The Brauer-Manin obstruction to strong approximation

Ivo Kok

Master project

Supervised by:

Dr. Martin Bright

Submitted in part fulfillment of the requirements for the degree of
Master of Science in Mathematics, 30-08-2018

Mathematical institute of Leiden University

Contents

1. Introduction

The motivation of this thesis is the final remark of [Bri11]. The smooth quadric surface $Y \subset \mathbb{P}^3_{\mathbf{Q}}$ defined by

$$Y_0^2 + 47Y_1^2 = 103Y_2^2 + (17 \cdot 47 \cdot 103)Y_3^2,$$

was used in the proof of [Bri11, Proposition 3.3] to show that the diagonal quartic surface Z defined by

$$X_0^4 + 47X_1^4 = 103X_2^4 + (17 \cdot 47 \cdot 103)X_3^4,$$

has a Brauer-Manin obstruction to the existence of a rational point. Let $\tilde{Y}$ be the reduction of Y modulo 17. One of the byproducts of the proof given in this article, which is also the final remark, is that for every point $\tilde{P} \in \tilde{Y}(\mathbb{F}_{17})$ at most half of the scalar multiples of $\tilde{P}$ lift to rational points of Y with coprime integer coordinates. The author of this article wondered whether this conclusion could be proven without using the variety Z. The answer is positive and it is the main theorem of this thesis, which will be proven in Section 6. More precisely, we will prove the following theorem:

Theorem 1.1. *Let X be the affine cone over Y with the vertex removed and let $P \in X(\mathbf{Z})$ with $P = (y_0', \ldots, y_3')$ coprime integers. Set $a_0 = 1, a_1 = 47, a_2 = -103$ and $a_3 = -(17 \cdot 47 \cdot 103)$. Then the quaternion algebra $(a_0a_1a_2a_3, a_0y_0'Y_0 + \cdots + a_3y_3'Y_3) \in \mathrm{Br}(X)$ gives a Brauer-Manin obstruction to strong approximation in X away from $\{\infty\}$.*

In Section 2 we recall a bit of theory regarding the p-adic numbers and Hensel's lemma, before moving on to the Hasse principle and the definitions of weak and strong approximation in Section 3. The Brauer group of a field and a variety are treated in Section 4, but the latter will not be explained in detail. We take the classical approach using central simple algebras and do not use any Galois cohomology whatsoever.

In order to prove that a variety contains $\mathbf{Q}$-rational points, assuming that it satisfies the Hasse principle, it suffices to show that it is locally soluble everywhere. There are infinitely many completions of a number field, so it is not evident that checking that a variety is locally soluble everywhere is a finite time procedure. Fortunately, checking that a smooth variety over $\mathbf{Q}$ defined by a single equation is locally soluble everywhere can be done in finite time, and this will be proven in Section 5.

2. The p-adic numbers and Hensel's lemma

2.1. The p-adic numbers.

Convention 2.1. *A norm on a field k is a map from k to $\mathbf{R}_{\geqslant 0}$, denoted by $|\cdot|$, which satisfies the following 3 axioms for all $x, y \in k$:*

(1) $|x| = 0$ *if and only if* $x = 0$,

(2) $|x \cdot y| = |x| \cdot |y|$ *and*

(3) $|x + y| \leqslant |x| + |y|$.

The map which sends all non-zero elements of k to 1 and 0 to 0 is easily seen to be a norm and it is called the trivial norm. A non-trivial norm is ***non-Archimedean*** *if $|x + y| \leqslant \max(|x|, |y|)$ for all $x, y \in k$, and it is* ***Archimedean*** *if it is not non-Archimedean.*

Example 2.2. *The usual absolute value on $\mathbf{Q}$ and $\mathbf{R}$ denoted by $|\cdot|_\infty$ is an Archimedean norm, just as the complex absolute value on $\mathbf{C}$* [1]*. The p-adic norm $|\cdot|_p$ on $\mathbf{Q}$ for a prime number p, which will be explained later, is a non-Archimedean norm.*

Definition 2.3. *Let p be a prime number and a a non-zero integer. The* ***order of*** *a* ***at*** *p, denoted by $ord_p(a)$, is the largest power of p which divides a. Equivalently it is the largest m such that $a \equiv 0 \mod p^m$. For a non-zero rational number $x = c/d$ we define $ord_p(x) := ord_p(c) - ord_p(d)$. This is well defined, for if we write $x = bc/bd$ for some $b \in \mathbf{Z}_{\neq 0}$ then $ord_p(bc) - ord_p(bd)$ attains the same value as $ord_p(c) - ord_p(d)$ since $ord_p(bc) = ord_p(b) + ord_p(c)$. It extends the definition for integers above.*

Example 2.4.

$ord_3(10) = 0$, $\quad ord_2(1024) = 10$, $\quad ord_3(\frac{2}{27}) = -3$, *and* $\quad ord_3(\frac{15}{27}) = ord_3(\frac{5}{9}) = -2$.

Definition 2.5. *Let p be a prime number. The* ***p-adic norm on $\mathbf{Q}$*** *is the map*

$$|\cdot|_p \colon \mathbf{Q} \to \mathbf{R}_{\geqslant 0},$$
$$x \mapsto \begin{cases} \frac{1}{p^{ord_p(x)}} & \text{if } x \neq 0; \\ 0 & \text{if } x = 0. \end{cases}$$

This indeed defines a norm: properties (1) and (2) are straightforward to check and property (3) is proven in [Kob84, p2]. Koblitz actually shows that $|\cdot|_p$ satisfies the stronger non-Archimedean inequality, so $|\cdot|_p$ is a non-Archimedean norm.

Example 2.6.

$$|2|_2 = \tfrac{1}{2}, \quad |4|_2 = \tfrac{1}{4}, \quad |\tfrac{64}{3}|_2 = \tfrac{1}{64}, \quad |15|_3 = \tfrac{1}{3}, \text{ and } \quad |\tfrac{1}{125}|_5 = 125$$

In particular one sees that rational numbers are "p-adically small" if the numerator is divisible by a large power of p and "p-adically large" if the denominator is divisible by a large power of p. Two rational numbers are "close" whenever their difference is divisible by a large power of p.

Let k be an algebraic number field. A norm on k defines a metric on k and two metrics d_1 and d_2 are equivalent if a sequence is Cauchy with respect to d_1 if and only if it is Cauchy with respect to d_2. Two norms are called equivalent if they give rise to equivalent metrics on k. This is an equivalence relation, and an equivalence class of norms on k is called a **place**. We denote the set of places of k by Ω_k. If v

[1] Since $|1 + 1| = 2 > 1 = \max(|1|, |1|)$.

is a place of k we denote by k_v the completion of k at v [2]. The following theorem tells us that "∞ and the prime numbers are the only places of $\mathbf{Q}$".

Theorem 2.7 (Ostrowski)**.** *Every non-trivial norm on $\mathbf{Q}$ is equivalent to either the usual archimedean absolute value $|\cdot|_\infty$ or a p-adic non-archimedean norm $|\cdot|_p$ for some prime number p.*

Proof. See [Kob84, Theorem 1, p3] or [Gou93, Theorem 3.1.3, p43].

■

Let p be a prime number. The field of p-adic numbers $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to the p-adic norm. Let $a \in \mathbf{Q}_p$ be an equivalence class and $(a_i)_{i=1}^\infty$ a Cauchy sequence representing a. The p-adic norm of a is defined as

$$|a|_p := \lim_{n\to\infty} |a_n|_p.$$

This limit exists and does not depend on the choice of a representing sequence [3]. Moreover, this defines a non-Archimedean norm which takes values in $\{0\}\cup\bigcup_{n\in\mathbf{Z}}\{p^n\}$ and extends the p-adic norm on $\mathbf{Q}$.

Almost no/one thinks about the real numbers as equivalence classes of Cauchy sequences of rational numbers, but instead one thinks of them as decimal expansions in base 10. Similarly we think about p-adic numbers as expansions in base p.

Lemma 2.8. *Every equivalence class $a \in \mathbf{Q}_p$ for which $|a|_p \leqslant 1$ has exactly one representative Cauchy sequence of the form $(a_i)_{i=1}^\infty$ with $a_i \in \mathbf{Z}$, such that for all i:*

(1) $0 \leqslant a_i < p^i$;

(2) $a_i \equiv a_{i+1} \mod p^i$.

Proof. See [Kob84, Theorem 2, p11].

■

Denote the set of p-adic integers by $\mathbf{Z}_p := \{a \in \mathbf{Q}_p \colon |a|_p \leqslant 1\}$. Let $a \in \mathbf{Z}_p$ be an equivalence class and $(a_i)_{i=1}^\infty$ the Cauchy sequence of Lemma 2.8 corresponding to a. For all $i \geqslant 1$ we have $a_{i+1} = a_i + b_i \cdot p^i$ for some unique $b_i \in \{0, \ldots, p-1\}$, and we denote the p-adic integer a by $b_0 + b_1 p + b_2 p^2 + \ldots$, where $b_0 := a_1$. We extend this notation to $\mathbf{Q}_p$ as follows: if $x \in \mathbf{Q}_p$, then there exist an integer $m \in \mathbf{Z}_{\geqslant 0}$ [4] such that $x \cdot p^m \in \mathbf{Z}_p$. This p-adic integer has an expansion of the form $b_0 + b_1 p + b_2 p^2 + \ldots$, and write $x = p^{-m} b_0 + b_1 p^{-m+1} + b_2 p^{-m+2} + \ldots$. Summarizing, we have:

Theorem 2.9. (1) *Every element of $\mathbf{Z}_p$ has a p-adic expansion of the form $\sum_{i=0}^\infty b_i p^i$ with $b_i \in \{0, \ldots, p-1\}$ for all i. Moreover, every expansion of this form represents a p-adic integer.*

---

[2] We write ∞ for the equivalence class of $|\cdot|_\infty$ and p for the equivalence class of $|\cdot|_p$ whenever we talk about k_v to ease the notation

[3] The existence of this limit is proven in [Kob84, p10] and the uniqueness follows by combining the fact that $|x+y| = \max(|x|, |y|)$ if $|x| \neq |y|$ for a non-Archimedean norm, and that $|a_i - b_i|_p \to 0$ for equivalent sequences $(a_i)_{i=1}^\infty$ and $(b_i)_{i=1}^\infty$, see [Bak17, p25].

[4] There exists a smallest such n, but any $m \geqslant n$ will work and they all give rise to the same notation because of the uniqueness of the expansion of elements of $\mathbf{Z}_p$.

(2) *Every element of* $\mathbf{Q}_p$ *has a* p*-adic expansion of the form* $\sum_{i=-m}^{\infty} b_i p^i$ *for some* $m \in \mathbf{Z}$ *and* $b_i \in \{0, \ldots, p-1\}$ *for all* i*. Moreover, every expansion of this form represents a* p*-adic number.*

Proof. The first part follows from Lemma 2.8. The second part follows from the fact that multiplying an arbitrary p-adic number by a large enough power of p yields a p-adic integer.

■

Remark 2.10. *Two* p*-adic numbers are the same if and only if their* p*-adic expansions coincide by Theorem 2.9. This is not true in the real case, since the expansions* $0.99\ldots$ *and* $1.00\ldots$ *with repeating* 9*'s and* 0*'s both represent the real number* 1*. Hence this is one example why* p*-adic numbers are more convenient to work with. Another difference is that we need a sign for the real numbers, but this is not needed for the* p*-adic numbers.*

Example 2.11. *Every positive integer has a finite expansion of the form* $\sum_{i=0}^{n} b_i p^i$ *for some* $n \in \mathbf{Z}_{\geqslant 0}$*. If a* p*-adic number* x *has a finite expansion of the form* $\sum_{i=-k}^{n} b_i p^i$ *for some* $k \in \mathbf{Z}_{\geqslant 0}$ *then* $x \cdot p^k$ *is a positive integer, so* x *is a positive rational number whose denominator is divisible by a power of* p*.*

Using these expansions we can do computations in $\mathbf{Q}_p$. The arithmetic in $\mathbf{Q}_p$ is rather similar as the one in $\mathbf{R}$, except that "carrying" and "borrowing" etc. now goes from left to right instead of right to left. For instance, in $\mathbf{Q}_3$:

$$(1+p) + (2+2p) = 3 + 3p = 4p = p + p^2.$$

Example 2.12. *We will compute the* 3*-adic expansion of* $1/2$ *in* $\mathbf{Q}_3$*. In* $\mathbf{Z}/3\mathbf{Z}$ *we have* $1/2 = 2$*, since* $2 \cdot 2 = 4 = 1 \mod 3$*. Likewise we have*

$$\begin{aligned}
1/2 &= 5 = 2 + 3 \text{ in } \mathbf{Z}/9\mathbf{Z},\\
1/2 &= 14 = 2 + 3 + 3^2 \text{ in } \mathbf{Z}/27\mathbf{Z},\\
1/2 &= 41 = 2 + 3 + 3^2 + 3^3 \text{ in } \mathbf{Z}/81\mathbf{Z}, \text{ and}\\
1/2 &= 122 = 2 + 3 + 3^2 + 3^3 + 3^4 \text{ in } \mathbf{Z}/243\mathbf{Z}.
\end{aligned}$$

Hence we claim that $1/2 = 2 + 3 + 3^2 + 3^3 + 3^4 + \cdots = 2 + \sum_{i=1}^{\infty} 3^i$*, and indeed,*

$$2 \cdot (2 + 3 + 3^2 + 3^3 + 3^4 + \ldots) = 4 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \cdots = 1,$$

since the 3 *is constantly carried over to the next term to make all the coefficients but the first one, zero. Another way to see this is as follows:*

$$2 + \sum_{i=1}^{\infty} 3^i = 2 + \frac{3}{1-3} = 2 - 3/2 = 1/2,$$

where the first equality is justified, because the sum $\sum_{i=1}^{n} 3^i$ *converges* 3*-adically as* $n \to \infty$*.*

Example 2.13. *The additive inverse of the* p*-adic expansion* $\sum_{i=-k}^{\infty} b_i p^i$ *where* b_{-k} *is non-zero, is given by* $(p - b_{-k})p^{-k} + \sum_{i=-k+1}^{\infty}(p - b_i - 1)p^i$*. Indeed:*

$$(p - b_{-k})p^{-k} + \sum_{i=-k}^{\infty} b_i p^i + \sum_{i=-k+1}^{\infty} (p - b_i - 1)p^i = pp^{-k} + \sum_{i=-k+1}^{\infty} (p-1)p^i,$$

and the p will constantly be carried over to the next term by construction, so the latter is divisible by arbitrary powers of p, i.e. it is zero. In particular one sees that

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots = \sum_{i=1}^{\infty} (p-1)p^i.$$

Example 2.14. *We will try to find a square root of 17 in $\mathbf{Z}_2$, so let $p = 2$. We are looking for $a_i \in \{0, 1\}$ such that*

$$\begin{aligned} 1 + p^4 &= (a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \dots)^2 \\ &= a_0^2 + 2a_0 a_1 p + (2a_0 a_2 + a_1^2)p^2 + (2a_0 a_3 + 2a_1 a_2)p^3 + \dots \\ &= a_0^2 + (2a_0 a_2 + a_1^2 + a_0 a_1)p^2 + (2a_0 a_3 + 2a_1 a_2)p^3 + \dots \\ &= a_0^2 + (a_1^2 + a_0 a_1)p^2 + (2a_0 a_3 + 2a_1 a_2 + a_0 a_2)p^3 + \dots \\ &= a_0^2 + (a_1^2 + a_0 a_1)p^2 + a_0 a_2 p^3 + \dots \end{aligned}$$

Comparing coefficients yields $a_0 = 1$ and a_1 can be either 0 or 1. We can choose either one of them, and both options will lead to a (distinct) square root of 17 in $\mathbf{Q}_2$. A priori is not immediate that this process of computing the coefficients can be continued indefinitely, but Hensel's lemma and generalizations of it in the next section tell us this is indeed the case.

We conclude this section with some remarks about the metric space $\mathbf{Q}_p$.

Convention 2.15. *Let z and a be two p-adic numbers. We write $z \equiv a \mod p^i$ for some $i \in \mathbf{Z}$ if the p-adic expansions of z and a coincide up to and including the $(i-1)$'th coefficient. This extends the congruence notation of integers.*

Remark 2.16 (Basis of open sets for $\mathbf{Q}_p$)**.** *The p-adic norm takes values in the set $\{0\} \cup \{(1/p^i) \colon i \in \mathbf{Z}\}$. The collection of open balls around varying points and of varying radius is a basis for a metric space, so a basis of open sets of $\mathbf{Q}_p$ is given by the collection of sets of the form*

$$\left\{z \in \mathbf{Q}_p \colon |z - a|_p \leqslant (1/p^i)\right\},$$

for $a \in \mathbf{Q}_p$ and $i \in \mathbf{Z}$. By definition we have $|z - a|_p \leqslant (1/p^i)$ if and only if $ord_p(z - a) \geqslant i$, that is if and only if $z \equiv a \mod p^i$. The latter will be used the most in this thesis, because it is easier to work with. Moreover, every basic open set above can be written as a union of smaller open subsets. More specifically, for every $a \in \mathbf{Q}_p$ and $i \in \mathbf{Z}$ we have

$$\left\{z \in \mathbf{Q}_p \colon z \equiv a \mod p^i\right\} = \bigcup_{k=0}^{p-1} \left\{z \in \mathbf{Q}_p \colon z \equiv a + kp^i \mod p^{i+1}\right\}.$$

Hence for every $N \in \mathbf{Z}$ the collection of sets of the form $\left\{z \in \mathbf{Q}_p \colon |z - a|_p \leqslant (1/p^i)\right\}$ with $a \in \mathbf{Q}_p$ and $i \geqslant N$ is a basis for the p-adic topology on $\mathbf{Q}_p$. The same is true for the p-adic topology on $\mathbf{Q}$, we only have to replace $a \in \mathbf{Q}_p$ by $a \in \mathbf{Q}$. This will be used in a later section with $N = 0$, see Example 3.12.

Example 2.17. *The open set $\{z \in \mathbf{Q} \colon z \equiv 1 \mod 3\}$ can be written as:*

$$\{z \in \mathbf{Q} \colon z \equiv 1 \mod 9\} \cup \{z \in \mathbf{Q} \colon z \equiv 4 \mod 9\} \cup \{z \in \mathbf{Q} \colon z \equiv 7 \mod 9\}$$

In a similar fashion, the set $\left\{z \in \mathbf{Q}_2 \colon z \equiv 2^{-6} + 2^{-4} \mod 2^{-3}\right\}$ is the union of

$$\left\{z \in \mathbf{Q}_2 \colon z \equiv 2^{-6} + 2^{-4} \mod 2^{-2}\right\} \quad \text{and} \quad \left\{z \in \mathbf{Q}_2 \colon z \equiv 2^{-6} + 2^{-4} + 2^{-3} \mod 2^{-2}\right\}.$$

2.2. **Hensel's lemma.**

Theorem 2.18 (Hensel's lemma)**.** *Let $F(x) \in \mathbf{Z}_p[X]$. Assume that $a_0 \in \mathbf{Z}_p$ satisfies $F(a_0) \equiv 0 \mod p$ and $F'(a_0) \not\equiv 0 \mod p$. Then there exists a unique p-adic integer a such $F(a) = 0$ and $a \equiv a_0 \mod p$.*

Proof. See [Kob84, Theorem 3, p16]. ∎

Hensel's lemma tells us that if we find a p-adic integer a_0 such that $F(a_0)$ is somewhat close to zero, i.e. in the disk $\{x \in \mathbf{Z}_p : |x|_p \leqslant 1/p\}$, then, under some smoothness condition, we can find a unique zero of F that is somewhat close to our approximate zero. The polynomial we are interested in for Example 2.14 is $F(X) = X^2 - 17$, so its derivative vanishes modulo 2. Hence the condition of Hensel's lemma is not satisfied. However, the following generalization of Hensel's lemma will be helpful for certain exceptions like this one.

Lemma 2.19 (Generalization of Hensel's lemma)**.** *Let $F(x) \in \mathbf{Z}_p[X]$. If $a_0 \in \mathbf{Z}_p$ satisfies*

$$\begin{aligned} F'(a_0) &\equiv 0 \mod p^m \\ F'(a_0) &\not\equiv 0 \mod p^{m+1} \\ F(a_0) &\equiv 0 \mod p^{2m+1}, \end{aligned}$$

for some $m \in \mathbf{Z}_{\geqslant 1}$, then there exists a unique $a \in \mathbf{Z}_p$ such that $F(a) = 0$ and $a \equiv a_0 \mod p^{m+1}$.

Proof. We will imitate the proof of [Kob84, Theorem 3, p16]. We claim that there exists a unique sequence of rational integers $a_1, a_2, \ldots$ such that for all $n \geqslant 1$:

$$\begin{aligned} F(a_n) &\equiv 0 \mod p^{2m+1+n} \\ a_n &\equiv a_{n-1} \mod p^{m+n} \\ 0 &\leqslant a_n < p^{m+1+n}. \end{aligned}$$

If $n = 1$, let $\tilde{a}_0$ be the unique integer in $\left\{0, 1, \ldots, p^{m+1-1}\right\}$ congruent to a_0 modulo p^{m+1}. By the second condition we must have $a_1 = \tilde{a}_0 + b_1 p^{m+1}$ for some b_1 with $0 \leqslant b_1 \leqslant p-1$. Expanding $F(a_1)$ modulo p^{2m+2} yields

$$\begin{aligned} F(a_1) &= F(\tilde{a}_0 + b_1 p^{m+1}) \\ &= F(\tilde{a}_0) + F'(\tilde{a}_0) b_1 p^{m+1} + \tfrac{1}{2} F''(\tilde{a}_0) b_1^2 p^{2m+2} + \ldots \\ &\equiv F(\tilde{a}_0) + F'(\tilde{a}_0) b_1 p^{m+1} \mod p^{2m+2}. \end{aligned}$$

Note that the second derivative of F is divisible by 2, so the $1/2$ above cancels out, and in general the n'th order derivative is divisible by $n!$. We can write $F(\tilde{a}_0) \equiv \alpha p^{2m+1}$ for some $\alpha \in \{0, 1, \ldots, p-1\}$ since $F(a_0) \equiv 0 \mod p^{2m+1}$. So in order to get $F(a_1) \equiv 0 \mod p^{2m+2}$ we must have $\alpha p^{2m+1} + F'(\tilde{a}_0) b_1 p^{m+1} \equiv 0 \mod p^{2m+2}$. Dividing this congruence by p^{m+1} yields $\alpha p^m + F'(\tilde{a}_0) b_1 \equiv 0 \mod p^{m+1}$. We have $F'(\tilde{a}_0) \not\equiv 0 \mod p^{m+1}$ by assumption, so we can solve this congruence for the unknown b_1.

Suppose $n \geqslant 2$ and assume we already know $a_1, a_2 \ldots, a_{n-1}$. We will find a_n. By the second and third condition we must have $a_n = a_{n-1} + b_n p^{m+n}$ for some b_n with

$0 \leqslant b_n \leqslant p-1$. Expanding $F(a_n)$ yields

$$\begin{aligned} F(a_n) &= F(a_{n-1} + b_n p^{m+n}) \\ &= F(a_{n-1}) + F'(a_{n-1}) b_n p^{m+n} + \tfrac{1}{2} F''(a_{n-1}) b_n^2 p^{2m+2n} + \dots \\ &\equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^{m+n} \mod p^{2m+2n}. \end{aligned}$$

We can write $F(a_{n-1}) \equiv \alpha p^{2m+n}$ for some $\alpha \in \{0, 1, \dots, p-1\}$ since $F(a_{n-1}) \equiv 0 \mod p^{2m+n}$ by our induction assumption. In order to get $F(a_n) \equiv 0 \mod p^{2m+1+n}$ we must have $\alpha p^{2m+n} + F'(a_{n-1}) b_n p^{m+n} \equiv 0 \mod p^{2m+1+n}$. Dividing this congruence by p^{m+n} yields $\alpha p^m + F'(a_{n-1}) b_1 \equiv 0 \mod p^{m+1}$. We have $a_{n-1} \equiv a_0 \mod p^{m+1}$, so it follows that $F'(a_{n-1}) \equiv F'(a_0) \not\equiv 0 \mod p^{m+1}$. Hence we can solve the congruence for the unknown b_n, which completes the induction step.

Finally we set $a = a_0 p^m + a_1 p^{m+1} + \dots$. For all $n \geqslant 1$ we have $F(a) \equiv F(a_n) \equiv 0 \mod p^{2m+1+n}$, so $F(a) = 0$ by continuity. Conversely every p-adic integer $a = a_0 p^m + a_1 p^{m+1} + \dots$ that satisfies $F(a) = 0$ gives a sequence as in the claim, and by the uniqueness of this sequence, see Lemma 2.8, it follows that a is unique.

■

Example 2.20. *Continuing Example 2.14, we will show that* 17 *has a square root (actually two) in* $\mathbf{Z}_2$*, i.e. that the polynomial* $F = X^2 - 17$ *has a zero in* $\mathbf{Z}_2$*. Our computations have already shown that* 1 *and* 3 *are zeroes of* F *modulo* 4*. Hence we first check if* 1 *lifts to* $\mathbf{Z}_2$*. To this end let* $a_0 = 1$ *and* $m = 1$*. Then* $F'(1) = 2 \equiv 0 \mod 2$ *and* $F'(1) \not\equiv 0 \mod 4$ *and* $F(1) = -16 \equiv 0 \mod 8$*, so all the conditions of Lemma 2.19 are satisfied. Hence there exists a unique lift of* 1 *modulo* 4 *to* $\mathbf{Z}_2$*. In the same fashion one verifies that* 3 *modulo* 4 *lifts to the other square root of* 17 *in* $\mathbf{Z}_2$ [5]*.*

Remark 2.21. *A* p*-adic number* $a \in \mathbf{Q}_p$ *is a zero of a polynomial* F *if and only if* $F(a) \equiv 0$ *modulo* p^i *for all* $i \geqslant 1$*. Hence, in order to show that a polynomial does not have a zero in* $\mathbf{Q}_p$ *it suffices to show that it does not have any zeroes modulo* p^i *for some* $i \geqslant 1$*. This can be used for example to show that* $\mathbf{Q}_5$ *does not contain a square root of* 7*, since the equation* $X^2 = 7$ *does not have any solutions modulo* 5*.*

Generalizing Hensel's lemma to multivariate polynomials yields

Lemma 2.22 (A generalization of Hensel's Lemma for multivariate polynomials)**.** *Let* $F \in \mathbf{Z}_p[X_1, \dots, X_n]$ *and assume that there exists a point* $x = (x_1, \dots, x_n) \in \mathbf{Z}_p^n$ *such that* $F(x) \equiv 0 \mod p$*. If for one of the derivatives* F_i *we have* $F_i(x) \not\equiv 0 \mod p$*, then there exists a solution* $\alpha \in \mathbf{Z}_p^n$ *such that* $F(\alpha) = 0$ *and* $\alpha \equiv x \mod p$*.*

Proof. Assume without loss of generality that $F_1(x) \not\equiv 0 \mod p$. We let G be the polynomial given by $G := F(X, x_2, \dots, x_n) \in \mathbf{Z}_p[X]$, so by assumption we have $G(x_1) = F(x) \equiv 0 \mod p$ and $G'(x_1) = F_1(x) \not\equiv 0 \mod p$. Hence by Hensel's lemma there exists a unique p-adic integer $\alpha_1 \in \mathbf{Z}_p$ such that $G(\alpha_1) = 0$ and $\alpha_1 \equiv x_1 \mod p$. It follows that $\alpha := (\alpha_1, x_2, \dots, x_n)$ is the desired solution.

■

[5] We do not have explicit formulas for these square roots, but we now know that we can continue the computations of 2.14 indefinitely to an arbitrary precision, just as in the real case.

Remark 2.23. *Unlike the solution of Hensel's lemma, this one is not unique. For example consider the polynomial $F = X_1 \in \mathbf{Z}_p[X_1, X_2]$ and let $x = (0, x_2) \in \mathbb{F}_p^2$ be any point. Clearly $F_1(x) = 1 \not\equiv 0 \mod p$, but any lift of x_2 to $\mathbf{Z}_p$ gives rise to a different solution.*

Even more generally we have:

Lemma 2.24 (Another Generalization of Hensel's lemma)**.** *Let $F \in \mathbf{Z}_p[X_1, \ldots, X_n]$ and assume that there exists a point $x = (x_1, \ldots, x_n) \in \mathbf{Z}_p^n$ such that $F(x) \equiv 0 \mod p^{2m+1}$ for some integer m. If for one of the derivatives F_i we have*

$$F_i(x) \equiv 0 \mod p^m$$
$$F_i(x) \not\equiv 0 \mod p^{m+1}$$

then there exists a solution $\alpha \in \mathbf{Z}_p^n$ such that $F(\alpha) = 0$ and $\alpha \equiv x \mod p^{m+1}$

Proof. Imitate the proof of Lemma 2.22 and use the result of Lemma 2.19.

■

Hensel's lemma is very useful to quickly show that a polynomial has solutions in $\mathbf{Q}_p$ for all (or many) primes p, i.e. that it is solvable locally everywhere, which is something we will need repeatedly in further sections. The following example illustrates the usefulness of Hensel's lemma:

Example 2.25. *The equation $X^4 - 17 = 2Y^2$ is solvable locally everywhere.*

Proof. The product of two quadratic non-residues is a quadratic residue. Hence for every $p \neq 7, 19$ at least one of $7, 19$ and $7 \cdot 19 = 133$ is a square modulo p. So at least one of the three points

$$(\sqrt{7}, 4), \quad (5, 4\sqrt{19}), \quad (\sqrt{133}, 94)$$

is defined over $\mathbf{Q}_p$ for $p \neq 2, 7, 19$ by Hensel's lemma. For $p = 2$ the point $(3, 4)$ modulo 32 lifts to a point in $\mathbf{Q}_2$ by Lemma 2.19. For $p = 7$ and $p = 19$ the points $(0, 3)$ modulo 7 and $(0, 1)$ modulo 19 lift to points in $\mathbf{Q}_7$ and $\mathbf{Q}_{19}$ by Hensel's lemma. Thus the equation is solvable locally everywhere.

■

3. The Hasse principle, weak approximation and strong approximation

3.1. **The Hasse principle.** Let X be a quasi-projective variety. If $X(k)$ is non-empty, then so is $\prod_{v\in\Omega_k} X(k_v)$ because k is contained in k_v for all places v. The converse is in general not true; there are varieties X such that $X(k_v)$ is non-empty for all places v, yet $X(k)$ is empty. An example of such a variety was given in 1957 by Selmer and he showed that the equation $3X^3 + 4Y^3 + 5Z^3 = 0$ has zeroes in $\mathbf{Q}_v$ for all places v and that it does not contain any $\mathbf{Q}$-rational point [Sel51]. We say that this equation is solvable locally everywhere, but not globally. Another example of such a variety is the zero set of the equation $X^4 - 17 = 2Y^2$ over $\mathbf{Q}$, discovered by Lind and Reichardt independently in 1940 and 1942.

Example 3.1. *The equation $X^4 - 17 = 2Y^2$ is solvable locally everywhere, but it is not solvable in $\mathbf{Q}$.*

Proof. We have already shown that the equation is solvable locally everywhere in Example 2.25. Now suppose that (u, v) is a rational solution, and write $u = a/c$ and $v = b/d$ with $a, b, c, d \in \mathbf{Z}$ such that $cd \neq 0$ and $\gcd(a, c) = \gcd(b, d) = 1$. Substituting this into the equation and multiplying both sides by c^4d^4 yields the equation $(ad)^4 - 17(cd)^4 = 2(bc^2d)^2$. Hence we have an non-trivial integer solution of the equation $X^4 - 17Z^4 = 2Y^2$. Let $(x, y, z) \in \mathbf{Z}^3_{\geqslant 0}$ be such a non-trivial solution of this equation and note that $y > 0$ since there are no non-trivial integral solutions to $X^4 - 17Z^4 = 0$.

Assume that a prime p divides both x and z. Then p^4 divides $2y^2$, so p^2 divides y. Thus $(x/p, y/p, z/p^2)$ is another integer solution of the equation, so we may assume that $\gcd(x, z) = 1$. If $17 \mid y$ then $17 \mid x^4$, so $17 \mid x$. Hence $17^2 \mid x^4 - 2y^2 = 17z^4$, which implies that $17 \mid z$, contradicting our assumption that $\gcd(x, z) = 1$.

If a prime $p \neq 17$ divides y, then $p^2 \mid 2y^2 = x^4 - 17z^4$, so $x^4 \equiv 17z^4 \mod p$. In particular we have $x \equiv 0 \mod p$ if and only if $z \equiv 0 \mod p$, so both are non-zero modulo p by our assumption. Hence $17 \equiv (x/z)^4 \mod p$, which implies that 17 is a square modulo p. So p is a square modulo 17 by quadratic reciprocity. Thus y is a square modulo 17 since it is a product of squares. Let $b \in \mathbf{Z}$ be given such that $y \equiv b^2 \mod 17$. Note that $b \not\equiv 0 \mod 17$, otherwise we would have $17 \mid y$, a contradiction. Then $x^4 \equiv 2b^4 \mod 17$, so $2 \equiv (x/b)^4 \mod 17$. It follows that 2 is a fourth power modulo 17, which is a contradiction. Thus we conclude that the equation is not solvable in $\mathbf{Q}$.

■

There are however certain classes of varieties such that the implication

$$(\text{for all places } v:\ X(k_v) \neq \varnothing) \quad \Rightarrow \quad X(k) \neq \varnothing$$

holds, and if this is the case we say that the **Hasse principle** holds for these classes of varieties. In general it is not very useful to say that a single variety satisfies the Hasse principle. However, knowing that a whole class of varieties satisfies the Hasse principle is already more convenient. For if you are given a variety of that class and want to know if it contains a rational point, you only need to check whether it is solvable locally everywhere, which can be done in finite time as explained later on in Section 5. One example for which this can be used is the collection of quadrics in projective space:

Theorem 3.2 (Hasse–Minkowski)**.** *A quadratic form with rational coefficients is solvable in the field of rational numbers if and only if it is solvable locally everywhere.*

Proof. [Ser73, Theorem 8, p41]

■

Moreover, we say that X gives an obstruction to the Hasse principle if the implication above does not hold for X. The fact that the cubic curve above defined by the equation $3X^3 + 4Y^3 + 5Z^3 = 0$ does not satisfy the Hasse principle is not exceptional, since Bhargava has recently shown that a positive proportion of all ternary cubic forms over $\mathbf{Z}$, ordered by the size of their coefficients, fail the Hasse principle [Bha14]. Additionally, he also showed that a positive proportion all ternary cubic forms over $\mathbf{Z}$ satisfy the Hasse principle nontrivially.

3.2. **Weak approximation.**

Definition 3.3. *A variety X satisfies **weak approximation** if the image of $X(k)$ in $\prod_{v\in\Omega_k} X(k_v)$ is dense under the diagonal embedding, where the latter is given the product topology, and we say that X gives an obstruction to weak approximation if this is not the case. Moreover, if $S \subset \Omega_k$ is a finite set of places then X satisfies **weak approximation away from** S if the image of $X(k)$ in $\prod_{v\in\Omega_k\setminus S} X(k_v)$ is dense under the diagonal embedding.*

If $X(k_v)$ is empty for some place $v \in \Omega_k$, then so are $X(k)$ and the product above. In this case it does not make any sense to approximate k_v-rational solutions by k-rational numbers, since there are none. In particular the variety then trivially satisfies weak approximation, so from now on we implicitly assume throughout this section that $X(k_v)$ is non-empty for all places $v \in \Omega_k$.

Remark 3.4. *Equivalently, a variety X satisfies weak approximation if and only if for all non-empty open subsets $U \subset \prod_{v\in\Omega_k} X(k_v)$, the intersection of U and the diagonal image of $X(k)$ is non-empty. A basis open of $\prod_{v\in\Omega_k} X(k_v)$ is of the form $\prod_{v\in\Omega_k} U_v$ where $U_v \subset X(k_v)$ is open and $U_v \neq X(k_v)$ for finitely many v. Hence if $\prod_{v\in\Omega_k} X(k_v)$ is non-empty then X satisfies weak approximation if and only if for every finite subset $T \subset \Omega_k$ and open sets U_v for $v \in T$, there exists a point in the intersection of the diagonal embedding of $X(k)$ and*

$$\prod_{v\notin T} X(k_v) \times \prod_{v\in T} U_v,$$

where the places v range over all of Ω_k. A basis open of $\prod_{v\in\Omega_k\setminus S} X(k_v)$ is of the form $\prod_{v\in\Omega_k\setminus S} U_v$ where $U_v \subset X(k_v)$ is open and $U_v \neq X(k_v)$ for finitely many v. Hence X satisfies weak approximation away from S if and only if for every finite subset $T \subset \Omega_k \setminus S$ and open sets U_v for $v \in T$, there exists a point in the intersection of the diagonal embedding of $X(k)$ and

$$\prod_{v\in(\Omega_k\setminus S)\setminus T} X(k_v) \times \prod_{v\in T} U_v.$$

Note that no condition is set on the k_v-rational points with $v \in S$. Thus, since we assume that $X(k_v)$ is non-empty for all places $v \in \Omega_k$, we could as well assume that this k-rational point must lie in $X(k_v)$. This does not add anything extra, because any k-rational point is trivially a k_v-rational point, but it makes the notation easier [6] *as follows: if $\prod_{v\in\Omega_k} X(k_v)$ is non-empty then X satisfies weak approximation away from S if and only if for every finite subset $T \subset \Omega_k$ with $S \subset T$ and open sets U_v*

[6] Compare the following with Remark 3.10.

for $v \in T$, there exists a point in the intersection of the diagonal embedding of $X(k)$ and

$$\prod_{v \notin T \setminus S} X(k_v) \times \prod_{v \in T \setminus S} U_v,$$

where the places v range over all of Ω_k.

Remark 3.5. *The term weak approximation is quite fitting, because it is about approximating finitely many k_v-points by a single k-point. If a variety X satisfies weak approximation, then given a finite set of places v and k_v-points x_v, there always exists a k-point such that $|x - x_v|_v$ is arbitrary small for all these finitely many v simultaneously. By the previous remark it follows immediately that weak approximation away from S is a weaker condition than weak approximation. Exactly as the name says, when one has to check whether a variety satisfies weak approximation away from S, you do not have to approximate k-rational points by k_v-rational points any more for $v \in S$.*

Example 3.6 (The affine line satisfies weak approximation)**.** *Let $X = \mathbb{A}^1_{\mathbf{Q}}$ be the affine line over $\mathbf{Q}$. A basic open subset of $\prod_{p \in \Omega_k \setminus \{\infty\}} \mathbf{Q}_p$ is of the form $\prod_{p \in \Omega_k \setminus \{\infty\}} U_p$, where the U_p are open in $\mathbf{Q}_p$ and $U_p \neq \mathbf{Q}_p$ for finitely many p. A basic open subset of $\mathbf{Q}_p$ is of the form $\left\{x \in \mathbf{Q}_p \colon x \equiv a \mod p^{N_p}\right\}$ for some $a \in \mathbf{Q}_p$ and $N_p \in \mathbf{Z}$ which may depend on p, see Remark 2.16. Hence in order to show that X satisfies weak approximation, it suffices to prove that, given a finite set of places $p \leqslant \infty$ and $x_p \in \mathbf{Q}_p$, we can always find a rational number x that is arbitrary to all the x_p with respect to the p-adic norm. Equivalently, if S is a finite set of places then the diagonal image of X is dense in $\prod_{v \in S} \mathbf{Q}_v$. This is a particular case of the following theorem.*

Theorem 3.7 (Weak approximation)**.** *Let S be a finite set of inequivalent nontrivial norms of a field k. Then the diagonal image of X is dense in $\prod_{v \in S} k_v$.*

Proof. A little bit technical, see for example [Ste04, p126].

■

Weak approximation is a stronger condition on a variety than the Hasse principle, for if $X(k)$ is dense in $\prod_{v \in \Omega_k} X(k_v)$ and $\prod_{v \in \Omega_k} X(k_v)$ is non-empty, then so is $X(k)$. Satisfying weak approximation is actually a strictly stronger condition than satisfying the Hasse principle. An example of a variety that satisfies the Hasse principle but does not satisfy weak approximation is the cubic surface in $\mathbb{P}^3_{\mathbf{Q}}$ defined by the equation $t(x^2 + y^2) = (4z - 7y)(z^2 - 2t^2)$, for details see [SD62]. In a sense the Hasse principle tells something about the existence of k-rational points of a variety, while weak approximation says something about the density of these points.

3.3. **Strong approximation.** A condition that is even stronger than weak approximation is strong approximation. Before we give this definition we need some remarks about fixing equations for a variety. Suppose we were interested in the set of rational points of the equation $x^2 + 4y^2 = 1$. Any solution (a, b) of this equation gives rise to a solution $(a, 2b)$ of the equation $x^2 + y^2 = 1$, and this gives a one-to-one correspondence between rational solutions of these equations. In particular, if we know all the solutions of one of these equations, then we also know all the solutions of the other one. Hence if we are looking for rational points of $x^2 + 4y^2 = 1$ we could as well look for rational points on $x^2 + y^2 = 1$. The varieties defined by these equations are actually isomorphic over $\mathbf{Q}$. Whenever one considers varieties it is

therefore useful to not always fix one equation, but use the one which is easier to work with.

However, when looking for integral points on a variety given by an equation with integer coefficients, this is no longer true in general. Our first equation for example has only 2 integral points, while the latter has 4, so the $\mathbf{Z}$-points of these equations are not in a one-to-one correspondence. Thus an explicit equation with integer coefficients should be fixed when one considers integral points on a variety.

For a quasi-projective variety defined by integral equations, scheme theory gives a definition of integral points. In Section 6 this definition is only needed for quasi-affine varieties. Such a variety is of the form $X = \{f_i = 0\} \setminus \{g_j = 0\}$ of finitely many polynomials f_i and g_j with integral coefficients. In this special case, the set of integral points of X is defined as:

$$X(\mathbf{Z}) := \begin{array}{c} \{(x_0, \ldots, x_n) \in \mathbf{Z}^{n+1} : \forall i\, f_i(x_0, \ldots, x_n) = 0 \text{ and} \\ \forall p : \neg(g_0(x_0, \ldots, x_n) \equiv \cdots \equiv g_r(x_0, \ldots, x_n) \equiv 0 \mod p)\} \end{array}$$

and the set of $\mathbf{Z}_v$ integral points is defined in a similar fashion.

In the following we will follow section 2.6 of the notes of Bjorn Poonen [Poo10] and section 2 of [CTX13]. Let X be a quasi-projective variety over a number field k and Ω_k the set of places of k. Let $\mathcal{O}_v$ be the valuation ring of k_v if v is non-archimedean and let $\mathcal{O}_v = k_v$ if v is archimedean. The set of adelic points of X, denoted by $X(\mathbb{A}_k)$ is the restricted product $\prod'_{v\in\Omega_k}(X(k_v), X(\mathcal{O}_v))$, i.e. it is the set

$$\left\{(P_v)_{v\in\Omega_k} \in \prod_{v\in\Omega_k} X(k_v) : P_v \text{ has coordinates in } \mathcal{O}_v \text{ for all but finitely many } v\right\}.$$

Let $S \subset \Omega_k$ be a finite set of places of k containing all the archimedean places of k [7]. The set of adelic points of X away from S, denoted by $X(\mathbb{A}_k^S)$ is the restricted product $\prod'_{v\in\Omega_k\setminus S}(X(k_v), X(\mathcal{O}_v))$ [8].

Definition 3.8. *Let X be a variety over k and $S \subset \Omega_k$ a finite set of places of k containing all the archimedean places of k. The variety X satisfies **strong approximation away from** S if the image of $X(k)$ in $X(\mathbb{A}_k^S)$ is dense under the diagonal embedding and we say that X gives an obstruction to strong approximation away from S if this is not the case.*

Remark 3.9. *If X is a projective variety then $X(\mathcal{O}_v) = X(k_v)$ since we can clear denominators of a point. Hence weak approximation away from a non-empty set S of places and strong approximation away from S coincide for projective varieties. Thus it makes sense to only check whether certain affine varieties satisfy strong approximation away from S.*

Remark 3.10. *A basis of open subsets of $X(\mathbb{A}_k^S)$ is given by the collection of all sets of the form $\prod_{v\in T\setminus S} U_v \times \prod_{v\notin T} X(\mathcal{O}_v)$ with $T \supseteq S$ a finite set and open subsets $U_v \subset X(k_v)$ for $v \in T \setminus S$. Hence, similar as in the last part of Remark 3.4, if $\prod_{v\in\Omega_k} X(k_v)$ is non-empty then X satisfies strong approximation away from S if*

[7] The number of archimedean places of a number field is indeed finite, which is a consequence of [Cla12, Theorem 1.17c, p18]

[8] We want S to contain the archimedean places, because the statement that an $x_v \in X(k_v)$ is contained in $\mathcal{X}(\mathcal{O}_v)$ is saying nothing for archimedean places v. In particular these places are left out, since they do not add anything extra

and only if for every finite subset $T \subset \Omega_k$ with $S \subset T$ and open sets U_v for $v \in T \setminus S$, there exists a point in the intersection of the diagonal embedding of $X(k)$ and

$$\prod_{v \in S} X(k_v) \times \prod_{v \in T \setminus S} U_v \times \prod_{v \notin T} X(O_v),$$

where the places v range over all of Ω_k.

Remark 3.11. *Just as we did with weak approximation, we could say that a variety X satisfies strong approximation if it satisfies strong approximation away from $\varnothing$. However, this is not a very useful definition, because no affine variety satisfies this condition, as is mentioned in* [Poo10, p52]*, while strong approximation is equivalent to weak approximation for projective varieties. It is too strong a condition, so we will only consider strong approximation away from S, where S is a non-empty set.*

Example 3.12 (The affine line satisfies strong approximation away from infinity)**.** *Let $X = \mathbb{A}^1(\mathbf{Q})$ be the affine line over $\mathbf{Q}$. Then X satisfies strong approximation away from infinity by* [CF67, Section 15, p67][9]*, and we will give a concrete example to convey the idea of the proof. In order to show that X satisfies strong approximation away from $\{\infty\}$ it suffices to prove that, given a finite set T of primes $p < \infty$ and open $U_p \subset \mathbf{Q}_p$ for $p \in T$, we can find a rational number that is contained in all the U_p for $p \in T$ and integral at all other primes. A basis of open sets for the p-adic topology on $\mathbf{Q}$ is given by the collection of all sets of the form $\left\{z \in \mathbf{Q} \colon z \equiv a \mod p^i\right\}$ with $a \in \mathbf{Q}$ and $i \geqslant 0$, see Remark 2.16. Hence we may assume without loss of generality that the U_p are of this form.*

For convenience, assume that we are looking for a rational number that is contained in both $U_2 := \{z \in \mathbf{Q} : z \equiv 1/10 \mod 8\}$ and $U_3 := \{z \in \mathbf{Q} : z \equiv 1/6 \mod 9\}$ and integral at all other primes[10]*. Observe that $z \equiv 1/10 \mod 8$ is equivalent to $2z \equiv 1/5 \mod 16$, which is turn is equivalent to $2z \equiv 13 \mod 16$. In a similar fashion it follows that $z \equiv 1/6 \mod 9$ is equivalent to $3z \equiv 14 \mod 27$. Combining the latter two and using the fact that 2 and 3 are coprime, we conclude that we are looking for a ration number z such that $6z \equiv 39 \mod 16$ and $6z \equiv 28 \mod 27$. Such a rational number z exists by the Chinese Remainder Theorem* [11]*, and $6z = 55$, or equivalently $z = 55/6$ suffices, which is indeed integral at all primes $p \neq 2, 3$.*

Example 3.13. *The affine line over $\mathbf{Q}$ does not satisfy strong approximation (away from $\varnothing$)* [12]*. For there exists no rational point that is both contained in $(0, 1)$ and in $X(\mathbf{Z}_p)$ for all primes p, since the latter is equivalent to saying that the rational point is an integer.*

Remark 3.14. *Note the resemblance between weak approximation, weak approximation away from S and strong approximation away from S, as explained in Remark 3.4 and Remark 3.10. A variety X satisfies weak approximation away from S if we can approximate finitely many k_v points with $v \notin S$ by a single k-rational point and it satisfies weak approximation if we drop the condition on S. Strong approximation away from S is satisfied if we can simultaneously approximate finitely many k_v points with $v \notin S$ by a single k-rational point with the condition that this point is integral at all other places.*

---

[9] Cassels proves that a global field satisfies strong approximation away from any single place.

[10] The general case is very similar, but a little bit of a hassle.

[11] The fact that the affine line satisfies strong approximation away from infinity is actually just a restatement of the Chinese Remainder Theorem.

[12] Note that this is a consequence of Remark 3.11.

4. The Brauer group

4.1. Central simple algebras and Brauer groups.

Definition 4.1. *An **algebra** A over a field k, or a k-algebra, is a non-zero k-vector space equipped with a bilinear product and we say that it is associative if this multiplication operation is associative. It is **unital** if A contains an identity element 1 for the multiplication and in this case we get a natural map $k \to A$ by sending λ to $\lambda \cdot 1$. In particular we view k as a subring of A. A unital associative algebra A over a field k is **central** if the centre of A is k. Every non-zero algebra A has at least two two-sided ideals, the zero ideal and A itself, and we say that A is **simple** if A has exactly two two-sided ideals, i.e. if these are the only ones. A **central simple algebra** A over a field k is a unital associative finite dimensional algebra over k which is central and simple.*

Example 4.2. *The matrix algebra $M_n(k)$ of $n \times n$ matrices over a field k is a central simple algebra for all $n \geqslant 1$, which is a consequence of* [GS06, Example 2.1.2, p18]. *In particular k itself is a central simple algebra over k. More generally, if A is a central simple algebra over k, then so is $M_n(A)$* [13]. *Another example is the Hamilton quaternions, which is the 4-dimensional $\mathbf{R}$-vector space with basis $(1, i, j, ij)$ and multiplication defined by $i^2 = j^2 = -1$ and $ji = -ji$. Also note that the definition of a central simple algebra depends on the field k; the complex numbers $\mathbf{C}$ are a central simple algebra over $\mathbf{C}$ but not over $\mathbf{R}$ because $\mathbf{C}$ is not central over $\mathbf{R}$.*

In this thesis we will mostly deal with quaternion algebras, which are a particular type of central simple algebras [14]. They are a generalization of the Hamilton quaternions.

Definition 4.3. *Let k be a field of characteristic different from 2 and let a and b be two non-zero elements of k. The **quaternion algebra** $(a, b)_k$ is the algebra whose underlying vector space is k^4 with basis $(1, i, j, ij)$ and multiplication defined by*

$$i^2 = a, \quad j^2 = b, \quad ji = -ij.$$

Definition 4.4. *Let k be an algebraic number field, let v a place of k and let a and b be two non-zero elements of k_v. The **Hilbert symbol** $[a, b]_v$ of a and b is defined as*

$$[a, b]_v = \begin{cases} 1 & \text{if the conic } ax^2 + by^2 = z^2 \text{ has a non-zero } k_v\text{-rational point;} \\ -1 & \text{otherwise.} \end{cases}$$

The Hilbert symbol is bilinear [Ser73, Chapter 3][15], but if defined for more general k it is not in general bilinear. The symbols used for the quaternion algebra and the Hilbert symbol of a and b are similar for a reason; the following lemma tells us that they are closely related, and the proof will follow later.

Lemma 4.5. *Let k be a field of characteristic different from 2, let v a place of k and let a and b be two non-zero elements of k_v. Then the Hilbert symbol satisfies $[a, b]_v = 1$ if and only if the quaternion algebra $(a, b)_{k_v}$ is isomorphic to a matrix algebra over k_v.*

[13] Two-sided ideals of A are in one-to-one correspondence with two sides ideals of $M_n(A)$: every two-ideal I of A corresponds to the two-sided ideal of $n \times n$ matrices with entries in I. Moreover, the centre of A is in bijection with the centre of $M_n(A)$ via the map $a \mapsto \mathrm{Id} \cdot a$, where Id is the $n \times n$ identity matrix.

[14] They are indeed central simple algebras, see [Pie82, p14]

[15] Serre proves the bilinearity only in the case $k = \mathbf{Q}$, but that is all we need in this thesis.

Several of the following properties of the Hilbert symbol will be used later in this thesis.

Proposition 4.6. *Let k be a field of characteristic not 2 and $a, b, c \in k_v^\times$, then*

(1) $[a,b]_v = [b,a]_v$;

(2) *If a or b is a square in k_v then $[a,b]_v = 1$;*

(3) $[a,b]_v = [a, bc^2]_v$.

(4) *If $c \in N_{k_v(\sqrt{a})/k_v} k_v(\sqrt{a})^\times$ then $[a,b]_v = [a,bc]_v$*

Proof. The first three statements are immediate by definition, a proof of the latter can be found in [Ser73, Chapter 3].

■

A k-algebra homomorphism is a k-linear ring homomorphism, and we say that two central simple algebras A and B over the same field k are equivalent if there exist positive integers m, n such that $M_m(A)$ and $M_n(B)$ are isomorphic as k-algebras. This induces an equivalence relation on the set of isomorphism classes of central simple algebras; the only non-trivial part to check is the transitivity but this follows from the fact $M_m(M_n(A))$ and $M_{mn}(A)$ are isomorphic.

Definition 4.7. *A unital associative algebra D over k is called a **division algebra** if every non-zero element of A has an inverse.*

Remark 4.8. *Every central simple algebra A is isomorphic to $M_n(D)$ for some positive integer n and division algebra D by the theorem of Wedderburn* [GS06, Theorem 2.1.3]. *Moreover the division algebra D and the integer n are unique op to isomorphism of D and D is both finite dimensional and central. Hence it follows that every equivalence class of isomorphism classes of central simple algebras contains a unique division algebra D and all the other central simple algebras in this class are isomorphic to matrix algebras over D.*

Proof of Lemma 4.5. The quaternion algebra $\mathcal{A} = (a,b)_{k_v}$ is either a division algebra or isomorphic to $M_2(k_v)$ by the classification of central simple algebras stated in Remark 4.8. Moreover $\mathcal{A}$ is a division algebra if and only if $[a,b]_v = -1$ by [Pie82, p15], which completes the proof.

■

Definition 4.9. *The **Brauer group** $\mathrm{Br}(k)$ of a field k is the abelian group of equivalence classes of central simple algebras over k with the addition operation defined by $[A] + [B] := [A \otimes_k B]$. The identity element of $\mathrm{Br}(k)$ is $[k]$ and the inverse of a class $[A]$ is given by $[A^{opp}]$, where A^{opp} is the opposite algebra, i.e. the multiplication is reversed.*

Remark 4.10. *All the statements above, both implicit and explicit, need to be checked. We just mention what needs to be checked and remark that the proofs of these claims can be found in* [Mil13, p123-126]. *First of all, one shows that this operation is well-defined by using the fact that $A \otimes_k M_n(B) \cong M_n(A \otimes B)$ for all k-algebras A, B. The tensor product of two central simple algebras is again a central simple algebra and if A is a central simple algebra, then so is A^{opp}. The tensor product is also commutative, associative and satisfies $A \otimes_k k = A$, so $[A]+[k] = [A]$.*

If A is a central simple algebra then $A \otimes_k A^{opp}$ is isomorphic to a matrix algebra over k, so $[A] + [A^{opp}] = [A \otimes_k A^{opp}] = [k]$ by Remark 4.8.

Example 4.11. *Again we only mention some examples, the proofs can be found in* [Mil13, p128-138]*. The Brauer group of $\mathbf{C}$ is is the trivial group, and in general the Brauer group of any algebraically closed field is trivial. The Brauer group of $\mathbf{R}$ is isomorphic to $\mathbf{Z}/\frac{1}{2}\mathbf{Z}$ and is generated by the class of the Hamilton quaternions. The Brauer group of a finite field is trivial and the Brauer group of the p-adic numbers $\mathbf{Q}_p$ with p a prime is isomorphic to $\mathbf{Q}/\mathbf{Z}$.*

Until now we have only defined the Brauer group for fields, but this can be generalized to local rings. For this we need Azumaya algebras:

Definition 4.12. *Let R be a local ring with maximal ideal $\mathfrak{m}$. An **Azumaya algebra** over R is an algebra $\mathcal{A}$ over R such that $\mathcal{A} \cong R^m$ as an R-module for some m, and such that $\mathcal{A}/\mathfrak{m}\mathcal{A}$ is a central simple algebra over $R/\mathfrak{m}$. Two Azumaya algebras $\mathcal{A}, \mathcal{B}$ are said to be equivalent whenever there exist m, n such that $\mathcal{A} \otimes_R M_m(R)$ and $\mathcal{B} \otimes_R M_n(R)$ are isomorphic as R-algebras. The **Brauer group** $\mathrm{Br}(R)$ of R is the set of equivalence classes of Azumaya algebras over R with the tensor product as the product operation. The identity element of $\mathrm{Br}(R)$ is $[R]$ and the inverse of a class $[\mathcal{A}]$ is $[\mathcal{A}^{opp}]$.*

Remark 4.13. *Just as in Remark 4.10, all the explicit and implicit statements above need to be checked, but most of them follow immediately from the corresponding statements about central simple algebras.*

Definition 4.14. *Let R be a commutative local ring with residue characteristic different from 2 and let a and b be two non-zero elements of R. The quaternion ring $(a, b)_R$ is the free R-module with basis $(1, i, j, ij)$ and multiplication defined by the same rules as in Definition 4.3.*

Example 4.15. *Every central simple algebra over a field k is by definition an Azumaya algebra over k. For a less trivial example, let $X = \mathbb{A}^1_k$ be the affine line over a field k and let x be the origin of X. The local ring $R = \mathcal{O}_{X,x} = k[t]_{(t)}$ of X at x has maximal ideal (t) and the quaternion algebra $\mathcal{A} = (-1, t-1)_R$ is an Azumaya algebra* [16] *over R since $\mathcal{A}/(t)\mathcal{A} = (-1, -1)_k$ is a central simple algebra over $R/(t) = k$. The quaternion algebra $(-1, t)_R$ is however not an Azumaya algebra, because $(-1, 0)_k$ is not a central simple algebra over k.*

Lemma 4.16. *Let R be a regular local domain with quotient field K. There is a natural inclusion $\mathrm{Br}(R) \hookrightarrow \mathrm{Br}(K)$ induced by the inclusion $R \hookrightarrow K$.*

Proof. [AG60, Theorem 7.2]

■

We finally have all the ingredients to define the Brauer group of a smooth irreducible variety:

Definition 4.17. *Let X be a smooth irreducible variety over a field k and let $\kappa(X)$ be the function field of X. Let $\overline{k}$ be an algebraic closure of k. For $P \in X(\overline{k})$ we denote by $\mathcal{O}_{X,P} \subset \kappa(X)$ the local ring of X at P, which is the set of regular functions on a neighborhood of P. It is regular since X is smooth. Hence $\mathrm{Br}(\mathcal{O}_{X,P})$*

[16] Not $\mathcal{A}$ itself but the class of A is an element of $\mathrm{Br}(R)$ but this makes it easier to read and it is clear that we mean the class of A.

is a subgroup of $\mathrm{Br}(\kappa(X))$ *by the previous lemma, and the* ***Brauer group*** $\mathrm{Br}(X)$ *of* X *is defined as*

$$\mathrm{Br}(X) := \bigcap_{P \in X(\overline{k})} \mathrm{Br}(\mathscr{O}_{X,P}) \subset \mathrm{Br}(\kappa(X)).$$

We will only use the fact that $\mathrm{Br}(X)$ is a subgroup of $\mathrm{Br}(\kappa(X))$ and that we can evaluate elements of $\mathrm{Br}(X)$ at all points of $X(k)$ and $X(k_v)$ to get elements of $\mathrm{Br}(k)$ and $\mathrm{Br}(k_v)$ respectively. Our focus lies on quaternion algebras and Lemma 6.1 in one of the next sections will tell us exactly when a specific kind of quaternion algebra is an element of $\mathrm{Br}(X)$.

4.2. **Brauer-Manin obstructions.** Let k_v be a local field, then there exists a canonical injective invariant map, called the Hasse invariant

$$\mathrm{inv}_v \colon \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z},$$

which is an isomorphism if k_v is non-Archimedean. The construction of the invariant map involves a lot of local class field theory, so we will not go any deeper into this [17]. One of the things it is used for is proving that certain varieties do not satisfy strong approximation. By adding all the invariant maps together for all places v we get a map $\sum_v \mathrm{inv}_v \colon \bigoplus \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z}$.

Let $\mathcal{A} \in \mathrm{Br}(X)$ and recall that we can evaluate $\mathcal{A}$ at points of X. The following diagram is commutative:

$$\begin{array}{ccccc} X(k) & \longrightarrow & X(\mathbb{A}_k) & & \\ \downarrow & & \downarrow & & \\ \mathrm{Br}(k) & \longrightarrow & \bigoplus \mathrm{Br}(k_v) & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbf{Q}/\mathbf{Z} \end{array}$$

where the top horizontal arrow is the diagonal embedding and the two vertical arrows are the maps given by evaluating $\mathcal{A}$ at points. We indeed have an evaluation map from $X(\mathbb{A}_k)$ to $\bigoplus \mathrm{Br}(k_v)$ because for all $P \in X(k_v)$ and all but finitely many v we have $\mathcal{A}(P) = 0$ in $\mathrm{Br}(k_v)$ by [Sko01, p101]. The bottom horizontal arrow is injective by a consequence of the Albert-Hasse-Brauer-Noether theorem [Pie82, Section 8.4] and the bottom row is exact by [Pie82, p357]. In particular it follows that $\sum_v \mathrm{inv}_v(\mathcal{A}(P)) = 0$ for all $P \in X(k)$. We now define

$$X(\mathbb{A}_k)^{\mathcal{A}} := \left\{ (P_v)_v \in X(\mathbb{A}_k) : \sum_v \mathrm{inv}_v(\mathcal{A}(P_v)) = 0 \right\},$$

and for a subset $B \subset \mathrm{Br}(X)$ we set

$$X(\mathbb{A}_k)^{B} := \left\{ (P_v)_v \in X(\mathbb{A}_k) : \sum_v \mathrm{inv}_v(\mathcal{A}(P_v)) = 0 \text{ for all } \mathcal{A} \in B \right\}.$$

For every subset $B \subset \mathrm{Br}(X)$ we have $X(k) \subset X(\mathbb{A}_k)^B$, where $X(k)$ is considered as a subset of $X(\mathbb{A}_k)^B$ through the diagonal embedding of $X(k)$ to $X(\mathbb{A}_k)$. Hence in order to show that $X(k)$ is empty it suffices to show that $X(\mathbb{A}_k)^B$ is empty for some subset $B \subset \mathrm{Br}(X)$. If $X(\mathbb{A}_k)$ is non-empty but $X(\mathbb{A}_k)^B$ is empty for some B, then X gives an obstruction to the Hasse principle. In this case we say that there

[17] In Milne's class field theory notes [Mil13, Section *IV*.4] this invariant map is explicitly constructed for non-archimedean places v of a number field k. He also proves that it is a bijection for these places. More about the invariant map can be found in [Pie82, Section 17.10, p338].

is a Brauer-Manin obstruction to the Hasse principle on X coming from B. One could wonder whether all the counterexamples to the Hasse principle come from a Brauer-Manin obstruction, but this is not the case. See [Sko99, Section 2] for an example of a surface where the failure of the Hasse principle is not accounted for by a Brauer-Manin obstruction.

The set $X(\mathbb{A}_k)^{\mathcal{A}}$ is closed in $X(\mathbb{A}_k)$ since it is the fiber of a locally constant map [Poo10, Corollary 8.2.11]. Hence so is $X(\mathbb{A}_k)^B$, because it is the intersection of the $X(\mathbb{A}_k)^{\mathcal{A}}$ with $\mathcal{A} \in B$. Thus if the inclusion $X(\mathbb{A}_k)^B \subset X(\mathbb{A}_k)$ is strict, then X gives an obstruction to weak approximation. In this case we say that there is a Brauer-Manin obstruction to weak approximation on X (coming from B).

For a subset $B \subset \mathrm{Br}(X)$, denote by $X(\mathbb{A}_k^S)^B$ the image of $X(\mathbb{A}_k)^B$ under the projection map from $X(\mathbb{A}_k)$ to $X(\mathbb{A}_k^S)$. Then $X(\mathbb{A}_k^S)^B$ contains the diagonal image of $X(k)$. Hence if the inclusion $\overline{X(\mathbb{A}_k^S)^B} \subset X(\mathbb{A}_k^S)$ is strict, then X gives an obstruction to strong approximation away from S. In this case we say that there is an Brauer-Manin obstruction to strong approximation on X away from S (coming from B). Moreover, all the obstructions mentioned above can be computed explicitly in some cases, for example when $\mathrm{Br}\, X/\mathrm{Br}\, k$ is finite.

5. Checking that a variety is locally empty can be done in finite time

In this section we will prove the following theorem

Theorem 5.1. *Let $n \geqslant 1$ be an integer and $f \in \mathbf{Q}[X_1, \ldots, X_n]$ be a homogeneous polynomial such that $X := Z(f) \subset \mathbb{P}^n$ is a smooth variety. Then there exists an algorithm to compute whether $X(\mathbf{Q}_p)$ is empty for all p in finite time and this algorithm does not depend on f.*

In order to prove this theorem, we first need several lemmas.

For a field k we denote by $\bar{k}$ an algebraic closure. The zero locus of an ideal $I \subset k[X_1, \ldots, X_n]$ is denoted by $Z(I) := \left\{x \in \bar{k}^n : f(x) = 0 \text{ for all } f \in I\right\}$. If I is generated by a single polynomial f we write $Z(f)$ instead of $Z(I)$.

Lemma 5.2. *Let k be a field. If $f_1, \ldots, f_r \in k[X_1, \ldots, X_n]$ are polynomials such that $Z(f_1, \ldots, f_r)$ is empty, then $(f_1, \ldots, f_r) = k[X_1, \ldots, X_n]$.*

Proof. By Hilbert's Nullstellensatz we have

$$\sqrt{(f_1, \ldots, f_r)} = I(Z(f_1, \ldots, f_r)) = I(\varnothing) = k[X_1, \ldots, X_n],$$

which implies that $1 \in (f_1, \ldots, f_r)$.

■

Lemma 5.3. *Let $R := \mathbf{Q}[X_1, \ldots, X_n]$. If $f_1, \ldots, f_r \in R$ do not have a common zero in $\overline{\mathbf{Q}}$, then they do not have a common zero over any non-zero $\mathbf{Q}$-algebra.*

Proof. Let A be a $\mathbf{Q}$-algebra. Every point $a = (a_1, \ldots, a_n) \in A^n$ gives rise to an evaluation homomorphism $\varphi_a : R \to A$. We have $\varphi_a(1) = 1 \neq 0$, so $\ker(\varphi_a) \subsetneq R$. By assumption the polynomials $f_1, \ldots, f_r$ do not have a common zero in $\overline{\mathbf{Q}}$, hence $(f_1, \ldots, f_r) = R$ by Lemma 5.2. Assume for a contradiction that the polynomials $f_1, \ldots, f_r$ have a common zero over A, i.e. $f_1(a) = \cdots = f_r(a) = 0$ for some $a \in A$. Then it follows that $(f_1, \ldots, f_r) \subset \ker(\varphi_a)$, which contradicts the fact that $\ker(\varphi_a)$ is strictly contained in $R = (f_1, \ldots, f_r)$.

■

Let k be a field and let $\bar{k}$ be its algebraic closure. We say that a variety $X = Z(f)$ is smooth over k if it is smooth over $\bar{k}$.

Lemma 5.4. *Let $n \geqslant 1$ be an integer and let $f \in \mathbf{Z}[X_1, \ldots, X_n]$ be a homogeneous polynomial such that $X := Z(f) \subset \mathbb{P}^n$ is a smooth variety over $\mathbf{Q}$. Then X is a smooth variety over $\mathbb{F}_p$ for all but finitely many primes p. Moreover, computing the primes for which X is smooth can be done in finite time.*

Proof. We denote the i'th partial derivative of f by f_i. Since X is smooth over $\mathbf{Q}$ it follows that $\left\{x \in \overline{\mathbf{Q}}^n : f(x) = f_1(x) = \cdots = f_n(x) = 0\right\}$ is empty. Hence there exist polynomials $g, g_1, \ldots, g_r \in \mathbf{Q}[X_1, \ldots, X_n]$ such that $fg + f_1 g_1 + \ldots f_n g_n = 1$ by Lemma 5.2. Moreover, these polynomials can be computed in finite time. By clearing denominators we may assume that $fg + f_1 g_1 + \cdots + f_n g_n = d$ with $g, g_i \in \mathbf{Z}[X_0, \ldots, X_n]$ and $d \in \mathbf{Z}$. It follows that X is smooth over $\mathbb{F}_p$ for all primes $p \nmid d$. For let p be a prime such that $p \nmid d$, then $\overline{fg} + \overline{f_1 g_1} + \cdots + \overline{f_n g_n} = \overline{d} \neq 0 \mod p$. If $X/\mathbb{F}_p$ is not smooth, then there exists an $x \in \overline{\mathbb{F}_p}^n$ such that $f(x) = f_1(x) = \cdots =$

$f_n(x) = 0$. Hence $\overline{d} = \overline{f}(x)\overline{g}(x) + \overline{f_1}(x)\overline{g_1}(x) + \cdots + \overline{f_n}(x)\overline{g_n}(x) = 0 \mod p$, which is a contradiction.

■

We finally have enough ingredients to prove the theorem.

Proof of Theorem 5.1. By clearing denominators we may and will assume that $f \in \mathbf{Z}[X_1, \ldots, X_n]$. Moreover $X(\mathbf{Q}_p) \neq \varnothing$ if and only if $X(\mathbf{Z}_p) \neq \varnothing$ which follows by clearing denominators and using the assumption that f is homogeneous. We also know that X is smooth over $\mathbb{F}_p$ for all but finitely many p by Lemma 5.4. Additionally $X(\mathbb{F}_p)$ is non-empty for large enough p by estimates of Lang and Weil [LW54], and this bound on p is computable. For such large enough p of good reduction let $x \in X(\mathbb{F}_p)$. Since $X/\mathbb{F}_p$ is smooth it follows that $f_i(x) \neq 0$ for some i. Hence there exists a lift $\alpha \in \mathbf{Z}_p^n$ of x such that $\alpha \in X(\mathbf{Z}_p)$ by Lemma 2.22, so $X(\mathbf{Z}_p)$ is non-empty for these p.

It remains to check whether $X(\mathbf{Z}_p)$ is empty for a finite number of p. If $X(\mathbb{F}_p)$ is empty then $X(\mathbf{Z}_p)$ is also empty because every point of $X(\mathbf{Z}_p)$ reduces to a point of $X(\mathbb{F}_p)$. Thus we only need to consider the case where $X(\mathbb{F}_p)$ is non-empty and not smooth. In this case, let $x \in X(\mathbb{F}_p)$ be a point and lift it to a point $\alpha_1 \in \mathbb{P}^n(\mathbf{Z}_p)$. By assumption we have $\overline{f}(x) = 0$ in $\mathbb{F}_p$, so $f(\alpha_1) = 0 \mod p$. If $|f(\alpha_1)| < |f_i(\alpha_1)|^2$ for some partial derivative f_i then α_1 lifts to a point $X(\mathbf{Z}_p)$ by a slight generalization of Hensel's lemma, see Lemma 2.24. In particular $X(\mathbf{Z}_p)$ is non-empty in this case. Hence we assume that $|f_i(\alpha_1)|^2 \leqslant |f(\alpha_1)| \leqslant p^{-1}$ for all i. If there does not exist an α_2 such that $f(\alpha_2) \equiv 0 \mod p^2$ and such that $\alpha_2 \equiv \alpha_1 \mod p$ then there does not exist a lift α_2 of α_1 and we are done since α_1 cannot be lifted to a point of $X(\mathbf{Z}_p)$. Assume that such an α_2 exists, then we have to check whether $|f_i(\alpha_2)|^2 \leqslant |f(\alpha_2)| \leqslant p^{-2}$ for all i and we are done if this is false.

Assume for a contradiction that this process does not stop. In other words, for every $k \in \mathbf{Z}_{\geqslant 1}$ we have an α_k such that $f(\alpha_k) \equiv 0 \mod p^k$ and $\alpha_{k+1} \equiv \alpha_k \mod p^k$. In particular the sequence $(\alpha_k)_{k \in \mathbf{Z}_{\geqslant 1}}$ converges to an $\alpha \in \mathbb{P}^n(\mathbf{Z}_p)$ and this limit satisfies $f(\alpha) = 0$ because polynomials are continuous. Hence $\alpha \in X(\mathbf{Z}_p)$. Moreover, for all i we have $f_i(\alpha) = 0$, so we found a common zero over the $\mathbf{Q}$-algebra $\mathbf{Q}_p^{n+1}$, contradicting Lemma 5.3. Thus we conclude that the process above must stop. Note that if $X(\mathbf{Z}_p)$ is non-empty then we know when to stop the process above, since there is a smallest k such that $f_i(\alpha_k)0 \mod p^k$ for some i, and this puts a bound on the number of steps needed. Thus we conclude that the algorithm to compute whether $X(\mathbf{Q}_p)$ is empty for all p, takes finite time.

■

6. The main theorem

We consider smooth quadric surfaces Y of the form

$$a_0Y_0^2 + a_1Y_1^2 + a_2Y_2^2 + a_3Y_3^2 = 0,$$

where the a_i are coprime integers. Let X be the affine cone over Y with the vertex removed, so

$$X = \left\{a_0Y_0^2 + a_1Y_1^2 + a_2Y_2^2 + a_3Y_3^2 = 0\right\} \setminus \left\{Y_0 = Y_1 = Y_2 = Y_3 = 0\right\}.$$

Using the definition of integral points given in 3, it follows that the set of integral points of X is given by

$$X(\mathbf{Z}) = \left\{(y_0, \dots, y_3) \in \mathbf{Z}^4 : a_0y_0^2 + a_1y_1^2 + a_2y_2^2 + a_3y_3^2 = 0 \text{ and } \forall p \neg(y_0 \equiv \cdots \equiv y_3 \equiv 0 \mod p)\right\},$$

thus

$$X(\mathbf{Z}) := \left\{(y_0, \dots, y_3) \in X(\mathbf{Q}) : y_i \in \mathbf{Z} \text{ coprime integers}\right\},$$

and for a place v of k:

$$X(\mathbf{Z}_v) := \left\{(y_0, \dots, y_3) \in X(\mathbf{Q}_v) : y_i \in \mathbf{Z}_v \text{ not all divisible by a prime } p\right\}.$$

We denote the natural projection from X to Y by π.

Lemma 6.1. *Let $P \in X(\mathbf{Z})$ with $P = (y_0', \dots, y_3')$ and assume that $\theta = a_0a_1a_2a_3$ is not a square in $\mathbf{Q}$. Then the quaternion algebra $(a_0a_1a_2a_3, a_0y_0'Y_0 + \cdots + a_3y_3'Y_3)$ is the unique non-trivial element of order 2 of $\mathrm{Br}(X)/\mathrm{Br}(k)$.*

Proof. [BK17, Lemma 3.1]

■

We now consider the surface $Y \subset \mathbb{P}^3_k$ defined by

$$Y_0^2 + 47Y_1^2 = 103Y_2^2 + (17 \cdot 47 \cdot 103)Y_3^2,$$

so in the following $a_0 = 1, a_1 = 47, a_2 = -103$ and $a_3 = -(17{\cdot}47{\cdot}103)$, and note that this equation does have integral solutions, one of them being $(21, 43, 7, 1)$.

Theorem 6.2. *Let $P \in X(\mathbf{Z})$ with $P = (y_0', \dots, y_3')$ coprime integers. Then the quaternion algebra $(a_0a_1a_2a_3, a_0y_0'Y_0 + \cdots + a_3y_3'Y_3) \in \mathrm{Br}(X)$ with the a_i as above gives a Brauer-Manin obstruction to strong approximation in X away from $\{\infty\}$.*

We first give a sketch before we prove this theorem in detail.

Sketch of the proof. Let $S = \{\infty\}$ and $T = \{17, \infty\}$ and denote the quaternion algebra $(a_0a_1a_2a_3, a_0y_0'Y_0 + \cdots + a_3y_3'Y_3)$ by (θ, f). We will show that there exists an open set $U_{17} \subset X(\mathbf{Z}_{17})$ that has empty intersection with $X(\mathbf{Q})$. To this end we first prove that the invariant of $(\theta, f(Q))$ is zero for all $v \neq 17$ and $Q \in \mathbf{Z}_v$.

If 17 is a square in $\mathbf{Q}_v$ or if $f(Q)$ is 0 modulo v then this follows rather easily. Assuming neither of these two assumptions hold, and leaving the case $v = 17$ for the very end, we first show that P and Q are the same point in Y modulo v for $v \neq 17$. Then there exists another point $P' \in X(\mathbf{Z})$ such that P and P' do not reduce to the same point modulo v. Denote the corresponding linear form for the tangent plane at P' by f'. It follows that the invariant of $(\theta, f'(Q))$ is zero, so it remains to show that the invariants of $(\theta, f(Q))$ and $(\theta, f'(Q))$ coincide.

This is shown by first proving that they differ by some constant algebra $\mathcal{A} \in \mathrm{Br}(\mathbf{Q})$. The invariant of $\mathcal{A}$ is zero for all $v \neq 17$, so the invariant is also zero at 17 because

the sum of the invariants of a constant algebra is zero. Thus $\mathcal{A}$ is a trivial algebra and the invariants of $(\theta, f(Q))$ and $(\theta, f'(Q))$ coincide and are zero for $v \neq 17$.

If $f(Q)$ is not a square modulo 17 then the invariant of $(\theta, f(Q))$ is $1/2$. Hence points contained in the open set $U_{17} := \left\{ Q \in X(\mathbf{Z}_{17}) \,|\, \overline{f(Q)} \notin (\mathbb{F}_{17}^{\times})^2 \right\}$ do not come from points of $X(\mathbf{Q})$. Thus we have an obstruction to strong approximation in X away from $\{\infty\}$, since there are no points in $X(\mathbf{Q})$ contained in $X(\mathbf{R}) \times U_{17} \times \prod_{v \neq 17,\infty} X(\mathbf{Z}_v)$.

■

Proof. Let f and g be as in the proof of Lemma 6.1 and again write $\theta = a_0a_1a_2a_3$. Let v be a place of $\mathbf{Q}$ and assume that 17 is a square in $\mathbf{Q}_v$. Then so is θ, and in this case $(\theta, f)_{\kappa(X_v)} = 1$ by Proposition 4.6, where X_v is the variety defined by the same equation as X but over $\mathbf{Q}_v$ instead of over $\mathbf{Q}$. Hence the quaternion algebra $(\theta, f)_{\kappa(X_v)}$ is isomorphic to a matrix algebra over $\kappa(X_v)$ by Lemma 4.5, so in particular it is trivial in $\mathrm{Br}(X_v)$. The following diagram is commutative:

$$\begin{array}{ccc} \mathrm{Br}(X) & \longrightarrow & \mathrm{Br}(X_v) \\ & \searrow^{\mathrm{ev}_Q} & \downarrow{\scriptstyle \mathrm{ev}_Q} \\ & & \mathrm{Br}(\mathbf{Q}_v) \end{array}$$

so it follows that $(\theta, f(Q))$ is also trivial in $\mathrm{Br}(\mathbf{Q}_v)$ for all $Q \in X(\mathbf{Z}_v)$, which implies that $\mathrm{inv}_v((\theta, f(Q))_{\mathbf{Q}}) = 0$.

From now on we will assume that 17 is not a square in $\mathbf{Q}_v$ [18]. Let $Q \in X(\mathbf{Z}_v)$, then $f(Q) \in \mathbf{Z}_v$, so we can reduce $f(Q)$ modulo v. Then either $\overline{f(Q)} \neq 0$ or $\overline{f(Q)} = 0$ in $\mathbb{F}_v$ and we will consider both cases separately. First assume that $\overline{f(Q)} \neq 0$. The equation $17x^2 + \overline{f(Q)}y^2 = z^2 \mod v$ is homogeneous and the number of variables exceeds the degree, so it has a non-trivial solution by the Chevalley-Warning theorem. For $v \notin \{2, 17\}$ and $\overline{f(Q)} \neq 0 \mod v$, we can lift this solution to a solution in $\mathbf{Z}_v$ by Hensel's lemma. Hence in this case we have $\mathrm{inv}_v(17, f(Q)) = 0$ by definition of the Hilbert symbol combined with Lemma 7.1.

Now assume that $\overline{f(Q)} = 0 \mod v$ and let ℓ be the polynomial

$$\ell = Y_0^2 + 47Y_1^2 - 103Y_2^2 - (17 \cdot 47 \cdot 103)Y_3^2,$$

defining the surface Y. We define $\overline{Y} := \left\{ x \in \mathbb{P}^3_{\mathbb{F}_v} : \overline{\ell}(x) = 0 \right\}$, so by construction we have $\overline{\pi(Q)} \in \overline{Y} \cap \left\{ \overline{f} = 0 \right\} \subseteq \mathbb{P}^3_{\mathbb{F}_v}$. The quadric $\overline{Y}$ is smooth for $v \notin \{2, 17, 47, 103\}$ and 17 is a square in $\mathbf{Q}_2, \mathbf{Q}_{47}$ and in $\mathbf{Q}_{103}$, so these three exceptions are already covered. The case $v = 17$ will be handled separately at the end of the proof, so we also assume that $v \neq 17$. Hence $\overline{Y} \cap \left\{ \overline{f} = 0 \right\}$ is the union of two distinct conjugate lines defined over $\mathbb{F}_v(\sqrt{\theta}) = \mathbb{F}_v(\sqrt{17})$ by Lemma 7.2. The group $\mathrm{Gal}(\mathbb{F}_v(\sqrt{17})/\mathbb{F}_v)$ acts on these lines by sending a point on one of the lines to its conjugate on the other line. The lines intersect in exactly one point, so this is the only point defined over $\mathbb{F}_v$. Hence $\overline{\pi(P)} = \overline{\pi(Q)}$, since both points are defined over $\mathbb{F}_v$ and lie on $\overline{Y} \cap \left\{ \overline{f} = 0 \right\}$.

[18] So in particular $v \neq 2, \infty$, because 17 is a square in $\mathbf{R}$ and 17 is a square in $\mathbf{Z}_2$ as was shown in Example 2.20

We will show that there exists a $P' \in X(\mathbf{Z})$ such that $\pi(P') \not\equiv \pi(P) \mod v$. By [BK17, Lemma 2.2] it follows that $Y(\mathbb{F}_v)$ contains at least p^2+1 points. Hence there exists a point $R' \in Y(\mathbb{F}_v)$ such that $R' \not\equiv P \mod v$. The surface $Y(\mathbb{F}_v)$ is smooth, so we can lift this point to a point $R \in Y(\mathbf{Z}_v)$ by Hensel's lemma. Smooth projective quadrics satisfy weak approximation by [Har04, Theorem 2.2.1], so the image of $Y(\mathbf{Z}) \to \prod_v Y(\mathbf{Z}_v)$ is dense. Hence every non-empty open in $\prod_v Y(\mathbf{Z}_v)$ contains a point of $Y(\mathbf{Z})$. The set $U = \{(x_w) \in \prod_w Y(\mathbf{Q}_w) \,|\, x_v \equiv R' \mod v\}$ is non-empty [19] and open in $\prod_v Y(\mathbf{Z}_v)$, thus we find a point $P'' \in Y(\mathbf{Z}) \cap U$ and lifting this point to X yields the desired P'.

Let P' be as above and let g' be the corresponding linear form just as in the proof of Lemma 6.1. Then g' is an equation for the tangent space to Y at P'. Consider g' as a rational function on X and call it f'. Then $f'(Q) \neq 0 \mod v$, for if $f'(Q) \equiv 0 \mod v$ then $\pi(P') \equiv \pi(Q) \equiv \pi(P) \mod v$ by the same argument as above, contradicting our assumption. Hence by the same arguments as in the second and third paragraph it follows that $\mathrm{inv}_v(\theta, f'(Q)) = 0$.

We will show that (θ, f) and (θ, f') differ by a constant algebra, following the proof of [Bri11, Lemma 2.1]. In the first paragraph of the proof we showed that the divisor of vanishing of g on Y is given by $L + L'$, where L and L' are conjugate lines defined over $\mathbf{Q}(\sqrt{17})$. The divisor of vanishing of g' is then given by $L_1 + L_1'$, where L_1 is a line defined over $\mathbf{Q}(\sqrt{17})$, linearly equivalent to L and L_1' its conjugate over $\mathbf{Q}$. Hence we can find a rational function h on $Y_{\mathbf{Q}(\sqrt{17})}$ such that $(h) = L - L'$. Then $(g' N_{\mathbf{Q}(\sqrt{\theta})/\mathbf{Q}}(h)/Y_0) = (g/Y_0)$, so g is a constant multiple of $g' N_{\mathbf{Q}(\sqrt{\theta})/\mathbf{Q}} h$. Thus f/f' is a constant multiplied by the norm of a rational function defined over $\mathbf{Q}(\sqrt{17})$, so (θ, f) and (θ, f') differ by a constant algebra.

By the previous paragraph we know that $(\theta, f') = (\theta, f) + \mathcal{A}$ for some $\mathcal{A} \in \mathrm{Br}(\mathbf{Q})$, and we will now show that $\mathcal{A} = 0$. Let $Q' \in X(\mathbb{F}_v)$ be given such that $Q' \neq \overline{\pi(P)}$ and $Q' \neq \overline{\pi(P')}$. Such a Q' exists because $Y(\mathbb{F}_v)$ contains at least p^2+1 points. By Hensel's lemma we can lift Q' to a point $Q \in X(\mathbf{Z}_v)$. By assumption it follows that $\overline{f(Q)} \neq 0 \mod v$ and $\overline{f'(Q)} \neq 0 \mod v$, for if either $\overline{f(Q)} = 0 \mod v$ or $\overline{f'(Q)} = 0 \mod v$, then either $\overline{\pi(Q)} = \overline{\pi(P)}$ or $\overline{\pi(Q)} = \overline{\pi(P')}$ contradicting our construction of Q. Hence $\mathrm{inv}_v(17, f(Q)) = \mathrm{inv}_v(17, f'(Q)) = 0$ for all $v \neq 17$, so

$$\begin{aligned} \mathrm{inv}_v(\mathcal{A}) &= \mathrm{inv}_v(\mathcal{A}(Q)) = \mathrm{inv}_v((\theta, f')(Q) - (\theta, f)(Q)) \\ &= \mathrm{inv}_v((\theta, f')(Q)) - \mathrm{inv}_v((\theta, f)(Q)) = 0 \end{aligned}$$

By the exactness of the short exact sequence

$$0 \to \mathrm{Br}(\mathbf{Q}) \to \sum_v \mathrm{Br}(\mathbf{Q}_v) \overset{\sum_v \mathrm{inv}_v}{\to} \mathbf{Q}/\mathbf{Z} \to 0,$$

it follows that we also must have $\mathrm{inv}_{17}(\mathcal{A}) = 0$. Hence the invariant of $\mathcal{A}$ is zero at all places. The invariant $\mathrm{inv}_v \colon \mathrm{Br}(\mathbf{Q}_v) \to \mathbf{Q}/\mathbf{Z}$ is an isomorphism for all finite places and injective for the real place, so $\mathcal{A}(Q) = 0$ in $\sum_v \mathrm{Br}(\mathbf{Q}_v)$. Thus $\mathcal{A} = 0$ by the short exact sequence above. We conclude that $(\theta, f') = (\theta, f)$ and in particular that $\mathrm{inv}_v(\theta, f(Q)) = \mathrm{inv}_v(\theta, f'(Q)) = 0$.

[19] It is non-empty because otherwise every point in $Y(\mathbf{Z}_v)$ is congruent to R' modulo v, contradicting the fact that Y satisfies weak approximation

The only case that remains to be checked is $v = 17$. Suppose that $\overline{f(Q)} \neq 0$ in $\mathbb{F}_{17}$. Then it follows by [Ser73, Section III, Theorem 1]:

$$\mathrm{inv}_{17}((\theta, f(Q))_{\mathbf{Q}}) = (\theta, f(Q))_{17} = \left(\frac{\overline{f(Q)}}{17}\right).$$

Hence if $\overline{f(Q)}$ is not a square modulo 17 then $\mathrm{inv}_{17}((\theta, f(Q))_{\mathbf{Q}}) = 1/2$. Thus in the case we have $\sum_v \mathrm{inv}_v((\theta, f(Q))_{\mathbf{Q}}) = 1/2$. Let

$$\begin{aligned} U_{17} &:= \left\{ Q \in X(\mathbf{Z}_{17}) \,|\, \overline{f(Q)} \notin (\mathbb{F}_{17}^{\times})^2 \right\} \\ &= \bigcup_{a \in \mathbb{F}_p,\, a \notin (\mathbb{F}_{17}^{\times})^2} \left\{ Q \in X(\mathbf{Z}_{17}) \,|\, \overline{f(Q)} = a \mod 17 \right\}, \end{aligned}$$

so U_{17} is open because it is a union of open sets. We will show that it is also nonempty. To this end we observe that $X(\mathbf{Z}_{17})$ is non-empty, so let $Q \in X(\mathbf{Z}_{17})$. If $\overline{f(Q)}$ is a quadratic non-residue, then we are done, so assume that $\overline{f(Q)}$ is a quadratic residue. Then the point Q' obtained by multiplying Q by a quadratic non-residue is also contained in $X(\mathbf{Z}_{17})$ and $\overline{f(Q')}$ is a quadratic non-residue. Hence Q' is contained in U_{17}, and in particular at least half of the scalar multiples of Q are contained in U_{17}. It follows that the non-empty set

$$U_{17} \times \prod_{v \neq 17, \infty} X(\mathbf{Z}_v)$$

is open and it has empty intersection with $X(\mathbb{A}_k^S)^B$, so the inclusion $\overline{X(\mathbb{A}_k^S)^B} \subset X(\mathbb{A}_k^S)$ is strict, which finishes the proof.

■

7. Appendix

Lemma 7.1. *Let v be a valuation of $\mathbf{Q}$ and $a, b \in \mathbf{Q}^\times$. The value of the invariant at v of the quaternion algebra $(a,b)_{\mathbf{Q}}$ is equal to the Hilbert symbol $(a,b)_v$ under the unique group isomorphism between $\{\pm 1\}$ and $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$. In particular $\mathrm{inv}_v((a,b)_{\mathbf{Q}}) = 0$ if and only if $(a,b)_v = 1$.*

Proof. This follows by combining Lemma 4.5 and the fact that the invariant map is injective.

■

Lemma 7.2. *Let k be a field with $\mathrm{char}(k) \neq 2$ and let $Q \subset \mathbb{P}^3_k$ be a smooth quadric surface with M the corresponding symmetric matrix such that $\det(M)$ is not a square. Let $P \in Q$ be a point and denote the tangent space of Q at P by $T_P Q$. Then $T_P Q \cap Q$ is the union of two conjugate lines defined over $k(\sqrt{\det M})$.*

Proof. [BK17, Lemma 2.1]

■

References

[AG60] Maurice Auslander and Oscar Goldman. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1960.

[Bak17] Andrew Baker. An introduction to p-adic numbers and p-adic analysis, 2017. Available at http://www.maths.gla.ac.uk/ ajb/dvi-ps/padicnotes.pdf.

[Bha14] Manjul Bhargava. A positive proportion of plane cubics fail the hasse principle. 2014. Available at arXiv:1402.1131.

[BK17] Martin Bright and Ivo Kok. Failure of strong approximation on an affine cone. 2017. Available at arXiv:1707.04177.

[Bri11] Martin Bright. The Brauer-Manin obstruction on a general diagonal quartic surface. *Acta Arithmetica*, 147:291–302, 2011.

[CF67] J. W. S. Cassels and A. Fröhlich. *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

[Cla12] Pete L. Clark. Algebraic number theory ii: Valuations, local fields and adeles, 2012. Available at http://math.uga.edu/ pete/8410FULL.pdf.

[CTX13] Jean-Louis Colliot-Thélène and Fei Xu. Strong approximation for the total space of certain quadric fibrations. *Acta Arithmetica*, 157:169–199, 2013.

[Gou93] Fernando Q. Gouvêa. *p-adic Numbers: an introduction*. Universitext. Springer-Verlag, 1993.

[GS06] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[Har04] David Harari. Weak approximation on algebraic varieties. *Arithmetic of Higher-Dimensional Algebraic Varieties*, 226:43–60, 2004.

[Kob84] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984.

[LW54] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math*, 76:819–827, 1954.

[Mil13] J. S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[Pie82] Richard S. Pierce. *Associative Algebras*, volume 88 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982.

[Poo10] Bjorn Poonen. Rational points on varieties, 2010. Available at http://www-math.mit.edu/ poonen/papers/Qpoints.pdf.

[SD62] H. P. F. Swinnerton-Dyer. Two special cubic surfaces. 9:54–56, 1962.

[Sel51] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. 85:203–362, 1951.

[Ser73] J.-P. Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1973.

[Sko99] Alexei N. Skorobogatov. Beyond the Manin obstruction. *Invent. Math.*, 135:399–424, 1999.

[Sko01] Alexei N. Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.

[Ste04] William Stein. A brief introduction to classical and adelic algebraic number theory, 2004.