A}_K)^A$ for all $A \in \mathrm{Br}(X)$, namely

$$X(\mathbb{A}_K)^{\mathrm{Br}} := \bigcap_{A \in \mathrm{Br}(X)} X(\mathbb{A}_K)^A.$$

This is a set sandwiched between $X(K)$ and $X(\mathbb{A}_K)$, and it turns out to be precisely the obstruction set that explains the failure of the Hasse principle for the examples from before. In other words, if $X(\mathbb{A}_K) \neq \emptyset$ but $X(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$, say that there is a **Brauer–Manin obstruction to the Hasse principle** for X.

Note that if $X(K) \neq \emptyset$, but $X(K) \hookrightarrow X(\mathbb{A}_K)$ is not dense in the adèlic topology, the Brauer–Manin set may be able to explain the obstruction to strong approximation. The map $\langle A, - \rangle_K$ is continuous for any $A \in \mathrm{Br}(X)$, so $X(\mathbb{A}_K)^{\mathrm{Br}}$ is closed, and hence contains the closure of $X(K)$. In other words,

$$X(K) \subseteq \overline{X(K)} \subseteq X(\mathbb{A}_K)^{\mathrm{Br}} \subseteq X(\mathbb{A}_K),$$

so say that there is a **Brauer–Manin obstruction to strong approximation** for X if $X(\mathbb{A}_K)^{\mathrm{Br}} \neq X(\mathbb{A}_K)$.

Example. *There is a Brauer–Manin obstruction for the following varieties:*

- *all the individual varieties from before*
- *torsors of abelian varieties*
- *conjecturally all rationally connected varieties*

Unfortunately, Skorobogatov gave an example of a Kummer variety where the Brauer–Manin obstruction cannot explain the failure of the Hasse principle. Furthermore, Poonen gave an example of a quadric bundle over a curve where no cohomological obstructions can explain the failure of the Hasse principle, so it remains an open problem to obtain an even finer obstruction to the Hasse principle.

References

CTS21 J-L Colliot-Thél'ene and A Skorobogatov (2021) *The Brauer–Grothendieck group*

Poo17 B Poonen (2017) *Rational points on varieties*

Sko01 A Skorobogatov (2001) *Torsors and rational points*

Vir23 B Viray (2023) *Rational points on varieties and the Brauer–Manin obstruction*