On a Shimura curve that is a counterexample to the Hasse principle

Samir Siksek and Alexei Skorobogatov

Abstract

Let X be the Shimura curve corresponding to the quaternion algebra over $\mathbb{Q}$ ramified only at 3 and 13. B. Jordan showed that $X_{\mathbb{Q}(\sqrt{-13})}$ is a counterexample to the Hasse principle. Using an equation of X found by A. Kurihara, we show, by elementary means, that X has no $\mathbb{Q}(\sqrt{-13})$-rational divisor classes of odd degree. A corollary of this is the fact that this counterexample is explained by the Manin obstruction.

Mathematics subject classification (2000): 11G18, 11G05, 11G30

1 Introduction

Let X be a smooth and projective variety over a number field k. Assume that X is a counterexample to the Hasse principle, that is, X has no k-rational point but has rational points in all the completions of k. If we denote by $\mathbb{A}_k$ the adèles of k, then the global reciprocity applied to the Brauer–Grothendieck group $\mathrm{Br}(X)$ defines a certain subset $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)$ which contains the diagonal image of $X(k)$. One says that the failure of the Hasse principle for X is explained by the Manin obstruction if $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.

Now let X be a curve. It is an open question whether or not all counterexamples to the Hasse principle on curves can be accounted for by the Manin obstruction. (The answer to the same question for surfaces is known to be negative, see [9], Sect. 8). One can easily give a conditional answer if X already has no rational divisor class of degree 1; then the finiteness of the Tate–Shafarevich group of the Jacobian of X implies that $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$, see [9], Cor. 6.2.5. A few examples of this kind are known: over $k = \mathbb{Q}$ we have Schinzel's curve $x^4 + 17y^4 - 2(4y^2 + z^2)^2 = 0$, Cassels's curve $x^4 + y^4 - 241^2 z^4 = 0$ and a more complicated curve in [2]. These curves have genus 3. When X has a rational divisor class of degree 1 very little is known. A simplest case when our question can be answered is when X is equipped with a morphism $f : X \to A$, where A is an abelian variety such that $A(k)$ is finite. Two typical cases are when X can be realised as a subvariety of its Jacobian (using a

rational divisor class of degree 1), or when f is a finite covering of an elliptic curve. In some other cases our problem can be resolved by descent. See [9], pp. 127–128.

One difficulty for general curves seems to be a 'lack of structure', so hopefully the problem should become more tractable if we restrict ourselves to a class of 'modular curves', say Shimura curves. Motivated by this goal, we study in this paper, by elementary methods, one particular Shimura curve that is a counterexample to the Hasse principle. Let B be the quaternion algebra over $\mathbb{Q}$ ramified only at 3 and 13, and let $X_B/\mathbb{Q}$ be the corresponding Shimura curve. Using subtle properties of the Galois representation on certain points of finite order of abelian surfaces parametrized by the points of X_B, Bruce Jordan [3] showed that $X_B(K) = \emptyset$ where $K = \mathbb{Q}(\sqrt{-13})$. On the other hand, the question of existence of local points on Shimura curves is completely answered by Shimura and Jordan–Livné [4]. In particular, $X_B(\mathbb{A}_K) \neq \emptyset$. The question which naturally arises is whether this counterexample to the Hasse principle can be accounted for by the Manin obstruction. We work with the equation of X_B obtained by Akira Kurihara in [7]. Unlike the classical modular curves the equations of Shimura curves are difficult to obtain. The method in [7] is based on a (very plausible) guess, and so, until that guess is proved correct, our main result should be regarded as concerning not the Shimura curve X_B itself but the curve X of genus 3 given by the equations

$$X : \begin{cases} v^2 = -(3u^2 + 12u + 13)(u^2 + 12u + 39) \\ z^2 = 2u^2 + 6u + 5 \end{cases} \tag{1}$$

In this paper we prove that:

- X has no divisor classes of odd degree over $K = \mathbb{Q}(\sqrt{-13})$; in particular it does not have any divisor class of degree 1.
- The failure of the Hasse principle for X_K is explained by the Manin obstruction.

As we mentioned earlier, the second claim follows from the first one if one assumes that the Tate–Shafarevich group of the Jacobian of X_K is finite. We do not make this assumption; indeed our results do not rely on any conjectures.

2 Divisor classes of degree 1

Note that X covers the curve

$$Y : v^2 = -(3u^2 + 12u + 13)(u^2 + 12u + 39). \tag{2}$$

We begin by studying the arithmetic of Y. Clearly Y is a genus 1 curve and a short search reveals that Y has a K-point

$$P_0 = [(-39 + 4\sqrt{-13})/7, (260 - 120\sqrt{-13})/49].$$

It is straighforward to give a birational map from Y to its jacobian elliptic curve

$$E : y^2 = (x-10)(x+3)(x+6)$$

taking P_0 to the point at infinity on E. The map however is complicated and we do not give the equations here. The reader who would like to check this and other calculations made in this paper should look at
`http://www.ma.ic.ac.uk/~anskor/publ.htm`

Lemma 2.1 *$E(K)$ has rank 1; a $\mathbb{Z}$-basis for $E(K)$ is*

$$S_1 = [10, 0], S_2 = [-3, 0], S_3 = [-14/13, (480/169)\sqrt{-13}].$$

Proof. Let

$$E_{-13} : y^2 = (x+130)(x-39)(x-78)$$

be the -13-twist of E. Cremona's program `mwrank` tells us that the rank of $E(\mathbb{Q})$ is 0 and that 2-division points $[10, 0]$, $[-3, 0]$ form a basis for $E(\mathbb{Q})$. The same program tells us that $[-130, 0]$, $[39, 0]$, $[14, 480]$ is a basis for $E_{-13}(\mathbb{Q})$ (now of rank 1). Suppose now that $S \in E(K)$ and let σ be the non-trivial automorphism of K. Then $S+S^\sigma$ is in $E(\mathbb{Q})$ and so belongs to the subgroup generated by S_1, S_2. Likewise $S - S^\sigma$ is in $E_{-13}(\mathbb{Q})$, and hence belongs to the subgroup generated by S_1, S_2, S_3. Hence $2S = (S + S^\sigma) + (S - S^\sigma)$ is also in the subgroup generated by S_1, S_2, S_3. It is easy to check that S_1, S_2, S_3 are independent modulo $2E(K)$. Hence S_1, S_2, S_3 is a basis. QED

Using our birational map we find that the images of these three points on Y are the points

$$P_1 = [(-39 - 4\sqrt{-13})/7, (-260 - 120\sqrt{-13})/49],$$

$$P_2 = [(-39 - 4\sqrt{-13})/19, (-1300 + 120\sqrt{-13})/361],$$

$$P_3 = \left[\frac{(-11442639 - 2077204\sqrt{-13})}{3412219}, \frac{(-74800945937900 + 46469317632360\sqrt{-13})}{11643238503961}\right].$$

Corollary 2.2 *The classes $[P_1 - P_0]$, $[P_2 - P_0]$, $[P_3 - P_0]$ form a $\mathbb{Z}$-basis for $\mathrm{Pic}^0(Y)$.*

Lemma 2.3 *Let $f \in K(Y)$ be the function given by $f = u^2 + 12u + 39$ on the affine equation for Y in (2). Let $v_{\sqrt{-13}} : K^* \to \mathbb{Z}$ be the valuation corresponding to the prime $\sqrt{-13}$ over K. Then*

$$v_{\sqrt{-13}}(f(P_0)) = v_{\sqrt{-13}}(f(P_1)) = v_{\sqrt{-13}}(f(P_2)) = v_{\sqrt{-13}}(f(P_3)) = 1.$$

Proof. From the definition of f all we have to check is that $v_{\sqrt{-13}}(u(P_i)) = 1$ for $i = 0, \ldots, 3$. This is immediate for $i = 0, 1, 2$ and a short calculation for $i = 3$. QED

Lemma 2.4 *Suppose that $Q \in Y(\overline{K})$, and let $L = K(Q)$. Suppose that the extension L/K has odd degree. Then there is a prime $\mathfrak{P}$ of L such that*

- $\mathfrak{P}|\sqrt{-13}$,
- $\deg(\mathfrak{P}/\sqrt{-13})$ *is odd, and*
- $\mathfrak{P}|u(Q)$.

In particular, if $Q \in Y(K)$ *then* $\sqrt{-13}|u(Q)$.

Proof. Let $Q_1, \ldots, Q_n$ be the conjugates of Q ($Q_1 = Q$), and note that $n = [L : K]$. Thus the divisor $\sum Q_i - nP_0$ is K-rational of degree 0 and Corollary 2.2 implies that

$$\sum_{i=1}^{n} Q_i - nP_0 \sim \sum_{j=1}^{3} n_j(P_j - P_0)$$

for some integers n_j. Taking everything to one side we find

$$\sum_{i=1}^{n} Q_i - \sum_{j=0}^{3} m_j P_j \sim 0$$

for some integers m_j. Thus there exists a function $g \in K(Y)$ whose divisor equals the divisor on the left hand side:

$$\operatorname{div}(g) = \sum_{i=1}^{n} Q_i - \sum_{j=0}^{3} m_j P_j,$$

and we note for future reference that

$$m_0 + m_1 + m_2 + m_3 = n = [L : K] \quad \text{is odd.} \tag{3}$$

It is easy to see that $\operatorname{div}(f)$ and $\operatorname{div}(g)$ have disjoint support. Weil's reciprocity (see, for example, [8], page 43) asserts that

$$f(\operatorname{div}(g)) = g(\operatorname{div}(f)). \tag{4}$$

Now $f = u^2 + 12u + 39$ is a factor of the right hand side of the equation (2) and it is clear that it has double zeros at two ramification points and double poles at the two points at infinity. Thus $\operatorname{div}(f) = 2D$ for some K-rational divisor D. Hence, from (4) we have

$$\left(\prod_{i=1}^{n} f(Q_i)\right)\left(\prod_{j=0}^{3} f(P_j)^{m_j}\right)^{-1} = g(D)^2 \in K^{*2}.$$

The previous lemma asserts that the $f(P_j)$ all have valuation 1 at $\sqrt{-13}$, and from (3) we get that

$$v_{\sqrt{-13}}\left(\prod_{i=1}^{n} f(Q_i)\right) \text{ is odd.}$$

Now $\prod_{i=1}^{n} f(Q_i) = \mathrm{Norm}_{L/K}(u(Q)^2 + 12u(Q) + 39)$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ be the distinct primes ideals of L dividing $\sqrt{-13}$. We can write

$$(u(Q)^2 + 12u(Q) + 39) = \left(\prod \mathfrak{P}_j^{r_j}\right) \mathfrak{a}$$

for some fractional ideal $\mathfrak{a}$ not having any of the $\mathfrak{P}_j$ in its support. Taking norms we deduce that

$$\sum r_j \deg(\mathfrak{P}_j/\sqrt{-13}) = v_{\sqrt{-13}}(\mathrm{Norm}_{L/K}(u(Q)^2 + 12u(Q) + 39));$$

we know that the right hand side is odd and hence, for some j, both r_j and $\deg(\mathfrak{P}_j/\sqrt{-13})$ are odd. Thus there is a prime $\mathfrak{P}|\sqrt{-13}$ such that $\deg(\mathfrak{P}/\sqrt{-13})$ is odd and $v_{\mathfrak{P}}(u(Q)^2 + 12u(Q) + 39)$ is odd. We see that $v_{\mathfrak{P}}(u(Q)) \geq 0$ otherwise the valuation would have been even. Further, from the equation (2) we have that $v_{\mathfrak{P}}(3u(Q)^2 + 12u(Q) + 13)$ is also odd. Hence $\mathfrak{P}|(u(Q)^2 + 12u(Q))$ and $\mathfrak{P}|(3u(Q)^2 + 12u(Q))$ and thus $\mathfrak{P}|u(Q)$. QED

Theorem 2.5 *X does not have any K-rational divisor classes of odd degree.*

Proof. Let $\overline{K}$ be an algebraic closure of K. Since X has points everywhere locally we have an equality

$$H^0(\mathrm{Gal}(\overline{K}/K), \mathrm{Pic}(\overline{X})) = \mathrm{Pic}(X)$$

and so it is sufficient to show that there are no K-rational divisors of odd degree, or equivalently that there are no points defined over extensions of K of odd degree. Thus suppose R is a point on X such that $K(R)/K$ is of odd degree, and we seek to derive a contradiction. Let Q be the image of R on Y. Clearly the point Q lies on the affine patch given by the equation (2). Since the v- and the z-coordinates of R are given by quadratic equations over the u-coordinate and the extension $K(R)/K$ is odd it follows that

$$K(u(Q)) = K(Q) = K(R).$$

Let $L = K(Q) = K(R)$. Hence L/K has odd degree. By the previous Lemma we know that there exists a prime ideal $\mathfrak{P}$ of L such that $\mathfrak{P}|\sqrt{-13}$, $\mathfrak{P}|u(Q)$, and $\deg(\mathfrak{P}/\sqrt{-13})$ is odd. But $u(Q) = u(R)$. Thus $\mathfrak{P}|u(R)$. From the second equation in (1) we have

$$z(R)^2 \equiv 5 \pmod{\mathfrak{P}}$$

and hence 5 is a square in the field $\mathcal{O}_L/\mathfrak{P}$. The crucial point now is that

$$\left[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\sqrt{-13}\right] = \deg(\mathfrak{P}/\sqrt{-13})$$

which is odd. Taking norms we get that $5^{\deg(\mathfrak{P}/\sqrt{-13})}$ is a square in $\mathcal{O}_K/(\sqrt{-13})$. This is a contradiction since $\mathcal{O}_K/(\sqrt{-13}) = \mathbb{Z}/13$, 5 is a quadratic non-residue modulo 13 and $\deg(\mathfrak{P}/\sqrt{-13})$ is odd. Hence there are no divisor classes of odd degree over K. QED

3 The Manin obstruction on X

We now come to proving that the Manin obstruction explains the failure of the Hasse principle for X_K. For this it would be enough to know the finiteness of the Tate–Shafarevich group of the Jacobian of X_K. However, using the computations of the previous section we deduce the desired statement from a simpler fact: the finiteness of $Ш(E_K)$, the Tate–Shafarevich group of the Jacobian of Y_K. The finiteness of this group follows from the result of Kolyvagin, which says that a modular elliptic curve over $\mathbb{Q}$ with analytic rank at most 1 has a finite Tate–Shafarevich group [5], [6]. All elliptic curves over $\mathbb{Q}$ are modular by a theorem of C. Breil, B. Conrad, F. Diamond and R. Taylor [1].

Lemma 3.1 *The group $Ш(E_K)$ is finite.*

Proof. We make use of John Cremona's tables:
`http://www.maths.nottingham.ac.uk/personal/jec/ftp/data/INDEX.html`
- specifically the files `allbsd.1-8000` and `allbsd.8001-12000`. The curves $E/\mathbb{Q}$ and $E_{-13}/\mathbb{Q}$ (respectively the curves 39A1 and 8112HH2 in these tables) have analytic ranks 0 and 1 according to these tables.

By Kolyvagin it follows that $Ш(E)$ and $Ш(E_{-13})$ are finite. Let us show that this implies the finiteness of $Ш(E_K)$. Let $A = R_{K/\mathbb{Q}}(E_K)$ be the abelian surface over $\mathbb{Q}$ which is the Weil descent of E_K. We then have $H^1(\mathbb{Q}, A) = H^1(K, E_K)$ and $H^1(\mathbb{Q}_v, A) = \prod_{w|v} H^1(K_w, E_K)$. The functoriality of restriction maps implies that we have a natural isomorphism $Ш(A) = Ш(E_K)$. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, $\overline{E} = E \times_{\mathbb{Q}} \overline{\mathbb{Q}}$, $\overline{A} = A \times_{\mathbb{Q}} \overline{\mathbb{Q}}$. By the definition of Weil descent $\overline{A}$ is isomorphic to $\overline{E} \times \overline{E}$. Using explicit action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ one easily checks that the map of $\overline{\mathbb{Q}}$-varieties $\overline{E} \times \overline{E} \to \overline{E} \times \overline{E}$ given by $(x, y) \mapsto (x + y, x - y)$ descends to a map of $\mathbb{Q}$-varieties $A \to E \times E_{-13}$. This map is an isogeny of degree 4. The property of the Tate–Shafarevich group to be finite is preserved by isogenies. Hence the finiteness of $Ш(A) = Ш(E_K)$ follows from the finiteness of $Ш(E \times E_{-13})$. QED

Lemma 3.2 *If $(Q_v)_v \in Y(\mathbb{A}_K)^{\mathrm{Br}}$, then u is regular at $Q_{\sqrt{-13}}$ and $\sqrt{-13}|u(Q_{\sqrt{-13}})$ (where $Q_{\sqrt{-13}}$ is the $\sqrt{-13}$-adic component of the adelic point).*

Proof. We can regard Y_K as an elliptic curve. By Lemma 3.1 its Tate–Shafarevich group is finite. It is well known that $Y(\mathbb{A}_K)^{\mathrm{Br}}$ is generated by the closure of the diagonal image of $Y(K)$ and the connected component of 0 (see, e.g., [9], Prop. 6.2.4). Then $Q_{\sqrt{-13}}$ is in the $\sqrt{-13}$-adic closure of $Y(K)$. However, by Lemma 2.4

$$Y(K) \subseteq \{Q \in Y(K_{\sqrt{-13}}) : \ u \text{ is regular at } Q \text{ and } \sqrt{-13}|u(Q)\}$$

and we know that the set on the right hand side is closed. Thus $Q_{\sqrt{-13}}$ belongs to that set. QED

Theorem 3.3 *The set* $X(\mathbb{A}_K)^{\mathrm{Br}}$ *is empty.*

Proof. Let $\phi : X \to Y$ be the obvious map. Suppose that $(R_v)_v \in X(\mathbb{A}_K)^{\mathrm{Br}}$. By the functoriality of the Brauer group (see [9], (5.3)) we have $\phi((R_v)_v) \in Y(\mathbb{A}_K)^{\mathrm{Br}}$. Thus u is regular at $R_{\sqrt{-13}}$, and $\sqrt{-13}|u(R_{\sqrt{-13}})$ by the previous Lemma. However from the second equation for X we have $z(R_{\sqrt{-13}})^2 \equiv 5 \pmod{\sqrt{-13}}$, and this is impossible. QED

References

1. C. Breuil, B. Conrad, F. Diamond, R. Taylor, 'On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises' *J. Amer. Math. Soc.* 14 (2001) 843–939.

2. J.W.S. Cassels, 'The arithmetic of certain quartic curves' *Proc. Royal Soc. Edinburgh* 100A (1985) 201–218.

3. B.W. Jordan, 'Points on Shimura curves rational over number fields' *J. reine angew. Math.* 371 (1986) 92–114.

4. B.W. Jordan and R.A. Livné, 'Local Diophantine properties of Shimura curves' *Math. Ann.* 270 (1985) 235–248.

5. V.A. Kolyvagin, 'On the Mordell-Weil group and the Shaferevich-Tate group of modular elliptic curves'. In: *Proceedings of the International Congress of Mathematicians.* Vol I, II (Kyoto 1990), 429–436, Math. Soc. Japan, 1991.

6. V.A. Kolyvagin, 'Euler Systems'. In: *The Grothendieck Festschrift*, Vol II, 435–483, Progr. Math. 87, Birkhäuser, Boston, 1990.

7. A. Kurihara, 'On p-adic Poincaré series and Shimura curves' *Intern. J. Math.* 5 (1994) 747–763.

8. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

9. A.N. Skorobogatov, *Torsors and rational points*, Cambridge Univ. Press, 2001.

Department of Mathematics, Faculty of Science, Sultan Qaboos University, PO Box 36, Al-Khod 123, Oman

e-mail: siksek@squ.edu.om

Department of Mathematics, The Huxley Building, Imperial College, 180 Queen's Gate, London SW7 2BZ, England

e-mail: a.skorobogatov@ic.ac.uk