

# THE SET OF NONSQUARES IN A NUMBER FIELD IS DIOPHANTINE

BJORN POONEN

ABSTRACT. Fix a number field  $k$ . We prove that  $k^\times - k^{\times 2}$  is diophantine over  $k$ . This is deduced from a theorem that for a nonconstant separable polynomial  $P(x) \in k[x]$ , there are at most finitely many  $a \in k^\times$  modulo squares such that there is a Brauer-Manin obstruction to the Hasse principle for the conic bundle  $X$  given by  $y^2 - az^2 = P(x)$ .

## 1. INTRODUCTION

Throughout, let  $k$  be a global field; occasionally we impose additional conditions on its characteristic. Warning: we write  $k^n = \prod_{i=1}^n k$  and  $k^{\times n} = \{a^n : a \in k^\times\}$ .

**1.1. Diophantine sets.** A subset  $A \subseteq k^n$  is **diophantine over  $k$**  if there exists a closed subscheme  $V \subseteq \mathbb{A}_k^{n+m}$  such that  $A$  equals the projection of  $V(k)$  under  $k^{n+m} \rightarrow k^n$ . The complexity of the collection of diophantine sets over a field  $k$  determines the difficulty of solving polynomial equations over  $k$ . For instance, it follows from [Mat70] that if  $\mathbb{Z}$  is diophantine over  $\mathbb{Q}$ , then there is no algorithm to decide whether a multivariable polynomial equation with rational coefficients has a solution in rational numbers. Moreover, diophantine sets can be built up from other diophantine sets. In particular, diophantine sets over  $k$  are closed under taking finite unions and intersections. Therefore it is of interest to gather a library of diophantine sets.

**1.2. Main result.** Our main theorem is the following:

**Theorem 1.1.** *For any number field  $k$ , the set  $k^\times - k^{\times 2}$  is diophantine over  $k$ .*

In other words, there is an algebraic family of varieties  $(V_t)_{t \in k}$  such that  $V_t$  has a  $k$ -point if and only if  $t$  is *not* a square. This result seems to be new even in the case  $k = \mathbb{Q}$ .

**Corollary 1.2.** *For any number field  $k$  and for any  $n \in \mathbb{Z}_{\geq 0}$ , the set  $k^\times - k^{\times 2^n}$  is diophantine over  $k$ .*

*Proof.* Let  $A_n = k^\times - k^{\times 2^n}$ . We prove by induction on  $n$  that  $A_n$  is diophantine over  $k$ . The base case  $n = 1$  is Theorem 1.1. The inductive step follows from  $A_{n+1} = A_1 \cup \{t^2 : t \in A_n\}$ .  $\square$

---

*Date:* October 12, 2008.

*2000 Mathematics Subject Classification.* Primary 14G05; Secondary 11G35, 11U99, 14G25, 14J20.

*Key words and phrases.* Brauer-Manin obstruction, nonsquares, diophantine set, Châtelet surface, conic bundle, Hasse principle, rational points.

This research was supported by NSF grants DMS-0301280 and DMS-0841321.

**1.3. Brauer-Manin obstruction.** The main ingredient of the proof of Theorem 1.1 is the fact the Brauer-Manin obstruction is the only obstruction to the Hasse principle for certain Châtelet surfaces over number fields, so let us begin to explain what this means. Let  $\Omega_k$  be the set of nontrivial places of  $k$ . For  $v \in \Omega_k$ , let  $k_v$  be the completion of  $k$  at  $v$ . Let  $\mathbf{A}$  be the adèle ring of  $k$ . For a projective  $k$ -variety  $X$ , we have  $X(\mathbf{A}) = \prod_{v \in \Omega_k} X(k_v)$ ; one says that there is a Brauer-Manin obstruction to the Hasse principle for  $X$  if  $X(\mathbf{A}) \neq \emptyset$  but  $X(\mathbf{A})^{\text{Br}} = \emptyset$ . See [Sko01, §5.2].

**1.4. Conic bundles and Châtelet surfaces.** Let  $\mathcal{E}$  be a rank-3 vector sheaf over a base variety  $B$ . A nowhere-vanishing section  $s \in \Gamma(B, \text{Sym}^2 \mathcal{E})$  defines a subscheme  $X$  of  $\mathbb{P}\mathcal{E}$  whose fibers over  $B$  are (possibly degenerate) conics. As a special case, we may take  $(\mathcal{E}, s) = (\mathcal{L}_0 \oplus \mathcal{L}_1 \oplus \mathcal{L}_2, s_0 + s_1 + s_2)$  where each  $\mathcal{L}_i$  is a line sheaf on  $B$ , and the  $s_i \in \Gamma(B, \mathcal{L}_i^{\otimes 2}) \subset \Gamma(B, \text{Sym}^2 \mathcal{E})$  are sections that do not simultaneously vanish on  $B$ .

We specialize further to the case where  $B = \mathbb{P}^1$ ,  $\mathcal{L}_0 = \mathcal{L}_1 = \mathcal{O}$ ,  $\mathcal{L}_2 = \mathcal{O}(n)$ ,  $s_0 = 1$ ,  $s_1 = -a$ , and  $s_2 = -\tilde{P}(w, x)$  where  $a \in k^\times$  and  $\tilde{P}(w, x) \in \Gamma(\mathbb{P}^1, \mathcal{O}(2n))$  is a separable binary form of degree  $2n$ . Let  $P(x) := \tilde{P}(1, x) \in k[x]$ , so  $P(x)$  is a separable polynomial of degree  $2n - 1$  or  $2n$ . We then call  $X$  the conic bundle given by

$$y^2 - az^2 = P(x).$$

A Châtelet surface is a conic bundle of this type with  $n = 2$ , i.e., with  $\deg P$  equal to 3 or 4. See also [Poo08].

The proof of Theorem 1.1 relies on the Châtelet surface case of the following result about families of more general conic bundles:

**Theorem 1.3.** *Let  $k$  be a global field of characteristic not 2. Let  $P(x) \in k[x]$  be a nonconstant separable polynomial. Then there are at most finitely many classes in  $k^\times/k^{\times 2}$  represented by  $a \in k^\times$  such that there is a Brauer-Manin obstruction to the Hasse principle for the conic bundle  $X$  given by  $y^2 - az^2 = P(x)$ .*

*Remark 1.4.* Theorem 1.3 is analogous to the classical fact that for an integral indefinite ternary quadratic form  $q(x, y, z)$ , the set of nonzero integers represented by  $q$  over  $\mathbb{Z}_p$  for all  $p$  but not over  $\mathbb{Z}$  fall into finitely many classes in  $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ . J.-L. Colliot-Thélène and F. Xu explain how to interpret and prove this fact (and its generalization to arbitrary number fields) in terms of the integral Brauer-Manin obstruction: see [CTX07, §7], especially Proposition 7.9 and the very end of §7. Our proof of Theorem 1.3 shares several ideas with the arguments there.

**1.5. Definable subsets of  $k_v$  and their intersections with  $k$ .** The proof of Theorem 1.1 requires one more ingredient, namely that certain subsets of  $k$  defined by local conditions are diophantine over  $k$ . This is the content of Theorem 1.5 below, which is proved in more generality than needed. By a  $k$ -definable subset of  $k_v^n$ , we mean the subset of  $k_v^n$  defined by some first-order formula in the language of fields involving only constants from  $k$ , even though the variables range over elements of  $k_v$ .

**Theorem 1.5.** *Let  $k$  be a number field. Let  $k_v$  be a nonarchimedean completion of  $k$ . For any  $k$ -definable subset  $A$  of  $k_v^n$ , the intersection  $A \cap k^n$  is diophantine over  $k$ .*

1.6. **Outline of paper.** Section 2 shows that Theorem 1.5 is an easy consequence of known results, namely the description of definable subsets over  $k_v$ , and the diophantineness of the valuation subring  $\mathcal{O}$  of  $k$  defined by  $v$ . Section 3 proves Theorem 1.3 by showing that for most twists of a given conic bundle, the local Brauer evaluation map at one place is enough to rule out a Brauer-Manin obstruction. Finally, Section 4 puts everything together to prove Theorem 1.1.

## 2. SUBSETS OF GLOBAL FIELDS DEFINED BY LOCAL CONDITIONS

**Lemma 2.1.** *Let  $m \in \mathbb{Z}_{>0}$  be such that  $\text{char } k \nmid m$ . Then  $k_v^{\times m} \cap k$  is diophantine over  $k$ .*

*Proof.* The valuation subring  $\mathcal{O}$  of  $k$  defined by  $v$  is diophantine over  $k$ : see the first few paragraphs of §3 of [Rum80]. The hypothesis  $\text{char } k \nmid m$  implies the existence of  $c \in k^\times$  such that  $1 + c\mathcal{O} \subset k_v^{\times m}$ ; fix such a  $c$ . The denseness of  $k^\times$  in  $k_v^\times$  implies  $k_v^{\times m} \cap k = (1 + c\mathcal{O})k^{\times m}$ . The latter is diophantine over  $k$ .  $\square$

*Proof of Theorem 1.5.* Call a subset of  $k_v^n$  **simple** if it is of one of the following two types:  $\{\vec{x} \in k_v^n : f(\vec{x}) = 0\}$  or  $\{\vec{x} \in k_v^n : f(\vec{x}) \in k_v^{\times m}\}$  for some  $f \in k[x_1, \dots, x_n]$  and  $m \in \mathbb{Z}_{>0}$ . It follows from the proof of [Mac76, Theorem 1] (see also [Mac76, §2] and [Den84, §2]) that any  $k$ -definable subset  $A$  is a boolean combination of simple subsets. The complement of a simple set of the first type is a simple set of the second type (with  $m = 1$ ). The complement of a simple set of the second type is a union of simple sets, since  $k_v^{\times m}$  has finite index in  $k_v^\times$ . Therefore any  $k$ -definable  $A$  is a finite union of finite intersections of simple sets. Diophantine sets in  $k$  are closed under taking finite unions and finite intersections, so it remains to show that for every simple subset  $A$  of  $k_v^n$ , the intersection  $A \cap k$  is diophantine. If  $A$  is of the first type, then this is trivial. If  $A$  is of the second type, then this follows from Lemma 2.1.  $\square$

## 3. FAMILY OF CONIC BUNDLES

Given a  $k$ -variety  $X$  and a place  $v$  of  $k$ , let  $\text{Hom}'(\text{Br } X, \text{Br } k_v)$  be the set of  $f \in \text{Hom}(\text{Br } X, \text{Br } k_v)$  such that the composition  $\text{Br } k \rightarrow \text{Br } X \xrightarrow{f} \text{Br } k_v$  equals the map induced by the inclusion  $k \hookrightarrow k_v$ . The  $v$ -adic evaluation pairing  $\text{Br } X \times X(k_v) \rightarrow \text{Br } k_v$  induces a map  $X(k_v) \rightarrow \text{Hom}'(\text{Br } X, \text{Br } k_v)$ .

**Lemma 3.1.** *With notation as in Theorem 1.3, there exists a finite set of places  $S$  of  $k$ , depending on  $P(x)$  but not  $a$ , such that if  $v \notin S$  and  $v(a)$  is odd, then  $X(k_v) \rightarrow \text{Hom}'(\text{Br } X, \text{Br } k_v)$  is surjective.*

*Proof.* The function field of  $\mathbb{P}^1$  is  $k(x)$ . Let  $Z$  be the zero locus of  $\tilde{P}(w, x)$  in  $\mathbb{P}^1$ . Let  $G$  be the group of  $f \in k(x)^\times$  having even valuation at every closed point of  $\mathbb{P}^1 - Z$ . Choose  $P_1(x), \dots, P_m(x) \in G$  representing a  $\mathbb{F}_2$ -basis for the image of  $G$  in  $k(x)^\times / k(x)^{\times 2} k^\times$ . We may assume that  $P_m(x) = P(x)$ . Choose  $S$  so that each  $P_i(x)$  is a ratio of polynomials whose nonzero coefficients are  $S$ -units, and so that  $S$  contains all places above 2.

Let  $\kappa(X)$  be the function field of  $X$ . A well-known calculation (see [Sko01, §7.1]) shows that the class of each quaternion algebra  $(a, P_i(x))$  in  $\text{Br } \kappa(X)$  belongs to the subgroup  $\text{Br } X$ , and that the cokernel of  $\text{Br } k \rightarrow \text{Br } X$  is an  $\mathbb{F}_2$ -vector space with the classes of  $(a, P_i(x))$  for  $i \leq m - 1$  as a basis.

Suppose that  $v \notin S$  and  $v(a)$  is odd. Let  $f \in \text{Hom}'(\text{Br } X, \text{Br } k_v)$ . The homomorphism  $f$  is determined by where it sends  $(a, P_i(x))$  for  $i \leq m-1$ . We need to find  $R \in X(k_v)$  mapping to  $f$ .

Let  $\mathcal{O}_v$  be the valuation ring in  $k_v$ , and let  $\mathbb{F}_v$  be its residue field. For  $i \leq m-1$ , choose  $c_i \in \mathcal{O}_v^\times$  whose image in  $\mathbb{F}_v^\times$  is a square or not, according to whether  $f$  sends  $(a, P_i(x))$  to 0 or  $1/2$  in  $\mathbb{Q}/\mathbb{Z} \simeq \text{Br } k_v$ . Since  $v(a)$  is odd, we have  $(a, c_i) = f((a, P_i(x)))$  in  $\text{Br } k_v$ .

View  $\mathbb{P}^1 - Z$  as a smooth  $\mathcal{O}_v$ -scheme, and let  $Y$  be the finite étale cover of  $\mathbb{P}^1 - Z$  whose function field is obtained by adjoining  $\sqrt{c_i P_i(x)}$  for  $i \leq m-1$  and also  $\sqrt{P(x)}$ . Then the generic fiber  $Y_{k_v} := Y \times_{\mathcal{O}_v} k_v$  is geometrically integral. Assuming that  $S$  was chosen to include all  $v$  with small  $\mathbb{F}_v$ , we may assume that  $v \notin S$  implies that  $Y$  has a (smooth)  $\mathbb{F}_v$ -point, which by Hensel's lemma lifts to a  $k_v$ -point  $Q$ . There is a morphism from  $Y_{k_v}$  to the smooth projective model of  $y^2 = P(x)$  over  $k_v$ , which in turn embeds as a closed subscheme of  $X_{k_v}$ , as the locus where  $z = 0$ . Let  $R$  be the image of  $Q$  under  $Y(k_v) \rightarrow X(k_v)$ , and let  $\alpha = x(R) \in k_v$ . Evaluating  $(a, P_i(x))$  on  $R$  yields  $(a, P_i(\alpha))$ , which is isomorphic to  $(a, c_i)$  since  $c_i P_i(\alpha) \in k_v^{\times 2}$ . Thus  $R$  maps to  $f$ , as required.  $\square$

**Lemma 3.2.** *Let  $X$  be a projective  $k$ -variety. If there exists a place  $v$  of  $k$  such that the map  $X(k_v) \rightarrow \text{Hom}'(\text{Br } X, \text{Br } k_v)$  is surjective, then there is no Brauer-Manin obstruction to the Hasse principle for  $X$ .*

*Proof.* If  $X(\mathbf{A}) = \emptyset$ , then the Hasse principle holds. Otherwise, pick  $Q = (Q_w) \in X(\mathbf{A})$ , where  $Q_w \in X(k_w)$  for each  $w$ . For  $A \in \text{Br } X$ , let  $\text{ev}_A: X(L) \rightarrow \text{Br } L$  be the evaluation map for any field extension  $L$  of  $k$ . Let  $\text{inv}_w: \text{Br } k_w \rightarrow \mathbb{Q}/\mathbb{Z}$  be the usual inclusion map. Define

$$\begin{aligned} \eta: \text{Br } X &\rightarrow \mathbb{Q}/\mathbb{Z} \simeq \text{Br } k_v \\ A &\mapsto - \sum_{w \neq v} \text{inv}_w \text{ev}_A(Q_w). \end{aligned}$$

By reciprocity,  $\eta \in \text{Hom}'(\text{Br } X, \text{Br } k_v)$ . The surjectivity hypothesis yields  $R \in X(k_v)$  giving rise to  $\eta$ . Define  $Q' = (Q'_w) \in X(\mathbf{A})$  by  $Q'_w := Q_w$  for  $w \neq v$  and  $Q'_v := R$ . Then  $Q' \in X(\mathbf{A})^{\text{Br}}$ , so there is no Brauer-Manin obstruction.  $\square$

*Proof of Theorem 1.3.* Let  $S$  be as in Lemma 3.1. Enlarge  $S$  to assume that  $\text{Pic } \mathcal{O}_{k,S}$  is trivial. Then the set of  $a \in k^\times$  such that  $v(a)$  is even for all  $v \notin S$  has the same image in  $k^\times/k^{\times 2}$  as the finitely generated group  $\mathcal{O}_{k,S}^\times$ , so the image is finite.

Suppose that  $a \in k^\times$  has image in  $k^\times/k^{\times 2}$  lying outside this finite set. Then we can fix  $v \notin S$  such that  $v(a)$  is odd. Let  $X$  be the corresponding surface. Combining Lemmas 3.1 and 3.2 shows that there is no Brauer-Manin obstruction to the Hasse principle for  $X$ .  $\square$

#### 4. THE SET OF NONSQUARES IS DIOPHANTINE

*Proof of Theorem 1.1.* For each place  $v$  of  $k$ , define  $S_v := k^\times \cap k_v^{\times 2}$  and  $N_v := k^\times - S_v$ . By Theorem 1.5, the sets  $S_v$  and  $N_v$  are diophantine over  $k$ .

By [Poo08, Proposition 4.1], there is a Châtelet surface

$$X_1: y^2 - bz^2 = P(x)$$

over  $k$ , with  $P(x)$  a product of two irreducible quadratic polynomials, such that there is a Brauer-Manin obstruction to the Hasse principle for  $X_1$ . For  $t \in k^\times$ , let  $X_t$  be the (smooth

projective) Châtelet surface associated to the affine surface

$$U_t: y^2 - tbz^2 = P(x).$$

We claim that the following are equivalent for  $t \in k^\times$ :

- (i)  $U_t$  has a  $k$ -point.
- (ii)  $X_t$  has a  $k$ -point.
- (iii)  $X_t$  has a  $k_v$ -point for every  $v$  and there is no Brauer-Manin obstruction to the Hasse principle for  $X_t$ .

The implications (i)  $\implies$  (ii)  $\implies$  (iii) are trivial. The implication (iii)  $\implies$  (ii) follows from [CTCS80, Theorem B]. Finally, in [CTCS80], the reduction of Theorem B to Theorem A combined with Remarque 7.4 shows that (ii) implies that  $X_t$  is  $k$ -unirational, which implies (i).

Let  $A$  be the (diophantine) set of  $t \in k^\times$  such that (i) holds. The isomorphism type of  $U_t$  depends only on the image of  $t$  in  $k^\times/k^{\times 2}$ , so  $A$  is a union of cosets of  $k^{\times 2}$  in  $k^\times$ . We will compute  $A$  by using (iii).

The affine curve  $y^2 = P(x)$  is geometrically integral so it has a  $k_v$ -point for all places  $v$  outside a finite set  $F$ . So for any  $t \in k^\times$ , the variety  $X_t$  has a  $k_v$ -point for all  $v \notin F$ . Since  $X_1$  has a  $k_v$ -point for all  $v$  and in particular for  $v \in F$ , if  $t \in \bigcap_{v \in F} S_v$ , then  $X_t$  has a  $k_v$ -point for all  $v$ .

Let  $B := A \cup \bigcup_{v \in F} N_v$ . If  $t \in k^\times - B$ , then  $X_t$  has a  $k_v$ -point for all  $v$ , and there is a Brauer-Manin obstruction to the Hasse principle for  $X_t$ . By Theorem 1.3,  $k^\times - B$  consists of finitely many cosets of  $k^{\times 2}$ , one of which is  $k^{\times 2}$  itself. Each coset of  $k^{\times 2}$  is diophantine over  $k$ , so taking the union of  $B$  with all the finitely many missing cosets except  $k^{\times 2}$  shows that  $k^\times - k^{\times 2}$  is diophantine.  $\square$

#### ACKNOWLEDGEMENTS

I thank Jean-Louis Colliot-Thélène and Anthony Várilly-Alvarado for a few comments, and Alexandra Shlapentokh for suggesting some references.

#### REFERENCES

- [CTCS80] Jean-Louis Colliot-Thélène, Daniel Coray, and Jean-Jacques Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. Reine Angew. Math. **320** (1980), 150–191 (French). MR **592151** (82f:14020)  $\uparrow 4$
- [CTX07] Jean-Louis Colliot-Thélène and Fei Xu, *Brauer-Manin obstruction for integral points of homogeneous spaces and representation of integral quadratic forms*, December 12, 2007. preprint.  $\uparrow 1.4$
- [Den84] J. Denef, *The rationality of the Poincaré series associated to the  $p$ -adic points on a variety*, Invent. Math. **77** (1984), no. 1, 1–23. MR **751129** (86c:11043)  $\uparrow 2$
- [Mac76] Angus Macintyre, *On definable subsets of  $p$ -adic fields*, J. Symbolic Logic **41** (1976), no. 3, 605–610. MR 0485335 (58 #5182)  $\uparrow 2$
- [Mat70] Yu. Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian). MR 0258744 (41 #3390)  $\uparrow 1.1$
- [Poo08] Bjorn Poonen, *Existence of rational points on smooth projective varieties*, June 4, 2008. Preprint, to appear in *J. Europ. Math. Soc.*  $\uparrow 1.4, 4$
- [Rum80] R. S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), no. 1, 195–217. MR583852 (81m:03053)  $\uparrow 2$
- [Sko01] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. MR1845760 (2002d:14032)  $\uparrow 1.3, 3$

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA  
02139-4307, USA  
*E-mail address:* `poonen@math.mit.edu`  
*URL:* `http://math.mit.edu/~poonen`