Mathematisches Institut
der
Ludwig-Maximilians-Universität München

Bachelorarbeit

Brauer-Manin obstructions for sums of two squares and a power

Verfasser: Fabian Gundlach

Betreuer: Prof. Dr. U. Derenthal

10. September 2012

Contents

1 Introduction

For integers $k \geq 2$ and m consider the equation

$$x^2 + y^2 + z^k = m. \tag{1}$$

For $k = 2$ the famous theorem of Gauß about sums of three squares says that (1) has an integral solution if and only if $m \geq 0$ and m is not of the form $4^u(8l + 7)$.

The theorem in [JK95] says that there is no integral solution if $k = 9$ and $m = (6p)^3$ for some prime $p \equiv 1 \mod 4$ and the following remark mentions that if k is an odd composite integer, then for some $m \in \mathbb{Z}$ equation (1) has no solution.

This thesis uses Brauer-Manin obstruction to analyze failures of strong approximation "at the variable Z" away from ∞ including those described in [JK95], [DE08a] and [DE08b].

Theorem 1. *The following equations do not fulfill strong approximation "at Z" away from ∞ due to Brauer-Manin obstruction:*

$$\begin{aligned} x^2 + y^2 + z^a &= n^a, && a \geq 3 \textit{ odd, } n \equiv 1 \mod 4 \\ x^2 + y^2 + z^a &= n^a, && a \geq 2 \textit{ even, } n > 0 \end{aligned}$$

Proof. See Example 4.3. □

The following theorems use Schinzel's hypothesis H (cf. [SS58]).

Theorem 2. *Each solution $(x_v, y_v, z_v)_v \in \prod_v \mathbb{Z}_v$ to equation* (1) *without any Brauer-Manin obstruction generated by Azumaya algebras of the form described in Section 3 can be approximated with respect to the variable Z by integral solutions to equation* (1).

Proof. See Theorem 5.5. □

Theorem 3. *Let k be prime. Then every integer is of the form $x^2 + y^2 + z^k$ for integral $x, y, z \in \mathbb{Z}$.*

Proof. See Corollary 5.10. □

Theorem 4. *Let $a, b \equiv 1 \mod 4$ be primes and $m \in \mathbb{Z} \setminus \{0\}$.*
Then the following statements are equivalent (for the implication "a) ⇒ b)" Schinzel's hypothesis H is not needed).

a) There exist $x, y, z \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^{ab} = m.$$

b) The following two statements are true:

- *There is no $n \equiv 6 \mod 8$ such that $m = n^a$ and for each prime $p \equiv 3 \mod 4$ dividing n:*
  $b \nmid v_p(n)$ or $2 \mid v_p(n)$ or there is no $z' \in \{0, \dots, p-1\}$ such that
  $$p \mid r_p(n)^{a-1} + \cdots + z'^{(a-1)b}.$$
- *There is no $n \equiv 6 \mod 8$ such that $m = n^b$ and for each prime $p \equiv 3 \mod 4$ dividing n:*
  $a \nmid v_p(n)$ or $2 \mid v_p(n)$ or there is no $z' \in \{0, \dots, p-1\}$ such that
  $$p \mid r_p(n)^{b-1} + \cdots + z'^{(b-1)a}.$$

Proof. See Theorem 5.12. □

Theorem 5. *Let $m \in \mathbb{Z} \setminus \{0\}$.*
Then the following statements are equivalent (for the implication "a) ⇒ b)" Schinzel's hypothesis H is not needed).

a) There exist $x, y, z \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^9 = m.$$

b) There is no integer $n \equiv 6 \mod 8$ such that $m = n^3$ and for each prime $p \equiv 3 \mod 4$ dividing $3n$:

- *$3 \nmid v_p(n)$ or*
- *$p = 3$ and $2 \nmid v_3(n)$ and $r_3(n) \not\equiv \pm 1 \mod 9$ or*
- *$p \neq 3$ and $2 \mid v_p(n)$ or there is no $z' \in \{0, \dots, p-1\}$ such that*
  $$p \mid r_p(n)^2 + r_p(n) z'^3 + z'^6.$$

Proof. See Theorem 5.13. □

For $m \in \mathbb{Z}$ and odd $k \geq 1$ an algorithm is given in Section 5.1, which determines whether m is of the form $x^2 + y^2 + z^k$ (again using Schinzel's hypothesis H).

Finally, lists of small positive integers not of the form $x^2 + y^2 + z^k$ are given for small odd k in Section 5.2.

2 Preliminaries

2.1 Definitions

For the rest of this thesis, let K be a number field, Ω the set of places of K and $\Omega_\infty \subseteq \Omega$ the set of archimedian places of K. Let K_v be the completion of K with respect to v for each $v \in \Omega$. Let $\mathcal{O}_v$ be the corresponding valuation ring for each $v \in \Omega \setminus \Omega_\infty$ and let $\mathcal{O}_v := K_v$ for each $v \in \Omega_\infty$. The valuation associated to $v \in \Omega \setminus \Omega_\infty$ is called v_v. The ring $\mathcal{O} := \{x \in K \mid v_v(x) \geq 0 \ \forall v \in \Omega \setminus \Omega_\infty\}$ is called the ring of integers of K.

Definition 2.1. A *variety* is an integral separated scheme of finite type over K.

In the following, X will always be a variety (or, depending on the context, a polynomial variable).

The set of R-rational points $X(R)$ obtains the induced topology for topological rings R.

Given a class of varieties, one often wants to know whether the existence of local solutions implies the existence of global solutions, or, even better, whether the existence of local integral solutions implies the existence of integral solutions. This leads to

Definition 2.2. Let S be a subset of Ω.

The set

$$\mathbb{A}_S := \left\{ (x_v)_{v \in \Omega \setminus S} \in \prod_{v \in \Omega \setminus S} K_v \;\middle|\; x_v \in \mathcal{O}_v \text{ for almost every } v \in \Omega \setminus S \right\}$$

is a ring by coordinatewise addition and multiplication.

The ring $\mathbb{A} := \mathbb{A}_\emptyset$ is called the *adele ring of* K.

The sets

$$\left\{ \prod_{v \in \Omega \setminus S} A_v \subseteq \prod_{v \in \Omega \setminus S} K_v \;\middle|\; A_v = \mathcal{O}_v \text{ for a.e. } v \in \Omega \setminus S \text{ and } A_v \text{ open in } K_v \text{ for all } v \in \Omega \setminus S \right\}$$

define a basis for the topology on $\mathbb{A}_S$.

The field K may for $S \subsetneq \Omega$ be diagonally embedded into $\mathbb{A}_S$ as for every $x \in K$ there are only finitely many v such that $x_v \notin \mathcal{O}_v$. Below, the images of these embeddings are identified with K.

Given a variety X and some $S \subsetneq \Omega$, obviously $X(K) \subseteq X(\mathbb{A}_S)$. It is of interest how $X(K)$ relates to $X(\mathbb{A}_S)$.

Definition 2.3. The variety X is said to satisfy the *Hasse principle* if and only if $X(\prod_v K_v) \neq \emptyset \Rightarrow X(K) \neq \emptyset$.

The variety X is said to satisfy *weak approximation* if and only if $\overline{X(K)} = X(\prod_v K_v)$ (where the closure is taken inside $X(\prod_v K_v)$), i.e., if and only if $X(K)$ is dense in $X(\prod_v K_v)$.

The variety X is said to satisfy *strong approximation away from $S \subset \Omega$* if and only if $\overline{X(K)} = X(\mathbb{A}_S)$ (where the closure is taken inside $X(\mathbb{A}_S)$), i.e., if and only if $X(K)$ is dense in $X(\mathbb{A}_S)$.

Remark 2.4. Weak approximation implies the Hasse principle.

Remark 2.5. If X satisfies strong approximation away from Ω_∞ and $X(\mathbb{A}_{\Omega_\infty}) \neq \emptyset$, then there is an integral point in $X(K)$.

Example 2.6 ([Neu92, III.§1 Exercise 1])**.** If $X = \operatorname{Spec} K[X]$, then X satisfies the Hasse principle, weak approximation and strong approximation away from every nonempty set $S \subset \Omega$.

2.2 Brauer-Manin obstruction

The following exposition is partly based on [Sko01] and [Gou09].

Lemma 2.7. *Let $A : X(K) \to \operatorname{Br}(K)$ and $A_v : X(K_v) \to \operatorname{Br}(K_v)$ (for every $v \in \Omega$) be maps, which "agree with A on $X(K)$", i.e., $A_v(x) = A(x) \otimes_K K_v$ for all $x \in X(K)$.*

Assume furthermore that for almost each $v \in \Omega$ for all $x \in X(\mathcal{O}_v)$ the following holds: $\operatorname{inv}_v(A_v(x)) = 0$

For each $T \subseteq X(\mathbb{A})$ let $T^A := \{(x_v)_v \in T \mid \sum_v \operatorname{inv}_v(A_v(x_v)) = 0\}$ (the sum is finite according to the previous assumption).

Then $X(K) \subseteq X(\mathbb{A})^A$.

If the map $s_A : X(\mathbb{A}) \to \mathbb{Q}/\mathbb{Z}, \quad (x_v)_v \mapsto \sum_v \operatorname{inv}_v(A_v(x_v)) = 0$ is continuous, then even $\overline{X(K)} \subseteq X(\mathbb{A})^A$.

Proof. Let $x \in X(K)$. According to the fundamental exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Br}(K) \arrow[r] & \bigoplus_{v\in\Omega} \operatorname{Br}(K_v) \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \\
 & B \arrow[r, mapsto] & (B \otimes_K K_v)_v & & \\
 & & (B_v)_v \arrow[r, mapsto] & \sum_v \operatorname{inv}_v(B_v) &
\end{tikzcd}$$

(cf. [Mil11, Thm. VIII.4.2]) we have $\sum_v \operatorname{inv}_v(A_v(x)) = \sum_v \operatorname{inv}_v(A(x) \otimes_K K_v) = 0$, i.e., $x \in X(\mathbb{A})^A$.

If s_A is continuous, then $X(\mathbb{A})^A = s_A^{-1}(0)$ is closed, which immediately yields the claim. □

Definition 2.8 ([Mil80, Chapter IV])**.** An $\mathcal{O}_X$-algebra A is called an *Azumaya algebra over* X, if it is coherent (i.e., there is some open covering by affine schemes $U_i \cong \operatorname{Spec} A_i$, such that $A|_{U_i} \cong \tilde{M}_i$ for some finitely generated A_i-module M_i for each i) and if $A(x) := A_x \otimes_{\mathcal{O}_{X,x}} \kappa(x)$ is a central simple algebra over $\kappa(x)$ for every $x \in X$.

If furthermore k is a field, then for each $x \in X(k)$ (i.e., each morphism $x : \operatorname{Spec} k \to X$ of schemes) let $A_k(x) := A_{x(\eta)} \otimes_{\mathcal{O}_{X,x(\eta)}} k$. The subscript will often be dropped: $A(x) = A_k(x)$

Remark 2.9. If A is an Azumaya algebra over X, then $A_k(x)$ is a central simple k-algebra for each $x \in X(k)$, as $A_{x(\eta)} \otimes_{\mathcal{O}_{X,x(\eta)}} \kappa(x(\eta))$ is a central simple $\kappa(x(\eta))$-algebra and k is a $\kappa(x(\eta))$-algebra by the morphism x, such that

$$A_k(x) \cong A_{x(\eta)} \otimes_{\mathcal{O}_{X,x(\eta)}} \kappa(x(\eta)) \otimes_{\kappa(x(\eta))} k \cong A(x(\eta)) \otimes_{\kappa(x(\eta))} k.$$

Theorem 2.10 ([Sko01, Chapter 5.2])**.** *Every Azumaya algebra A over X yields maps $A := A_K$ and $A_v := A_{K_v}$ which satisfy all assertions from Lemma 2.7. In fact the map $\operatorname{inv}_v \circ A_v : X(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z}$ is even locally constant. Hence $X(\mathbb{A})^A$ is open.*

Definition 2.11 ([Mil80, Chapter IV])**.** The *(Azumaya) Brauer group* of a variety X is the set of equivalence classes of Azumaya algebras over X with the following equivalence relation: $A \sim B \Leftrightarrow$ There are locally free $\mathcal{O}_X$-modules E, F of finite rank over $\mathcal{O}_X$ such that $A \otimes_{\mathcal{O}_X} \operatorname{End}_{\mathcal{O}_X}(E) \cong B \otimes_{\mathcal{O}_X} \operatorname{End}_{\mathcal{O}_X}(F)$.

We will often simply write A for the equivalence class of A.

Remark 2.12. $X(\mathbb{A})^A$ depends only on the equivalence class of A as $\operatorname{inv}_v(A_v(x))$ depends only on the equivalence class of $A_v(x)$ in $\operatorname{Br}(K_v)$.

Therefore the following definition makes sense:

Definition 2.13. Let

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

3 Azumaya algebra

Let $K = \mathbb{Q}$.
For each prime p and $x \in \mathbb{Q}_p^\times$ let $r_p(x) := \frac{x}{p^{v_p(x)}}$.

Lemma 3.1. *For each $v \in \Omega$ let $(\cdot,\cdot) : \mathbb{Q}_v^\times \times \mathbb{Q}_v^\times \to \{\pm 1\}$ denote the Hilbert symbol of degree 2 (i.e., $(a,b) = 1$ if and only if there exist $x, y \in \mathbb{Q}_v$ such that $a = y^2 - bx^2$).*
For each ring R of characteristic different from 2 and $a, b \in R^\times$ let $\left(\frac{a,b}{R}\right)$ denote the quaternion algebra over R with parameters a, b (i.e., it is a free R-module generated by some elements $1, i, j, ij$ and fulfills $i^2 = a$, $j^2 = b$ and $ji = -ij$).
Then for all $a \in \mathbb{Q}_v^\times$:

$$\begin{aligned}(a,-1) = 1 &\Leftrightarrow \exists x, y \in \mathbb{Q}_v : a = x^2 + y^2 \\ &\Leftrightarrow \operatorname{inv}_v \left(\frac{a,-1}{\mathbb{Q}_v}\right) = 0 \\ &\Leftrightarrow \begin{cases} a > 0, & v = \infty \\ r_2(a) \equiv 1 \mod 4, & v = 2 \\ 0 = 0, & v \equiv 1 \mod 4 \\ 2 \mid v_v(a), & v \equiv 3 \mod 4 \end{cases}\end{aligned}$$

Proof. See [Ser73, III.1, Theorem 1] and [GS06, Proposition 1.1.7]. □

Let $n \in \mathbb{Z} \setminus \{0\}$ and $a, b > 0$ be integers such that $n > 0$ or $2 \nmid ab$. Consider the equation

$$x^2 + y^2 + z^{ab} = n^a \tag{2}$$

Let

$$X := \operatorname{Spec} \mathbb{Q}[X,Y,Z]/(X^2 + Y^2 + Z^{ab} - n^a)$$

and

$$\mathfrak{X} := \operatorname{Spec} \mathbb{Z}[X,Y,Z]/(X^2 + Y^2 + Z^{ab} - n^a).$$

Let $U_1 := D(n - Z^b) \subseteq X$ and $U_2 := D(n^{a-1} + n^{a-2}Z^b + \cdots + nZ^{(a-2)b} + Z^{(a-1)b}) \subseteq X$. Consider the $\mathcal{O}_X|_{U_1}$-algebra

$$A_1 := \left(\frac{n - Z^b, -1}{\mathcal{O}_X(U_1)}\right)^\sim$$

and the $\mathcal{O}_X|_{U_2}$-algebra

$$A_2 := \left(\frac{n^{a-1} + \cdots + Z^{(a-1)b}, -1}{\mathcal{O}_X(U_2)}\right)^\sim.$$

As $a, n \in \mathbb{Q}^\times$, we have

$$V(n - Z^b) \cap V(n^{a-1} + \cdots + Z^{(a-1)b}) = V(n - Z^b, n^{a-1} + \cdots + Z^{(a-1)b}) = V(n - Z^b, an^{a-1}) = \emptyset.$$

Hence $U_1 \cup U_2 = X$.

Furthermore there is an $\mathcal{O}_X|_{U_1\cap U_2}$-algebra isomorphism $A_1|_{U_1\cap U_2} \xrightarrow{\sim} A_2|_{U_1\cap U_2}$ induced by

$$\begin{aligned} i &\mapsto \frac{Xi' + Yi'j'}{n^{a-1} + \cdots + Z^{(a-1)b}} \\ j &\mapsto j' \end{aligned}$$

where i, j and i', j' are the canonical generators of $A_1|_{U_1\cap U_2}$ and $A_2|_{U_1\cap U_2}$, respectively (this is an $\mathcal{O}_X|_{U_1\cap U_2}$-algebra isomorphism as $X^2-(-1)Y^2 = (n-Z^a)(n^{a-1}+\cdots+Z^{(a-1)b})$).

Hence A_1 and A_2 can be glued along $U_1 \cap U_2$ to get an $\mathcal{O}_X$-algebra A such that $A|_{U_1} \cong A_1$ and $A|_{U_2} \cong A_2$.

Quaternion algebras over fields (with nonzero arguments) are central simple algebras, so A is an Azumaya algebra.

Most of the rest of this section is devoted to calculating $I_v := \mathrm{inv}_v(A(\mathfrak{X}(\mathbb{Z}_v)))$ for all $v \in \Omega$ as a preparation for the main theorems in the following sections.

Obviously $\mathrm{inv}_v(A(x, y, z)) \in \{0, 1/2\}$ (remainders in $\mathbb{Q}/\mathbb{Z}$ will be denoted like numbers in $\mathbb{Q}$) as $\left(\frac{a,b}{k}\right) + \left(\frac{a,b}{k}\right) \sim k$ for each quaternion algebra $\left(\frac{a,b}{k}\right)$.

Furthermore

$$\begin{aligned} &\mathrm{inv}_v(A(x, y, z)) = 0 \Leftrightarrow (n - z^b, -1) = 1 && \text{if } n - z^b \neq 0 \quad \text{and} \\ &\mathrm{inv}_v(A(x, y, z)) = 0 \Leftrightarrow (n^{a-1} + \cdots + z^{(a-1)b}, -1) = 1 && \text{if } n^{a-1} + \cdots + z^{(a-1)b} \neq 0. \end{aligned}$$

Let $U := U_1 \cap U_2 = D(n^a - Z^{ab})$.

In the following, we are interested in strong approximation "at Z" away from ∞. To this end we choose a suitable topology:

In $\mathbb{Q}_v^3$ we equip the first two components (i.e., those belonging to the variables X and Y) with the indiscrete topology and the last one (i.e., that belonging to the variable Z) with the usual topology on $\mathbb{Q}_v$. Accordingly, the sets $X(\mathbb{A}) \subseteq \prod_v \mathbb{Q}_v^3$, $\mathfrak{X}(\mathbb{Z}_v) \subseteq \mathbb{Z}_v^3 \subseteq \mathbb{Q}_v^3$, etc. obtain the induced topologies.

It is then easy to see that $U(\mathbb{Q}_v)$ is dense in $X(\mathbb{Q}_v)$ and hence $U(\mathbb{Q}_v) \cap \mathfrak{X}(\mathbb{Z}_v)$ is dense in $\mathfrak{X}(\mathbb{Z}_v)$.

As $\mathrm{inv}_v \circ A : X(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z}$ is locally constant (even in the topology chosen above!), this implies that $a \in I_v$ if and only if there is some $L \in U(\mathbb{Q}_v) \cap \mathfrak{X}(\mathbb{Z}_v)$ such that $\mathrm{inv}_v(A(L)) = a$.

For each $z \in \mathbb{Z}_v$ there exist $x, y \in \mathbb{Z}_v$ such that $x^2 + y^2 = n^a - z^{ab}$ if and only if $(n^a - z^{ab}, -1) = 1$. Hence the problem of determining I_v can be simplified in the following way:

$$a \in I_v \Leftrightarrow \exists z \in \mathbb{Z}_v \text{ such that } (n^a - z^{ab}, -1) = 1 \text{ and } (n - z^b, -1) = \begin{cases} 1, & a = 0 \\ -1, & a = 1/2 \end{cases}$$

3.1 Place ∞

Lemma 3.2. $I_\infty = \{0\}$

Proof. $(0, 0, \sqrt[b]{n})$ is a real solution (as $n > 0$ or $2 \nmid b$), so $I_\infty \neq \emptyset$.
If $(x, y, z) \in U(\mathbb{R})$, then $n^a - z^{ab} = x^2 + y^2 \geq 0$ and $n > 0$ or $2 \nmid a$, so $n \geq z^b$. As $(x, y, z) \in U_1(\mathbb{R})$ we have $n \neq z^b$, i.e., $n - z^b > 0$, so $(n - z^b, -1) = 1$. Hence $\mathrm{inv}_\infty(A(x, y, z)) = 0$. □

3.2 Place 2

Lemma 3.3. *If $a = 1$ and b is odd, then $I_2 = \{0\}$.*

Proof. Due to $(n^a - z^{ab}, -1) = (n - z^b, -1)$ for $z \in \mathbb{Z}_2$ it is obvious that $I_2 \subseteq \{0\}$. The set I_2 is nonempty as there is some odd $z \in \mathbb{Z}_2$ such that $n - z \equiv 1$ or $2 \mod 8$ and this fulfills $n^a - z^{ab} \equiv n - z^b \equiv n - z \equiv 1$ or $2 \mod 8$ (as b and z are odd), so $(n^a - z^{ab}, -1) = 1$. □

Lemma 3.4. *If $r_2(n)^a \equiv 1 \mod 4$ then $I_2 \neq \emptyset$.*

Proof. Let $z := 0$. Then $r_2(n^a - z^{ab}) \equiv r_2(n)^a \equiv 1 \mod 4$, so $(n^a - z^{ab}, -1) = 1$. □

Lemma 3.5. *If $a \geq 2$ and $r_2(n)^a \equiv 1 \mod 4$ and $b \mid v_2(n) + 1$, then $I_2 = \{0, 1/2\}$.*

Proof. Let $z_1 := 0$ and $z_2 := 2^{(v_2(n)+1)/b}$. Now $r_2(n^a - z_1^{ab}) \equiv r_2(n)^a \equiv 1 \mod 4$ and $r_2(n^a - z_2^{ab}) \equiv r_2(r_2(n)^a - 2^a) \equiv r_2(n)^a \equiv 1 \mod 4$, so $(n^a - z_1^{ab}, -1) = (n^a - z_2^{ab}, -1) = 1$. Furthermore $r_2(n - z_1^b) \equiv r_2(n) \not\equiv r_2(n) - 2 \equiv r_2(r_2(n) - 2) \equiv r_2(n - z_2^b) \mod 4$, so $(n - z_1^b, -1) \neq (n - z_2^b, -1)$. □

Lemma 3.6. *If $a \geq 3$ and b are odd and $n \equiv 6 \mod 8$, then $1/2 \in I_2$.*

Proof. Let $z := -1$. Then $n^a - z^{ab} \equiv n^a + 1 \equiv 1 \mod 4$ and $n - z^b \equiv n + 1 \equiv 3 \mod 4$, so $1/2 \in I_2$. □

Lemma 3.7. *If $a, b \geq 3$ are odd and $n \equiv 6 \mod 8$, then $I_2 = \{1/2\}$.*

Proof. We know $1/2 \in I_2$ from the previous lemma.
Let $(x, y, z) \in U(\mathbb{Q}_2) \cap \mathfrak{X}(\mathbb{Z}_2)$.
If z is odd, then $n^{a-1} + \cdots + z^{(a-1)b} \equiv nz^{(a-2)b} + z^{(a-1)b} \equiv 2 + 1 \equiv 3 \mod 4$, so $(n^{a-1} + \cdots + z^{(a-1)b}, -1) = -1$.
If z is even, then

$$1 \equiv r_2(n^a - z^{ab}) \equiv r_2((n/2)^a - 2^{a(b-1)}(z/2)^{ab}) \equiv r_2(n/2)^a \equiv 3 \mod 4$$

yields a contradiction. □

Lemma 3.8. *If a, b are odd and $n \not\equiv 6 \mod 8$, then $0 \in I_2$.*

Proof. The values of z in the following table fulfill $r_2(n^a - z^{ab}) \equiv r_2(n - z^b) \equiv 1 \mod 4$:

$n \mod 8$	z
0	-1
1	0
2	0
3	1
4	-1
5	3
7	5

□

3.3 Odd places

Lemma 3.9. *$0 \in I_p$ for all odd primes p.*

Proof. n^a or $n^a - 1$ is not divisible by p. Set $z := 0$ or $z := 1$, respectively. Then $n^a - z^{ab}$ and hence $n - z^b$ are not divisible by p, so $(n^a - z^{ab}, -1) = (n - z^b, -1) = 1$. □

Hence it is only interesting whether $1/2 \in I_p$.

Lemma 3.10. *$I_p = \{0\}$ for all primes $p \equiv 1 \mod 4$.*

Proof. $I_p \neq \emptyset$ according to the previous lemma and $(t, -1) = 1$ for all $t \in \mathbb{Q}_p^\times$. □

Hence only the case $p \equiv 3 \mod 4$ is interesting, so let $p \equiv 3 \mod 4$ be prime for the rest of Section 3.3.

Lemma 3.11. *If $2 \mid a$ and $2 \nmid v_p(n)$, then $I_p = \{0, 1/2\}$.*

Proof. Take $z_1 := 1$ and $z_2 := 0$. Then

$$\begin{aligned}
(n^a - z_1^{ab}, -1) &= 1 && (\text{as } 2 \mid 0 = v_p(n^a - z_1^{ab}))\\
(n^a - z_2^{ab}, -1) &= 1 && (\text{as } 2 \mid a v_p(n) = v_p(n^a - z_2^{ab}))\\
(n - z_1^{b}, -1) &= 1 && (\text{as } 2 \mid 0 = v_p(n - z_1^{b}))\\
(n - z_2^{b}, -1) &= -1 && (\text{as } 2 \nmid v_p(n) = v_p(n - z_2^{b})).
\end{aligned}$$

□

Let a, b be odd for the rest of Section 3.3.
Then the following lemma simplifies the analysis of I_p.

Lemma 3.12. *Let $z \in \mathbb{Z}_p$ such that $n^a - z^{ab} \neq 0$. Then the following statements are equivalent:*

a) There are $x, y \in \mathbb{Z}_p$ such that $(x, y, z) \in \mathfrak{X}(\mathbb{Z}_p)$ and $\operatorname{inv}_v(A(x, y, z)) = 1/2$ (hence $1/2 \in I_p$).

b) $v_p(n) = v_p(z^b)$ and

$$\begin{aligned}
1 &\equiv v_p(r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}) && \mod 2\\
1 + v_p(n) &\equiv v_p(r_p(n) - r_p(z)^b) && \mod 2\\
v_p(n) &\equiv v_p(r_p(n)^a - r_p(z)^{ab}) && \mod 2.
\end{aligned}$$

Proof. a) ⇒ b) We must have (as $(n^{a-1} + \cdots + z^{(a-1)b}, -1) = -1$):

$$2 \nmid v_p(n^{a-1} + \cdots + z^{(a-1)b})$$

If $v_p(n) < v_p(z^b)$, then $2 \mid (a-1)v_p(n) = v_p(n^{a-1} + \cdots + z^{(a-1)b})$ yields a contradiction.

If $v_p(n) > v_p(z^b)$, then $2 \mid (a-1)v_p(z^b) = v_p(n^{a-1} + \cdots + z^{(a-1)b})$ yields a contradiction.

Hence $v_p(n) = v_p(z^b)$.

Then

$$\begin{aligned} 1 &\equiv v_p(n^{a-1} + \cdots + z^{(a-1)b}) \\ &\equiv (a-1)v_p(n) + v_p(r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}) \\ &\equiv v_p(r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}) \mod 2 \end{aligned}$$

and (as $(n - z^b, -1) = -1$)

$$\begin{aligned} 1 + v_p(n) &\equiv v_p(n) + v_p(n - z^b) \\ &\equiv 2v_p(n) + v_p(r_p(n) - r_p(z)^b) \\ &\equiv v_p(r_p(n) - r_p(z)^b) \mod 2 \end{aligned}$$

and (as $(n^a - z^{ab}, -1) = 1$)

$$\begin{aligned} v_p(n) &\equiv v_p(n) + v_p(n^a - z^{ab}) \\ &\equiv (a+1)v_p(n) + v_p(r_p(n)^a - r_p(z)^{ab}) \\ &\equiv v_p(r_p(n)^a - r_p(z)^{ab}) \mod 2. \end{aligned}$$

b) ⇒ a) From b) follows that

$$\begin{aligned} v_p(n^a - z^{ab}) &\equiv av_p(n) + v_p(r_p(n)^a - r_p(z)^{ab}) \\ &\equiv (a+1)v_p(n) \equiv 0 \mod 2, \end{aligned}$$

so there are $x, y \in \mathbb{Z}_p$ such that $(x, y, z) \in \mathfrak{X}(\mathbb{Z}_p)$.

Furthermore

$$v_p(n - z^b) \equiv v_p(n) + v_p(r_p(n) - r_p(z)^b) \equiv 1 \mod 2,$$

so $\mathrm{inv}_v(A(x, y, z)) = 1/2$. □

Remark 3.13. The sum of the first two congruences in statement b) is the third one.

Lemma 3.14. *Assume $p \nmid an$. Then $1/2 \notin I_p$.*

Proof. Suppose $(x, y, z) \in U(\mathbb{Q}_p) \cap \mathfrak{X}(\mathbb{Z}_p)$ and $\mathrm{inv}_p(A(x, y, z)) = 1/2$. Then $v_p(n - z^b)$ and $v_p(n^{a-1} + \cdots + z^{(a-1)b})$ are odd. Hence $n - z^b$ and $n^{a-1} + \cdots + z^{(a-1)b}$ have to be divisible by p, so together $p \mid an^{a-1}$. Therefore $p \mid an$. □

Lemma 3.15. *Assume $b \nmid v_p(n)$. Then $1/2 \notin I_p$.*

Proof. Suppose $(x, y, z) \in U(\mathbb{Q}_p) \cap \mathfrak{X}(\mathbb{Z}_p)$ and $\mathrm{inv}_p(A(x, y, z)) = 1/2$. According to Lemma 3.12 we have $v_p(n) = v_p(z^b)$, so $b \mid v_p(n)$. □

Lemma 3.16. *Let $p \nmid ab$. Then the following two statements are equivalent:*
a) $1/2 \in I_p$.
b) $b \mid v_p(n)$ *and* $2 \nmid v_p(n)$ *and there is some* $z' \in \mathbb{Z}$ *such that* $p \mid r_p(n)^{a-1} + \cdots + z'^{(a-1)b}$.

Proof. a) $\Rightarrow$ b) Let $(x, y, z) \in U(\mathbb{Q}_p) \cap \mathfrak{X}(\mathbb{Z}_p)$ such that $\mathrm{inv}_p(A(x, y, z)) = 1/2$.

Lemma 3.12 shows that $v_p(n) = v_p(z^b)$ (so $b \mid v_p(n)$).

It also shows that $2 \nmid v_p(r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b})$, so $p \mid r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}$.

If $2 \mid v_p(n)$, then, according to Lemma 3.12, $2 \nmid v_p(r_p(n) - r_p(z)^b)$. Hence $p \mid r_p(n) - r_p(z)^b$ and $p \mid r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}$. Together $p \mid ar_p(n)^{a-1}$, which is obviously impossible.

Therefore $2 \nmid v_p(n)$.

b) $\Rightarrow$ a) As $p \nmid ab$ and obviously $p \nmid z'$, we have

$$r_p(n)^a - z'^{ab} \not\equiv r_p(n)^a - z'^{ab} - abz'^{ab-1}p \equiv r_p(n)^a - (z' + p)^{ab} \mod p^2.$$

Hence $v_p(r_p(n)^a - z'^{ab}) \leq 1$ or $v_p(r_p(n)^a - (z' + p)^{ab}) \leq 1$. Let $z := p^{v_p(n)/b} z'$ or $z := p^{v_p(n)/b}(z' + p)$, respectively.

Therefore (as $p \mid r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}$)

$$1 \leq v_p(r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}) \leq v_p(r_p(n)^a - r_p(z)^{ab}) \leq 1,$$

so $v_p(r_p(n)^{a-1} + \cdots + r_p(z)^{(a-1)b}) = 1$ and $v_p(r_p(n)^a - r_p(z)^{ab}) \equiv 1 \equiv v_p(n) \mod 2$.

Then Lemma 3.12 (together with its remark) shows that $1/2 \in I_p$. □

Lemma 3.17. *Let* $a = b = 3$. *Then the following statements are equivalent:*
a) $1/2 \in I_3$.
b) Both

- $3 \mid v_3(n)$ *and*
- $2 \mid v_3(n)$ *or* $r_3(n) \equiv \pm 1 \mod 9$.

Proof. a) $\Rightarrow$ b) Let $(x, y, z) \in U(\mathbb{Q}_3) \cap \mathfrak{X}(\mathbb{Z}_3)$ and $\mathrm{inv}_3(A(x, y, z)) = 1/2$.

Lemma 3.12 shows that $v_3(n) = v_3(z^3)$ (so $3 \mid v_3(n)$) and

$$2 \nmid v_3(r_3(n)^2 + r_3(n)r_3(z)^3 + r_3(z)^6).$$

Therefore

$$\begin{aligned} 0 &\equiv r_3(n)^2 + r_3(n)r_3(z)^3 + r_3(z)^6 \\ &\equiv r_3(n)^2 + r_3(n)r_3(z) + r_3(z)^2 \\ &\equiv (r_3(n) - r_3(z))^2 \mod 3, \end{aligned}$$

so $r_3(n) \equiv r_3(z) \mod 3$.

If $r_3(n) \not\equiv \pm 1 \mod 9$, then

$$r_3(n) - r_3(z)^3 \equiv r_3(n) - r_3(n)^3 \equiv r_3(n)(1 - r_3(n))(1 + r_3(n)) \mod 9$$

is not congruent to 0 but divisible by 3. Hence (by Lemma 3.12)

$$1 \equiv v_3(r_3(n) - r_3(z)^3) \equiv 1 + v_3(n) \mod 2.$$

b) ⇒ a) Choose $z := 3^{v_3(n)/3} r_3(z)$ with $r_3(z)$ according to the following tables and apply Lemma 3.12.

Case $2 \mid v_3(n)$**:**

$r_3(n) \mod 81$	$r_3(z)$	$r_3(n) \mod 81$	$r_3(z)$	$r_3(n) \mod 81$	$r_3(z)$
1	10	28	1	55	1
2	2	29	2	56	2
4	1	31	1	58	1
5	2	32	2	59	2
7	1	34	1	61	1
8	11	35	2	62	2
10	4	37	4	64	13
11	2	38	2	65	2
13	1	40	1	67	1
14	2	41	2	68	2
16	1	43	1	70	1
17	5	44	14	71	5
19	16	46	7	73	7
20	2	47	2	74	2
22	1	49	1	76	1
23	2	50	2	77	2
25	1	52	1	79	1
26	17	53	8	80	8

Case $2 \nmid v_3(n)$ **and** $r_3(n) \equiv \pm 1 \mod 9$**:**

$r_3(n) \mod 27$	$r_3(z)$
1	4
8	5
10	1
17	2
19	1
26	2

□

3.4 Subsets of I_v

The following lemmas will not be statements on I_v but on subsets of it, namely ones corresponding to congruence conditions on the solutions.

Lemma 3.18. *If $b = 1$ and $n \equiv 1 \mod 4$ then*

$$\mathrm{inv}_2(A(\{(x, y, z) \in \mathfrak{X}(\mathbb{Z}_2) \mid z \equiv 2 \mod 4\})) \subseteq \{1/2\}.$$

Proof. Let now $(x, y, z) \in \mathfrak{X}(\mathbb{Z}_2)$ such that $z \equiv 2 \mod 4$. Then $r_2(n - z^b) \equiv 3 \mod 4$, so $(n - z^b, -1) = -1$. □

Lemma 3.19. *If $a \geq 3$ is odd, $b = 1$ and $n = p^2$ for some odd prime p not dividing a, then*

$$\mathrm{inv}_q(A(\{(x, y, z) \in \mathfrak{X}(\mathbb{Z}_q) \mid z \equiv 0 \mod a\})) \subseteq \{1/2\}$$

for each prime $q \equiv 3 \mod 4$.

Proof. Let $(x, y, z) \in \mathfrak{X}(\mathbb{Z}_q)$ and $z \equiv 0 \mod a$. Suppose $\mathrm{inv}_q(A(x, y, z)) \neq 0$.
Then $p^2 - z = 0$ or $v_q(p^2 - z)$ is odd. In the same manner $p^{2(a-1)} + \cdots + z^{a-1} = 0$ or $v_q(p^{2(a-1)} + \cdots + z^{a-1})$ is odd.
If $v_q(p^2) < v_q(z)$, then $2 \mid (a - 1)v_q(p^2) = v_q(p^{2(a-1)} + \cdots + z^{a-1}) < \infty$ yields a contradiction.
If $v_q(p^2) > v_q(z)$, then $2 \mid (a-1)v_q(z) = v_q(p^{2(a-1)} + \cdots + z^{a-1}) < \infty$ yields a contradiction.
Hence $v_q(p^2) = v_q(z)$.
Then $p^2 - z = 0$ or $2 \nmid v_q(p^2 - z) = v_q(p^2) + v_q(r_q(p^2) - r_q(z))$, so $q \mid r_q(p^2) - r_q(z)$.
Also $p^{2(a-1)} + \cdots + z^{a-1} = 0$ or

$$2 \nmid v_q(p^{2(a-1)} + \cdots + z^{a-1}) = (a - 1)v_q(p^2) + v_q(r_q(p)^{2(a-1)} + \cdots + r_q(z)^{a-1}),$$

so $q \mid r_q(p)^{2(a-1)} + \cdots + r_q(z)^{a-1}$. Together with $q \mid r_q(p^2) - r_q(z)$ this proves $q \mid ar_q(z)^{a-1}$, so (as obviously $q \nmid r_q(z)$): $q \mid a$. Furthermore z is divisible by a, so $q \mid z$. Using $v_q(p^2) = v_q(z)$ this proves $q \mid p^2$, so $q = p$ but this is a contradiction to $q \mid a$. □

Lemma 3.20. *If* $n \equiv 7 \mod 8$ *then*

$$\mathrm{inv}_2(A(\{(x,y,z) \in \mathfrak{X}(\mathbb{Z}_2) \mid \ 4 \mid z \text{ if } b = 1 \text{ and } 2 \mid z \text{ if } 2 \nmid b\})) \subseteq \{1/2\}.$$

Proof. Let $(x,y,z) \in \mathfrak{X}(\mathbb{Z}_2)$ such that $4 \mid z$ if $b = 1$ and $2 \mid z$ if $2 \nmid b$. If z is even, then $n - z^b \equiv 3 \mod 4$. If z is odd (hence $2 \mid b$), then $n - z^b \equiv 6 \mod 8$. □

Lemma 3.21. *If* $a = 2$, *then*

$$\mathrm{inv}_q(A(\{(x,y,z) \in \mathfrak{X}(\mathbb{Z}_q) \mid \gcd(n,z) = 1\})) \subseteq \{0\}$$

for each prime $q \equiv 3 \mod 4$.

Proof. Let $(x,y,z) \in \mathfrak{X}(\mathbb{Z}_q)$ such that $\gcd(n,z) = 1$. Assume $\mathrm{inv}_q(A(x,y,z)) \neq 0$. Then $n - z^b = 0$ or $2 \nmid v_q(n - z^b)$, so $q \mid n - z^b$. Furthermore $n + z^b = 0$ or $2 \nmid v_q(n + z^b)$, so $q \mid n + z^b$. Together $q \mid 2n$ and $q \mid 2z^b$ but this is impossible as $\gcd(n,z) = 1$ and $q \neq 2$. □

4 Failure of strong approximation

The following theorem explains failures of strong approximation away from ∞. Not all I_v have to be explicitly known to be able to apply it.

Theorem 4.1. *If $\mathfrak{X}(\mathbb{Z}_v) \neq \emptyset$ for each $v \in \Omega$ and if $|I_w| = 2$ for some $w \in \Omega$, then strong approximation "at Z" away from ∞ fails for the equation (2) due to Brauer-Manin obstruction.*

Proof. Let $L_v = L'_v \in \mathfrak{X}(\mathbb{Z}_v)$ for all $v \in \Omega \setminus \{w\}$ and $L_w, L'_w \in \mathfrak{X}(\mathbb{Z}_w)$ such that $\operatorname{inv}_w(A(L_w)) \neq \operatorname{inv}_w(A(L'_w))$. Then $\sum_{v\in\Omega} \operatorname{inv}_v(A(L_v)) \neq \sum_{v\in\Omega} \operatorname{inv}_v(A(L'_v))$. Hence $(L_v)_v$ or $(L'_v)_v \notin X(\mathbb{A})^A$, i.e., $(L_v)_v$ or $(L'_v)_v \notin \overline{X(\mathbb{Q})}$ although $(L_v)_v, (L'_v)_v \in X(\mathbb{A}_{\{\infty\}})$. □

Example 4.2. If $a \geq 2$ and $r_2(n)^a \equiv 1 \mod 4$ and $b \mid v_2(n) + 1$, then strong approximation "at Z" away from ∞ fails for (2) due to Brauer-Manin obstruction.

Proof. $\mathfrak{X}(\mathbb{Z}_v) \neq \emptyset$ for all $v \neq 2$ according to Lemmas 3.2 and 3.9. $|I_2| = 2$ according to Lemma 3.5. □

Example 4.3 (cf. Theorem 1)**.** According to the previous example the following equations do not fulfill strong approximation "at Z" away from ∞:

$$\begin{aligned} x^2 + y^2 + z^a &= n^a, \qquad a \geq 3 \text{ odd}, n \equiv 1 \mod 4 \\ x^2 + y^2 + z^a &= n^a, \qquad a \geq 2 \text{ even}, n > 0 \end{aligned}$$

Remark 4.4. Dietmann and Elsholtz showed in [DE08a] that for $k \geq 2$ and sufficiently large N the number of integers $0 < m \leq N$ such that $x^2 + y^2 + z^k = m$ does not fulfill strong approximation "at Z" away from ∞ is at least

$$\begin{cases} \frac{kN^{1/(2k)}}{\varphi(k)\log(N)}, & k \text{ odd} \\ \frac{N^{1/2}}{2\log(N)}, & k \text{ even} \end{cases}$$

The above example shows that this number is at least

$$\begin{cases} \frac{N^{1/k}+3}{4}, & k \text{ odd} \\ N^{1/k}, & k \text{ even} \end{cases}$$

The following example gives a better estimate.

Example 4.5. If $n > 0$ and $2 \mid a$ and n is not a sum of two squares, then strong approximation "at Z" away from ∞ fails for (2) due to Brauer-Manin obstruction.

Proof. There has to be some prime $p \equiv 3 \mod 4$ such that $2 \nmid v_p(n)$. Now $\mathfrak{X}(\mathbb{Z}_v) \neq \emptyset$ for all $v \in \Omega$ according to Lemmas 3.2, 3.4 and 3.9 and $|I_p| = 2$ according to Lemma 3.11. □

Unfortunately, Theorem 4.1 cannot explain the overall absence of integral solutions ($X(\mathbb{A})^A \neq \emptyset$ whenever its conditions are satisfied) and it does not return any explicit points which are not contained in $X(\mathbb{A})^A$. To accomplish this, I_v has to be explicitly computed for every $v \in \Omega$.

The following theorem is a generalization of the theorem in [JK95] (they gave an elementary proof for the case $a = b = 3$ and $n = 6q$ for primes $q \equiv 1 \mod 4$).

Theorem 4.6. *Let $a, b \geq 3$ be odd integers and $n \equiv 6 \mod 8$ such that $b \nmid v_p(n)$ for all prime divisors $p \equiv 3 \mod 4$ of an.*

Then (2) has no solutions in $\mathbb{Z}$ although it has v-adic integral solutions for each place v and this is explained by Brauer-Manin obstruction.

In particular, strong approximation away from ∞ fails.

Proof. $I_\infty = \{0\}$ according to Lemma 3.2. $I_p = \{0\}$ for all primes $p \equiv 1 \mod 4$ according to Lemma 3.10. $I_2 = \{1/2\}$ according to Lemma 3.7. $I_p = \{0\}$ for all primes $p \equiv 3 \mod 4$ according to Lemmas 3.9, 3.14 and 3.15.

Hence there are v-adic integral solutions for each v and $\sum_v \mathrm{inv}_v(A_v(x_v, y_v, z_v)) = 1/2$ for each $(x_v, y_v, z_v)_v \in \prod_v \mathfrak{X}(\mathbb{Z}_v)$. This implies $\mathfrak{X}(\mathbb{Z}) \subseteq X(\mathbb{A})^A \cap \mathfrak{X}(\mathbb{Z}) = \emptyset$. □

Remark 4.7. For odd $a, b \geq 3$ there is always an integer $n \equiv 6 \mod 8$ such that $b \nmid v_p(n)$ for all prime divisors $p \equiv 3 \mod 4$ of an, so there is an integer n such that (2) has no integral solutions.

Proof. Take

$$n := \begin{cases} 2\prod_{p|a} p, & \prod_{p|a} p \equiv 3 \mod 4 \\ 2q\prod_{p|a} p, & \prod_{p|a} p \equiv 1 \mod 4 \end{cases}$$

for some prime $q \equiv 3 \mod 4$. □

The following theorem has been proved elementarily in [DE08a, Thm. 1] in the case $p \equiv 1 \mod 4a$.

Theorem 4.8. *Let $a \geq 3$ be an odd integer, $b = 1$ and $p \in \mathbb{Z}$ an odd prime not dividing a such that $n = p^2$. Then (2) does not have any integral solution such that $z \equiv 2a \mod 4a$.*

However, there are v-adic integral solutions fulfilling $z \equiv 2a \mod 4a$ for each place v.

Hence the variety X does not fulfill strong approximation "at Z" away from ∞.

Proof. Let $I'_v := \mathrm{inv}_v(A(\{(x, y, z) \in \mathfrak{X}(\mathbb{Z}_v) \mid z \equiv 2a \mod 4a\}))$ for each $v \in \Omega$.

$I'_\infty = I_\infty = \{0\}$ according to Lemma 3.2. $I'_q \subseteq I_q = \{0\}$ for all primes $q \equiv 1 \mod 4$ according to Lemma 3.10 . $I'_q \neq \emptyset$ for all primes $q \equiv 1 \mod 4$ (you can take $z := 2a$). $I'_2 \subseteq \{1/2\}$ according to Lemma 3.18. $I'_2 \neq \emptyset$ (you can take $z := 2$). $I'_q \subseteq \{0\}$ for all primes $q \equiv 3 \mod 4$ according to Lemma 3.19. $I'_q \neq \emptyset$ for all primes $q \equiv 3 \mod 4$ (you can take $z := 2a$ if $q \mid a$ and $z := 0$ otherwise).

Hence altogether $\sum_v \operatorname{inv}_v(A_v(x_v, y_v, z_v)) = 1/2$ for each $(x_v, y_v, z_v)_v \in \prod_v \mathfrak{X}(\mathbb{Z}_v)$ such that $z \equiv 2a \mod 4a$.

This implies that there are no integers x, y, z fulfilling (2) and $z \equiv 2a \mod 4a$ (according to the fundamental exact sequence). □

In [DE08a, Thm. 2 and 3] (and in the case $a = b = 2$ in [DE08b]) Dietmann and Elsholtz showed

- that there are no nontrivial solutions $x, y, z \in \mathbb{Z}$ to (2) if $n \equiv 7 \mod 8$ is prime, $a = 2$ and $2 \mid b$ and
- that there are no nontrivial solutions $x, y, z \in \mathbb{Z}$ to (2) fulfilling $4 \mid z$ if $2 \nmid b$ if $n \equiv 7 \mod 8$ is prime.

Theorem 4.9. *Let $a = 2$ and $n \equiv 7 \mod 8$. Then (2) does not have any integral solution such that*

- $\gcd(n, z) = 1$ *and*
- $4 \mid z$ *if* $b = 1$ *and*
- $2 \mid z$ *if* $2 \nmid b$.

However, there are v-adic integral solutions fulfilling the above constraints for each place v.

Hence in this case the variety X does not fulfill strong approximation "at Z" away from ∞.

Proof. Let $I'_v := \operatorname{inv}_v(A(\{(x, y, z) \in \mathfrak{X}(\mathbb{Z}_v) \mid z \text{ as above}\}))$ for each $v \in \Omega$.

$I'_\infty = I_\infty = \{0\}$ according to Lemma 3.2. $I'_p \subseteq I_p = \{0\}$ for all primes $p \equiv 1 \mod 4$ according to Lemma 3.10. $I'_p \neq \emptyset$ for all primes $p \equiv 1 \mod 4$ (you can take $z := 4$). $I'_2 \subseteq \{1/2\}$ according to Lemma 3.20. $I'_2 \neq \emptyset$ (you can take $z := 4$). $I'_p \subseteq \{0\}$ for all primes $p \equiv 3 \mod 4$ according to Lemma 3.21. $I'_p \neq \emptyset$ for all primes $p \equiv 3 \mod 4$ (you can take $z := 0$ if $p \nmid n$ and $z := 1$ if $p \mid n$).

Hence $\sum_v \operatorname{inv}_v(A_v(x_v, y_v, z_v)) = 1/2 \neq 0$ for each $(x_v, y_v, z_v)_v \in \prod_v \mathfrak{X}(\mathbb{Z}_v)$ fullfilling the given congruence conditions.

This implies that there are no integers x, y, z fulfilling (2) and the above constraints (according to the fundamental exact sequence). □

5 Fulfillment of strong approximation

Lemma 5.1. *Let a, b be odd. Then there exist v-adic integral solutions for each place v.*

Proof. See Lemmas 3.2, 3.3, 3.6, 3.8 and 3.9. □

Let $k \geq 3$ be an odd integer and $m \in \mathbb{Z} \setminus \{0\}$.

Davenport and Heilbronn showed in [DH37], that for all except $o(N)$ integers $1 \leq m \leq N$ the equation

$$x^2 + y^2 + z^k = m \tag{3}$$

has a solution with $x, y, z \in \mathbb{Z}$.

As above, let

$$X := \operatorname{Spec} \mathbb{Q}[X, Y, Z]/(X^2 + Y^2 + Z^k - m)$$

and

$$\mathfrak{X} := \operatorname{Spec} \mathbb{Z}[X, Y, Z]/(X^2 + Y^2 + Z^k - m)$$

and

$$U := D(m - Z^k) \subseteq X.$$

Given k and m there may be multiple triples (a, b, n) of integers with $a, b > 0$ such that $k = ab$ and $m = n^a$, i.e., there may be multiple Azumaya algebras to consider for Brauer-Manin obstruction.

Let therefor $S(a, b, n) := \mathfrak{X}\left(\prod_v \mathbb{Z}_v\right)^A$ with A defined as in Section 3 and let $I_v(a, b, n) := I_v$ as defined in Section 3.

Then we can define the subset L of the solutions in $\mathbb{A}$ to equation (3) for which there is no Brauer-Manin obstruction corresponding to any Azumaya algebra from Section 3:

$$L := \bigcap_{\substack{a,b,n \in \mathbb{Z}: \\ a,b>0, \\ k=ab, \\ m=n^a}} S(a, b, n)$$

Of course, $\mathfrak{X}(\mathbb{Z}) \subseteq L$.

The next theorem will show that Brauer-Manin obstruction with such Azumaya algebras explains all failures of strong approximation "at Z" away from ∞ if Schinzel's Hypothesis H is true.

Lemma 5.2. *Let K be a field, $k \geq 1$ an odd integer and $u \in K$ such that u is not a p-th power in K for any prime divisor p of k.*

Then $[K(\sqrt[k]{u}) : K] = k$.

Proof. See [Lan05, Thm. VI.9.1]. □

Lemma 5.3. *Let $d, b \geq 1$ be odd integers and $n \in \mathbb{Q}$ such that n is not a p-th power for any prime divisor p of b.*
Then $\phi_d(X^b/n) \in \mathbb{Q}[X]$ is irreducible (where ϕ_d is the d-th cyclotomic polynomial).

Proof. The polynomial $\phi_d(X^b/n)$ has a root $\sqrt[b]{n} \cdot \zeta_{bd}$. Assume $\phi_d(X^b/n)$ is reducible. Hence (as $\deg \phi_d(X^b/n) = b\varphi(d)$)

$$[\mathbb{Q}(\sqrt[b]{n} \cdot \zeta_{bd}) : \mathbb{Q}(\zeta_d)]\varphi(d) = [\mathbb{Q}(\sqrt[b]{n} \cdot \zeta_{bd}) : \mathbb{Q}(\zeta_d)] \cdot [\mathbb{Q}(\zeta_d) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[b]{n} \cdot \zeta_{bd}) : \mathbb{Q}] < b\varphi(d),$$

so $[\mathbb{Q}(\sqrt[b]{n} \cdot \zeta_{bd}) : \mathbb{Q}(\zeta_d)] < b$. Lemma 5.2 therefore implies that $n \cdot \zeta_d$ is a p-th power in $\mathbb{Q}(\zeta_d)$ for some prime divisor p of b, say $x \in \mathbb{Q}(\zeta_d)$ and $x^p = n \cdot \zeta_d$.

Case $p \mid d$**:** Then $(x/\overline{x})^p = \zeta_d^2$, but this is impossible as the roots of unity in $\mathbb{Q}(\zeta_d)$ are μ_{2d} but $\mu_{2d}^p = \mu_{2d/p} \not\ni \zeta_d^2$.

Case $p \nmid d$**:** Let then $r \in \mathbb{Z}$ such that $rp \equiv 1 \mod d$. Hence for $y := x/\zeta_d^r$ we have

$$y^p = \frac{x^p}{\zeta_d^{rp}} = \frac{n \cdot \zeta_d}{\zeta_d} = n,$$

so in particular every $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_d)|\mathbb{Q})$ fulfills $(\tau y)^p = \tau y^p = y^p$. Therefore $(\tau y/y)^p = 1$ but this is only possible if $\tau y = y$ as $\mathbb{Q}(\zeta_d)$ contains no primitive p-th root of unity. Hence we conclude that $y \in \mathbb{Q}$. This yields a contradiction as $y^p = n$ but n is not a p-th power in $\mathbb{Q}$ by assumption. □

Lemma 5.4. *Let $f_1, \ldots, f_s \in \mathbb{Z}[X]$ be polynomials irreducible in $\mathbb{Q}[X]$ such that*

$$\gcd\{f_1(x) \cdots f_s(x) \mid x \in \mathbb{Z}\} = 1$$

and $f_i(x) \to \infty$ for $x \to \infty$ for each $1 \leq i \leq s$. Let furthermore $c, e \in \mathbb{Z}$ such that $v_p(f_i(c)) \leq v_p(e)$ for all prime divisors p of e and each i. Assume Schinzel's hypothesis H is true. Then there is some $x \equiv c \mod e$ such that $\frac{f_i(x)}{\gcd(f_i(c),e)}$ is prime for each i.

Proof. Let $g_i(X) := \frac{f_i(eX+c)}{\gcd(f_i(c),e)}$. Obviously $g_i \in \mathbb{Z}[X]$ and g_i is irreducible in $\mathbb{Q}[X]$.
Assume that p is a prime divisor of $\gcd\{g_1(x) \cdots g_s(x) \mid x \in \mathbb{Z}\}$.

Case $p \nmid e$**:** There must be some $y \in \mathbb{Z}$ such that $p \nmid f_1(y) \cdots f_s(y)$. As $p \nmid e$, there is some $r \in \mathbb{Z}$ such that $er + c \equiv y \mod p$. Then

$$p \mid g_1(r) \cdots g_s(r) \mid f_1(er+c) \cdots f_s(er+c),$$

so $0 \equiv f_1(er+c) \cdots f_s(er+c) \equiv f_1(y) \cdots f_s(y) \mod p$ yields a contradiction.

Case $p \mid e$**:** Then $v_p(f_i(c)) \leq v_p(e)$ and hence $p \nmid \frac{f_i(c)}{\gcd(f_i(c),e)} = g_i(0)$ for each i. Therefore $p \nmid g_1(0) \cdots g_s(0)$, which is a contradiction too.

Hence $\gcd\{g_1(x) \cdots g_s(x) \mid x \in \mathbb{Z}\} = 1$ and $g_i \in \mathbb{Z}[X]$ is irreducible for each i, so Schinzel's hypothesis H implies that there is some $z \in \mathbb{Z}$ such that $g_i(z) = \frac{f_i(ez+c)}{\gcd(f_i(c),e)}$ is prime for each i. The claim follows with $x := ez + c$. □

Theorem 5.5 (cf. Theorem 2)**.** *If Schinzel's hypothesis H is true, then* $\overline{\mathfrak{X}(\mathbb{Z})} = L$.

Proof. Let a be the largest divisor of k such that m is an a-th power. Let $n := \sqrt[a]{m}$ and $b := \frac{k}{a}$.

Consider the factorization[1]

$$X^{ab} + n^a = -n^a \left(\left(-\frac{X^b}{n} \right)^a - 1 \right) = -n^a \prod_{d|a} \phi_d \left(-\frac{X^b}{n} \right) = \prod_{d|a} (-n)^{\varphi(d)} \phi_d \left(-\frac{X^b}{n} \right).$$

The last equality follows from the fact that $\sum_{d|a} \varphi(d) = a$.

Let $f_d(X) := (-n)^{\varphi(d)} \phi_d \left(-\frac{X^b}{n} \right)$ for each divisor d of a.

The polynomials $f_d(X) \in \mathbb{Q}[X]$ are irreducible according to Lemma 5.3 and the choice of a.

Moreover $f_d(X) \in \mathbb{Z}[X]$ as $\phi_d(Y)$ has integral coefficients and degree $\varphi(d)$.

Take $(x_v, y_v, z_v)_v \in L$, a finite set $T \subseteq \Omega \setminus \{\infty\}$ and $t \geq 0$. We have to show that there is some $(x, y, z) \in \mathfrak{X}(\mathbb{Z})$ such that $v_p(z_p - z) \geq t$ for all $p \in T$.

As $U(\mathbb{Q}_v) \cap \mathfrak{X}(\mathbb{Z}_v)$ is dense in $\mathfrak{X}(\mathbb{Z}_v)$ for each $v \in \Omega$ and L is open (cf. Theorem 2.10), we can assume that $n^a - z_p^{ab} \neq 0$ for all primes p.

> **Claim:** For each $d \mid a$ we have $\prod_p (f_d(-z_p), -1) = 1$ where the product runs over all primes p (in particular $(f_d(-z_p), -1) = 1$ for almost all primes p).
>
> *Proof:* Assume $d \mid a$ is minimal such that the claim does not hold.
>
> The factors $(f_d(-z_p), -1)$ are welldefined as $f_d(-z_p) \neq 0$ due to $n^a - z_p^{ab} \neq 0$.
>
> As $(x_v, y_v, z_v)_v \in S(\frac{a}{d}, db, n^d)$, we conclude that $\prod_p (n^d - z_p^{db}, -1) = 1$. But
>
> $$X^{db} + n^d = \prod_{d'|d} (-n)^{\varphi(d')} \phi_{d'} \left(-\frac{X^b}{n} \right) = \prod_{d'|d} f_{d'}(X),$$
>
> so $n^d - z_p^{db} = \prod_{d'|d} f_{d'}(-z_p)$.
>
> Hence
>
> $$(f_d(-z_p), -1) = \frac{(n^d - z_p^{db}, -1)}{\prod_{d'|d,\ d'<d} (f_{d'}(-z_p), -1)},$$
>
> so (due to the minimality of d) the factors $(f_d(-z_p), -1)$ are almost all equal to 1 and
>
> $$\prod_p (f_d(-z_p), -1) = \frac{\prod_p (n^d - z_p^{db}, -1)}{\prod_{d'|d,\ d'<d} \prod_p (f_{d'}(-z_p), -1)} = 1.$$

□

[1] Below, "divisor" will mean "*positive* divisor".

Assume without loss of generality that $2 \in T$ and that for each prime p: If $p \in T$, then $t \geq v_p(f_d(-z_p)) + 2$ and if $(f_d(-z_p), -1) \neq 1$ for some $d \mid a$, then $p \in T$.

Let now $e := \prod_{p \in T} p^t$.

The leading coefficient of $f_d(X)$ is 1 and its degree is $b\varphi(d) > 0$, so $f_d(u) \to \infty$ for $u \to \infty$.

Futhermore $\gcd\{\prod_{d|a} f_d(u) \mid u \in \mathbb{Z}\} = \gcd\{u^{ab} + n^a \mid u \in \mathbb{Z}\} \mid \gcd(n^a, 1 + n^a) = 1$.

The Chinese remainder theorem shows that there is some $c \in \mathbb{Z}$ such that for each $p \in T$: $c \equiv -z_p \mod p^t$

Now $v_p(f_d(c)) = v_p(f_d(-z_p)) \leq t - 1 \leq v_p(e)$ for each $p \in T$.

Hence applying Lemma 5.4 proves that there is some $z \in \mathbb{Z}$ such that $-z \equiv c \mod e$ (in particular $v_p(z_p - z) \geq \min(v_p(z_p + c), v_p(-z - c)) \geq t$ for each prime $p \in T$) and $\frac{f_d(-z)}{\gcd(f_d(c),e)}$ is prime for each $d \mid a$.

Therefore $f_d(-z) \equiv f_d(c) \equiv f_d(-z_p) \mod p^t$, so in particular $v_p(f_d(-z)) = v_p(f_d(-z_p))$ and $r_p(f_d(-z)) \equiv r_p(f_d(-z_p)) \mod p^2$ as $t \geq v_p(f_d(-z_p)) + 2$ for each $p \in T$.

Hence $r_2(f_d(-z)) \equiv r_2(f_d(-z_2)) \mod 4$. As $\prod_p (f_d(-z_p), -1) = 1$ and moreover $p \in T$ whenever $(f_d(-z_p), -1) \neq 1$ (i.e., whenever $p^{v_p(f_d(-z_p))} \not\equiv 1 \mod 4$), the following congruence holds:

$$r_2(f_d(-z_2)) \equiv \prod_{p \neq 2} p^{v_p(f_d(-z_p))} \equiv \prod_{p \in T \setminus \{2\}} p^{v_p(f_d(-z_p))} \equiv r_2(\gcd(f_d(c), e)) \mod 4$$

Together we get $r_2(f_d(-z)) \equiv r_2(\gcd(f_d(c), e)) \mod 4$, so $r_2\left(\frac{f_d(-z)}{\gcd(f_d(c),e)}\right) \equiv 1 \mod 4$. As $\frac{f_d(-z)}{\gcd(f_d(c),e)}$ is prime, it is therefore a sum of two squares.

The product
$$\prod_{d|a} \gcd(f_d(c), e) = \prod_{p \in T} \prod_{d|a} p^{v_p(f_d(-z_p))} = \prod_{p \in T} p^{v_p(n^a - z_p^{ab})}$$
is also a sum of two squares as all primes $p \equiv 3 \mod 4$ occur an even number of times in it because they do so in $n^a - z_p^{ab} = x^2 + y^2$.

Now in the factorization
$$n^a - z^{ab} = \prod_{d|a} f_d(-z) = \prod_{d|a} \gcd(f_d(c), e) \cdot \prod_{d|a} \frac{f_d(-z)}{\gcd(f_d(c), e)}$$
the first product and each factor of the second product are sums of two squares, so $n^a - z^{ab}$ is a sum of two squares, too. □

Lemma 5.6. *$S(1, k, m) = \mathfrak{X}(\prod_v \mathbb{Z}_v)$.*

Proof. For each place v and $(x_v, y_v, z_v) \in U(\mathbb{Q}_v) \cap \mathfrak{X}(\mathbb{Z}_v)$ is
$$(m - z^k, -1) = (m^1 - z^{1 \cdot k}, -1) = 1,$$
so $\mathrm{inv}_v(A(x_v, y_v, z_v)) = 0$. □

Corollary 5.7. *Assume Schinzel's hypothesis H is true.*

Let k be an odd positive integer and assume that m is not a p-th power for any prime $p \mid k$. Then there exists an integral solution to equation (3)*.*

Proof. Then $\overline{\mathfrak{X}(\mathbb{Z})} = L = S(1, k, n) = \mathfrak{X}(\prod_v \mathbb{Z}_v) \neq \emptyset$ according to Lemmas 3.2, 3.3 and 3.9. □

Remark 5.8. The proof of Corollary 5.7 needs Schinzel's hypothesis H only in the case of one polynomial, also known as Bunyakovsky's conjecture.

Remark 5.9. This corollary includes the result of Davenport and Heilbronn mentioned above if Bunyakovsky's conjecture is true.

Corollary 5.10 (cf. Theorem 3)**.** *Assume Bunyakovsky's conjecture is true.*

Let k be an odd prime. Then there exists an integral solution to equation (3)*.*

Proof. If m is a k-th power, then $(0, 0, \sqrt[k]{m})$ is a solution. Otherwise the previous corollary applies. □

Lemma 5.11. *Let a, b be odd primes and $m \in \mathbb{Z} \setminus \{0\}$.*

Then the following statements are equivalent if Schinzel's hypothesis H is true. Otherwise at least a) $\Rightarrow$ b).

a) There exist $x, y, z \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^{ab} = m.$$

b) There is no $n \in \mathbb{Z}$ such that $m = n^a$ and $0 \notin I_2(a, b, n)$ and $1/2 \notin I_p(a, b, n)$ for each prime $p \equiv 3 \mod 4$ and
there is no $n \in \mathbb{Z}$ such that $m = n^b$ and $0 \notin I_2(b, a, n)$ and $1/2 \notin I_p(b, a, n)$ for each prime $p \equiv 3 \mod 4$.

Proof.

a) $\Rightarrow$ b) Assume without loss of generality that $n \in \mathbb{Z}$ and $m = n^a$ and $0 \notin I_2(a, b, n)$ and $1/2 \notin I_p(a, b, n)$ for each prime $p \equiv 3 \mod 4$. Then, according to Lemmas 3.2 and 3.10, $S(a, b, n) = \emptyset$. Hence $\mathfrak{X}(\mathbb{Z}) \subseteq S(a, b, n) = \emptyset$.

b) $\Rightarrow$ a) If m is an ab-th power, then $(0, 0, \sqrt[ab]{m})$ is a solution.

If m is neither an a-th power nor a b-th power, then Corollary 5.7 proves the claim.

Let therefore without loss of generality m be an a-th power but not an ab-th power, so there is some $n \in \mathbb{Z}$ such that $m = n^a$. Now b) implies that $0 \in I_2(a, b, n)$ or $1/2 \in I_p(a, b, n)$ for some prime $p \equiv 3 \mod 4$. Together with Lemmas 3.2, 3.7, 3.8 and 3.9 this shows that $S(a, b, n) \neq \emptyset$.

Moreover $S(1, ab, m) = \mathfrak{X}(\prod_v \mathbb{Z}_v)$ according to Lemma 5.6.

Hence $\overline{\mathfrak{X}(\mathbb{Z})} = S(1, ab, m) \cap S(a, b, n) = S(a, b, n) \neq \emptyset$. □

Theorem 5.12 (cf. Theorem 4)**.** *Let $a, b \equiv 1 \mod 4$ be primes and $m \in \mathbb{Z} \setminus \{0\}$. Then the following statements are equivalent if Schinzel's hypothesis H is true. Otherwise at least a) $\Rightarrow$ b).*

a) There exist $x, y, z \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^{ab} = m.$$

b) The following two statements are true:

- *There is no $n \equiv 6 \mod 8$ such that $m = n^a$ and for each prime $p \equiv 3 \mod 4$ dividing n:*
  $b \nmid v_p(n)$ or $2 \mid v_p(n)$ or there is no $z' \in \{0, \dots, p-1\}$ such that
  $$p \mid r_p(n)^{a-1} + \dots + z'^{(a-1)b}.$$
- *There is no $n \equiv 6 \mod 8$ such that $m = n^b$ and for each prime $p \equiv 3 \mod 4$ dividing n:*
  $a \nmid v_p(n)$ or $2 \mid v_p(n)$ or there is no $z' \in \{0, \dots, p-1\}$ such that
  $$p \mid r_p(n)^{b-1} + \dots + z'^{(b-1)a}.$$

Proof. Statement b) of Lemma 5.11 is equivalent to statement b) of this theorem according to Lemmas 3.7, 3.8, 3.14 and 3.16. □

Theorem 5.13 (cf. Theorem 5)**.** *Let $m \in \mathbb{Z} \setminus \{0\}$. The following statements are equivalent if Schinzel's hypothesis H is true. Otherwise at least a) $\Rightarrow$ b).*

a) There exist $x, y, z \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^9 = m.$$

b) There is no integer $n \equiv 6 \mod 8$ such that $m = n^3$ and for each prime $p \equiv 3 \mod 4$ dividing $3n$:

- *$3 \nmid v_p(n)$ or*
- *$p = 3$ and $2 \nmid v_3(n)$ and $r_3(n) \not\equiv \pm 1 \mod 9$ or*
- *$p \neq 3$ and $2 \mid v_p(n)$ or there is no $z' \in \{0, \dots, p-1\}$ such that*
  $$p \mid r_p(n)^2 + r_p(n)z'^3 + z'^6.$$

Proof. Statement b) of Lemma 5.11 is equivalent to statement b) of this theorem according to Lemmas 3.7, 3.8, 3.14, 3.16 and 3.17. □

5.1 Algorithm

We give an algorithm to decide for given $m \in \mathbb{Z}$ and odd $k > 0$ if the number m is of the form $x^2 + y^2 + z^k$.

```
function COMBI($a, b, n, p$)
    Consider all Hilbert symbols over $\mathbb{Q}_p$.
    Let $f_d(Z) := (-n)^{\varphi(d)} \phi_d(-Z^b/n)$.
    For each $z \in \mathbb{Z}$ let $w_z := \{d$ divisor of $a \mid (f_d(-z), -1) \neq 1\}$.
    For each $z \in \mathbb{Z}$ and $t \geq 0$ let $G_{t,z} := \{d$ divisor of $a \mid v_p(f_d(-z)) + 1 \geq t\}$.
    if $p \equiv 1 \mod 4$ then
        return $\{\emptyset\}$
    else
        $W \leftarrow \emptyset$
        $S_0 \leftarrow \{0\}$
        $t \leftarrow 0$
        while $S_t \neq \emptyset$ do
            $S_{t+1} \leftarrow \emptyset$
            for all $z \in S_t$ do
                if $(n^a - z^{ab}, -1) = 1$ then
                    $W \leftarrow W \cup \{w_z\}$
                end if
                if $|G_{t,z}| > 1$ or ($|G_{t,z}| = 1$ and $w_z \setminus G_{t,z} \notin W$ and $w_z \cup G_{t,z} \notin W$) then
                    $S_{t+1} \leftarrow S_{t+1} \cup \{z' \in [0, p^{t+1} - 1] \mid z' \equiv z \mod p^t\}$
                end if
            end for
            $t \leftarrow t + 1$
        end while
        return $W$
    end if
end function
```

Lemma 5.14. *Let $a \geq 1$ and $b \geq 3$ be odd integers, n an integer such that n is not a q-th power for any prime divisor q of b (then $n^a - z^{ab} \neq 0$ for all $z \in \mathbb{Z}$) and let p be prime.*

Use the notation from lines 2 to 5 above.

Then COMBI(a, b, n, p) *terminates and returns*

$$C := \{w_z \mid z \in \{0, 1, 2, \dots\} \text{ such that } (n^a - z^{ab}, -1) = 1\}.$$

Proof. For $p \equiv 1 \mod 4$ the result is immediate, so let $p \not\equiv 1 \mod 4$.

The algorithm describes a pruned breadth-first search on the infinite directed graph with the following node set V and edge set E:

$$V := \{(t, z) \mid t \geq 0 \text{ and } 0 \leq z \leq p^t - 1\}$$

$$E := \{((t, z), (t + 1, z')) \in V^2 \mid z \equiv z' \mod p^t\}$$

Each time a node (t, z) with $(n^a - z^{ab}, -1) = 1$ is visited, w_z is appended to $W \subseteq C$.

In this graph there is a path from $(t, z) \in V$ to $(t', z') \in V$ if and only if $t \leq t'$ and $z \equiv z' \mod p^t$.

Obviously every node can be reached from $(0, 0)$.

Therefore a complete breadth-first search would eventually find every $c \in C$.

Let (t, z) and (t', z') be nodes such that (t', z') is reachable from (t, z), i.e., $z' \equiv z \mod p^t$. If $d \notin G_{t,z}$ is a divisor of a, then $v_p(f_d(-z)) < t - 1$. Then $f_d(-z') \equiv f_d(-z) \mod p^t$ implies $v_p(f_d(-z')) = v_p(f_d(-z))$ and $r_p(f_d(-z')) \equiv r_p(f_d(-z)) \mod p^2$, so $(f_d(-z'), -1) = (f_d(-z), -1)$. Hence $w_{z'} \setminus G_{t,z} = w_z \setminus G_{t,z}$.

In particular $w_{z'} = w_z$ if $G_{t,z} = \emptyset$. Therefore the breadth-first search does not have to be continued from (t, z) on if $G_{t,z} = \emptyset$.

Every set $c \in C$ has an even number of elements as $\prod_{d|a}(f_d(-z), -1) = (n^a - z^{ab}, -1)$ for each $z \in \mathbb{Z}$. Hence for each subset w' of the set of divisors of a and each divisor g of a at least one of the sets $w' \setminus \{g\}$ and $w' \cup \{g\}$ is not contained in C.

Therefore, if $G_{t,z} = \{g\}$ for some divisor g of a and $w_z \setminus \{g\}$ or $w_z \cup \{g\}$ has already been found (and is therefore contained in C), then the breadth-first search does not have to be continued from (t, z), either.

Hence altogether the above algorithm finds every element of C, so the only remaining question is whether it terminates in a finite amount of time.

Assume it does not.

Then there has to be an infinite path $(0, z_0) \to (1, z_1) \to (2, z_2) \to \dots$ of which every edge is visited during the breadth-first search.

The definition of the edge set E proves that z_t converges to some $\overline{z} \in \mathbb{Z}_p$ such that $\overline{z} \equiv z_t \mod p^t$ for each $t \geq 0$.

If $d \in G_{t+1,z_{t+1}}$, then $f_d(-z_t) \equiv f_d(-z_{t+1}) \equiv 0 \mod p^t$, so $d \in G_{t,z_t}$.

Hence $G_{0,z_0} \supseteq G_{1,z_1} \supseteq G_{2,z_2} \supseteq \dots$.

If G_{t,z_t} was empty for some t, then the breadth-first search would not continue from the node (t, z_t) on.

Hence $\bigcap_{t \geq 0} G_{t,z_t} \neq \emptyset$.

If $g \in \bigcap_{t \geq 0} G_{t,z_t}$, then $f_g(-\overline{z}) \equiv f_g(-z_t) \equiv 0 \mod p^{t-1}$ for all $t \geq 0$, so $f_g(-\overline{z}) = 0$. However, the polynomials $f_d(Z)$ with $d \mid a$ are irreducible (according to Lemma 5.3) and pairwise distinct, so no two of them have any common roots. Hence $\bigcap_{t \geq 0} G_{t,z_t}$ contains exactly one element g. Let $T \geq 0$ such that $G_{T,z_T} = \{g\}$.

Then $w_{z_t} \setminus \{g\} = w_{z_T} \setminus \{g\}$ for each $t \geq T$.

As the breadth-first search continues at every node (t, z_t), it follows that neither $w_{z_T} \setminus \{g\}$ nor $w_{z_T} \cup \{g\}$ are found. As every element of C is eventually found, this shows that $w_{z_T} \setminus \{g\}, w_{z_T} \cup \{g\} \notin C$.

However,

$$n^a - (\overline{z} \pm p^s)^{ab} \equiv n^a - \overline{z}^{ab} \mp ab\overline{z}^{ab-1}p^s \equiv \mp ab\overline{z}^{ab-1}p^s \mod p^{2s}$$

(as $f_g(-\overline{z}) = 0$ and $f_g(Z)$ divides $n^a - Z^{ab}$). Therefore (as $\overline{z} \neq 0$ due to $n^a - \overline{z}^{ab} = 0$), by choosing s sufficiently large and the appropriate sign, we get some $z' \equiv \overline{z} \mod p^T$ such that $(n^a - z'^{ab}, -1) = 1$, so $w_{z'} \in C$. Moreover $w_{z'} \setminus \{g\} = w_{z_T} \setminus \{g\}$ because of $G_{t,z_t} = \{g\}$. This proves that $w_{z_T} \setminus \{g\} \in C$ or $w_{z_T} \cup \{g\} \in C$, which is a contradiction.

Therefore the algorithm terminates in a finite amount of time. □

Let $\triangle$ denote the symmetric difference (i.e., $A \triangle B = (A \setminus B) \cup (B \setminus A)$).

Consider now the following algorithm:

```
function ISPOSSIBLE($k, m$)
    if $\sqrt[k]{m} \in \mathbb{Z}$ then
        return true
    else
        $a \leftarrow \max\{d \text{ divisor of } k \mid m \text{ is } d\text{-th power}\}$
        $b \leftarrow \frac{k}{a}$
        $n \leftarrow \sqrt[a]{m}$
        $T \leftarrow \{\emptyset\}$
        for all $p \mid 2an$ prime do
            $W \leftarrow$ COMBI($a, b, n, p$)
            $T \leftarrow \{t \triangle w \mid t \in T, w \in W\}$
        end for
        return $\emptyset \in T$
    end if
end function
```

Theorem 5.15. *Let $k \geq 1$ be odd and $m \in \mathbb{Z}$.*

Then ISPOSSIBLE*(k, m) always terminates. If it returns "false", then m is not of the form $x^2 + y^2 + z^k$ for integers x, y, z. If Schinzel's hypothesis H is true, then the converse also holds.*

Proof. The case $\sqrt[k]{m} \in \mathbb{Z}$ is obvious, so assume $\sqrt[k]{m} \notin \mathbb{Z}$.

After line 38 the set T can, according to the previous lemma (and as $\{0, 1, 2, \dots\}$ is dense in $\mathbb{Z}_p$ and $\mathbb{Q}_p \setminus \{0\} \to \{\pm 1\}, \quad u \to (u, -1)$ is locally constant for each prime p), be described as follows:

$$T = \{ \mathop{\triangle}_{p|2an} w_{z_p} \mid (x_p, y_p, z_p)_p \in \prod_{p|2an} U(\mathbb{Q}_p) \cap \mathfrak{X}(\mathbb{Z}_p) \}$$

Hence $\emptyset \in T$ if and only if there is some $(x_p, y_p, z_p)_p \in \prod_{p|2an} U(\mathbb{Q}_p) \cap \mathfrak{X}(\mathbb{Z}_p)$ such that $\prod_{p|2an}(f_d(-z_p), -1) = 1$ for each divisor d of a.

If v is a prime not dividing $2an$ or $v = \infty$ and $(x_v, y_v, z_v) \in U(\mathbb{Q}_v) \cap \mathfrak{X}(\mathbb{Z}_v)$, then, according to Lemmas 3.2 and 3.14, $(n^d - z^{db}, -1) = 1$ for each $d \mid a$.

Furthermore, for each such place v the set $U(\mathbb{Q}_v) \cap \mathfrak{X}(\mathbb{Z}_v)$ is nonempty according to Lemmas 3.2 and 3.9.

The equation

$$(n^d - z^{db}, -1) = \prod_{d'|d} (f_d(-z), -1)$$

therefore shows (like in the proof of the claim in the proof of Theorem 5.5) that there is some $(x_v, y_v, z_v)_v \in \prod_v U(\mathbb{Q}_v) \cap \mathfrak{X}(\mathbb{Z}_v)$ such that $\prod_v (n^d - z_v^{bd}, -1) = 1$ for each $d \mid a$ if and only if $\emptyset \in T$.

Therefore $L \neq \emptyset$ if and only if $\emptyset \in T$.

Hence the claim follows with Theorem 5.5. □

5.2 Small exceptions

The following table lists possible values of m such that equation (3) has no integral solution. The lists might be incomplete if Schinzel's hypothesis H is false.

k	**List of those integers $1 \le m \le 10^9$ without integral solution**
9	$6^3, 30^3, 54^3, 78^3, 102^3, 126^3, 150^3, 174^3, 198^3, 222^3, 246^3, 294^3, 318^3, 342^3, 366^3, 390^3, 414^3, 438^3, 462^3, 486^3, 510^3, 534^3, 558^3, 582^3, 606^3, 630^3, 654^3, 678^3, 726^3, 750^3, 774^3, 798^3, 822^3, 846^3, 870^3, 894^3, 918^3, 942^3, 966^3, 990^3$
15	$6^3, 30^3, 54^3, 78^3, 102^3, 126^3, 150^3, 174^3, 198^3, 222^3, 246^3, 270^3, 294^3, 318^3, 342^3, 366^3, 390^3, 414^3, 438^3, 462^3, 510^3, 534^3, 558^3, 582^3, 606^3, 630^3, 654^3, 678^3, 702^3, 726^3, 750^3, 774^3, 798^3, 822^3, 846^3, 870^3, 894^3, 918^3, 942^3, 966^3, 990^3,$ $6^5, 14^5, 22^5, 30^5, 38^5, 46^5, 54^5, 62^5$
21	$6^3, 30^3, 54^3, 78^3, 102^3, 126^3, 150^3, 174^3, 198^3, 222^3, 246^3, 270^3, 294^3, 318^3, 342^3, 366^3, 390^3, 414^3, 438^3, 462^3, 486^3, 510^3, 534^3, 558^3, 582^3, 606^3, 630^3, 654^3, 678^3, 702^3, 726^3, 750^3, 774^3, 798^3, 822^3, 846^3, 870^3, 894^3, 918^3, 942^3, 966^3, 990^3,$ 14^7
25	$6^5, 14^5, 22^5, 30^5, 38^5, 46^5, 54^5, 62^5$
27	$6^3, 30^3, 46^3, 54^3, 62^3, 78^3, 102^3, 118^3, 126^3, 150^3, 174^3, 198^3, 206^3, 222^3, 246^3, 262^3, 270^3, 278^3, 294^3, 318^3, 334^3, 342^3, 366^3, 390^3, 414^3, 422^3, 438^3, 462^3, 478^3, 486^3, 494^3, 510^3, 534^3, 550^3, 558^3, 582^3, 606^3, 630^3, 638^3, 654^3, 678^3, 694^3, 702^3, 710^3, 726^3, 750^3, 766^3, 774^3, 798^3, 822^3, 846^3, 854^3, 870^3, 894^3, 910^3, 918^3, 926^3, 942^3, 966^3, 982^3, 990^3,$ 6^9
33	$6^3, 30^3, 54^3, 78^3, 102^3, 126^3, 150^3, 174^3, 198^3, 222^3, 246^3, 270^3, 294^3, 318^3, 342^3, 366^3, 390^3, 414^3, 438^3, 462^3, 486^3, 510^3, 534^3, 558^3, 582^3, 606^3, 630^3, 654^3, 678^3, 702^3, 726^3, 750^3, 774^3, 798^3, 822^3, 846^3, 870^3, 894^3, 918^3, 942^3, 966^3, 990^3$
35	$6^5, 14^5, 22^5, 30^5, 38^5, 46^5, 54^5, 62^5,$ 14^7
39	$6^3, 30^3, 54^3, 78^3, 102^3, 126^3, 150^3, 174^3, 198^3, 222^3, 246^3, 270^3, 294^3, 318^3, 342^3, 366^3, 390^3, 414^3, 438^3, 462^3, 486^3, 510^3, 534^3, 558^3, 582^3, 606^3, 630^3, 654^3, 678^3, 702^3, 726^3, 750^3, 774^3, 798^3, 822^3, 846^3, 870^3, 894^3, 918^3, 942^3, 966^3, 990^3$
45	$6^3, 30^3, 54^3, 78^3, 102^3, 126^3, 150^3, 174^3, 198^3, 222^3, 246^3, 270^3, 294^3, 318^3, 342^3, 366^3, 390^3, 414^3, 438^3, 462^3, 486^3, 510^3, 534^3, 558^3, 582^3, 606^3, 630^3, 654^3, 678^3, 702^3, 726^3, 750^3, 774^3, 798^3, 822^3, 846^3, 870^3, 894^3, 918^3, 942^3, 966^3, 990^3,$ $6^5, 14^5, 22^5, 30^5, 38^5, 46^5, 54^5, 62^5,$ 6^9
49	14^7

References

[DE08a] Rainer Dietmann and Christian Elsholz. Sums of two squares and a power. *unpublished manuscript*, 2008.

[DE08b] Rainer Dietmann and Christian Elsholz. Sums of two squares and one biquadrate. *Funct. Approx. Comment. Math.*, 38(2):233–234, 2008.

[DH37] Horace Davenport and Hans Heilbronn. Note on a result in the additive theory of numbers. *Proceedings of The London Mathematical Society*, 34(2):142–151, 1937.

[Gou09] Frank Gounelas. The Brauer-Manin obstruction. `http://people.maths.ox.ac.uk/gounelas/projects/bmo.pdf`, June 11, 2009.

[GS06] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology.* Cambridge University Press, 2006.

[JK95] William C. Jagy and Irving Kaplansky. Sums of squares, cubes, and higher powers. *Experimental Mathematics*, 4(3):169–173, 1995.

[Lan05] Serge Lang. *Algebra.* Graduate Texts in Mathematics. Springer, 2005.

[Mil80] James S. Milne. *Étale Cohomology.* Princeton University Press, 1980.

[Mil11] James S. Milne. Class field theory (v4.01). `http://www.jmilne.org/math/CourseNotes/CFT.pdf`, 2011.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic.* Graduate Texts in Mathematics. Springer, 1973.

[Sko01] Alexei Skorobogatov. *Torsors and Rational Points.* Cambridge University Press, 2001.

[SS58] Andrzej Schinzel and Wacław Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arithmetica*, 4(erratum 5):185–208, 1958.

[Ste11] William Stein. Algebraic number theory, a computational approach. `http://www.wstein.org/books/ant/ant.pdf`, September 26, 2011.

Selbstständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

____________________, den ____________________ ________________________

Ort Datum Unterschrift