ON GENUS ONE CURVES VIOLATING THE LOCAL-GLOBAL PRINCIPLE

HAN WU

Abstract. For any number field not containing \( \mathbb{Q}(i) \), we give an explicit construction to prove that there exists an elliptic curve defined over this field such that its Shafarevich-Tate group is nontrivial.

1. Introduction

1.1. Background. Let \( X \) be a proper algebraic variety defined over a number field \( K \). Let \( \Omega_K \) be the set of all nontrivial places of \( K \). Let \( K_v \) be the completion of \( K \) at \( v \in \Omega_K \). We say that \( X \) violates the local-global principle if \( X(K_v) \neq \emptyset \) for all \( v \in \Omega_K \), whereas \( X(K) = \emptyset \).

The Hasse-Minkowski theorem states that an algebraic variety defined by a quadratic form satisfies the local-global principle. As a consequence, the local-global principle holds for every smooth, projective and geometrically connected curve of genus-0. The first genus-1 curve violating the local-global principle was discovered by Lind [Lin40] and Reichardt [Rei42]. A simple one is Selmer’s cubic curve defined over \( \mathbb{Q} \) by \( 3w_0^3 + 4w_1^3 + 5w_2^3 = 0 \) in \( \mathbb{P}^2 \) with homogeneous coordinates \((w_0 : w_1 : w_2)\), cf. [Sel51]. Poonen [Poo10] proved that there exist curves over every global field violating the local-global principle. Clark [Cla09 Section 5 Conjecture 1] conjectured that genus-1 curve will be enough, i.e. for any given global field, there exists a genus-1 curve over this field violating the local-global principle.

Our goal is to prove that Clark’s conjecture [Cla09 Section 5 Conjecture 1] holds for any number field not containing \( \mathbb{Q}(i) \). More exactly, we will prove the following theorem.

**Theorem 1.1.0.1 (Theorem 6.0.0.1).** For any number field \( K \) not containing \( \mathbb{Q}(i) \), there exists an elliptic curve \( E \) defined over \( K \) such that \( \text{III}(K, E)[2] \neq 0 \). Here \( \text{III}(K, E)[2] \) is the 2-torsion subgroup of the Shafarevich-Tate group of \( E \).

The way to prove this theorem is to give an explicit construction of genus-1 curve violating the local-global principle. The curves that we consider in this paper, are the smooth projective models of plane curves defined by the equation

\[
qy^2 = x^4 - p
\]

in \( K[x, y] \) such that \( p, q \) are coprime integers in \( K \). These are genus-1 curves. We give smooth compactifications of these curves in Section 3. We discuss in which case these curves have local points in Section 4 and give sufficient conditions about whether they don’t exist \( K \)-rational points in Section 4. In Section 5 we will prove that if the number field \( K \) does not contain \( \mathbb{Q}(i) \), then we can choose parameters satisfying all conditions of Subsection 5.2 so that the chosen curve violates the local-global principle. Then the Jacobian of the chosen curve will meet the needs of Theorem 6.0.0.1.

Although we believe that for any number field, the curve given by the equation (1) can positively answer Clark’s conjecture [Cla09 Section 5 Conjecture 1] completely, it seems unreachable now. Our paper in progress will answer Clark’s conjecture [Cla09 Section 5 Conjecture 1] completely, but the proof is not given by an explicit construction.

\[
\text{2020 Mathematics Subject Classification. Primary 14H45; Secondary 11G05, 14G12, 14G05.}
\]

\[
\text{Key words and phrases. rational points, local-global principle, genus one curves, Brauer-Manin obstruction.}
\]
2. Notation

Given a number field $K$, let $\mathcal{O}_K$ be the ring of its integers, and let $\Omega_K$ be the set of all its nontrivial places. Let $\infty_K \subset \Omega_K$ be the subset of all archimedean places, and let $2_K \subset \Omega_K$ be the subset of all 2-adic places. Let $\infty' \subset \infty_K$ be the subset of all real places, and let $\Omega'_K = \Omega_K \setminus \infty_K$ be the set of all finite places of $K$. Let $K_v$ be the completion of $K$ at $v \in \Omega_K$. For $v \in \Omega'_K$, let $\mathbb{F}_v$ be its residue field. We say that an element is a prime element, if the ideal generated by this element is a prime ideal.

3. Compactification

In this section, we construct the smooth projective models of plane curves defined by the equation (1).

3.1. Zero loci in projective space bundles. Let $B$ be a smooth, projective, and geometrically connected variety over a number field $K$. Let $\mathcal{L}$ be a line bundle on $B$, and we assume the set of global sections $\Gamma(B, \mathcal{L}^{\otimes 2}) \neq 0$. Let $\mathcal{E} = \mathcal{O}_B \oplus \mathcal{L}$ be the rank-2 vector bundle on $B$. Let $a \in K^*$ be a constant, and let $s \in \Gamma(B, \mathcal{L}^{\otimes 2})$ be a nonzero global section. The zero locus of $(a, -s) \in \Gamma(B, \mathcal{O}_B \oplus \mathcal{L}^{\otimes 2}) \subset \Gamma(B, \text{Sym}^2 \mathcal{E})$ in the projective space bundle $\text{Proj}(\mathcal{E})$ is a projective scheme, denoted by $X$ with the natural projection $\alpha: X \to B$. We have the following lemma to ensure the smoothness of $X$.

Lemma 3.1.1. Given a number field $K$, we use the notation as in Subsection 3.1. The locus defined by $s = 0$ in $B$ is smooth, if and only if $X$ is smooth.

Proof. By the Jacobian criterion and local computation, this lemma follows. \hfill \Box

Remark 3.1.2. Consider the case that $B = \mathbb{P}^1$ and $\mathcal{L} = \mathcal{O}(n_0)$ for some fixed positive integer $n_0$. Let $s \in \Gamma(\mathbb{P}^1, \mathcal{O}(2n_0))$ be a global section, and let $s(x) \in K[x]$ be a dehomogenization of $s$. By Lemma 3.1.1 in order to ensure the smoothness of $X$, we assume that the polynomial $s(x)$ is separable of degree $2n_0$. Then $X$ is a smooth, projective, and geometrically connected curve, and it is the smooth compactification of the affine curve given by the equation $ay^2 = s(x) \in A^2$ with affine coordinates $(x, y)$.

Next, we consider the plane curve defined by the equation (1). By Remark 3.1.2, we choose the smooth projective model as in Subsection 3.1.

Corollary 3.1.3. Given a number field $K$, let $C$ be the smooth projective model of the plane curve defined by the equation (1). Then the genus of $C$ is one.

Proof. Since the polynomial $x^4 - p$ is separable over $K$, by Lemma 3.1.1 and Remark 3.1.2 we consider its smooth compactification as in 3.1 and let $\alpha: C \to \mathbb{P}^1$ be the natural projection. By Hurwitz’s Theorem [Har97, Chapter IV. Corollary 2.4], the genus of $C$ is one. \hfill \Box

4. Existence of local points

In this section, we discuss in which case the curve defined by the equation (1) has local points. By Lang-Weil estimate [LV54], a given curve over a number field $K$ has local points for almost all\footnote{The phrase "almost all" means "all but finite".} places of $K$. The following proposition tells all possible places where it doesn’t have local points. It is essential to judge whether the curve has local points.

Proposition 4.0.1. Given a number field $K$, let $C^0$ be the plane curve defined by the equation $qy^2 = x^4 - p$ in $K[x, y]$ such that $p, q$ are coprime integers in $K$. Let $S = \infty'_K \cup 2_K \cup \{v \in \Omega'_K | v(pq) \neq 0\}$ be a finite set. Then $C^0(K_v) \neq \emptyset$ for all $v \in \Omega_K \setminus S$. 

Proof. Let $C$ be the smooth compactification of $C_0$. By the implicit function theorem, we only need to check that $C(K_v) \neq \emptyset$. Suppose that $v \in \Omega_K \setminus S$, then $v$ is an odd place. If $q \in K_v^{\times 2}$, then the curve $C_0$ admits a $K_v$-point with $v(x) < 0$. Next, we consider the case $q \notin K_v^{\times 2}$. The curve $C$ has good reduction over $K_v$. Since any point in $\overline{C}(\mathbb{F}_v)$ can be lifted to a point in $C(K_v)$, we only need to prove that $\overline{C}(\mathbb{F}_v) \neq \emptyset$. Let $C'$ be the smooth compactification of the curve defined by $y^2 = x^4 - p$ in $K[x, y]$, and $C'$ be its reduction. By Remark 3.1.2 and Corollary 3.1.3, the curve $C'$ is an explicit curve over $\mathbb{F}_v$. By Hasse’s bound for elliptic over finite field [Sil90], Chapter V, Theorem 1.1], we have $2\overline{C}(\mathbb{F}_v) \leq 1 + 2\mathbb{F}_v + 2\sqrt{\mathbb{F}_v}$. So, we get $2\overline{C}(\mathbb{F}_v) < 2(1 + \mathbb{F}_v)$. If the polynomial $x^4 - p$ has a $\mathbb{F}_v$-root, then $\overline{C}(\mathbb{F}_v) \neq \emptyset$. Otherwise, we consider the map $\alpha : C' \to \mathbb{P}^1$ given by $(x, y) \mapsto x$, the same as in Subsection 3.1. Then $\mathbb{F}_v(\overline{C}(\mathbb{F}_v)) = \overline{C}(\mathbb{F}_v)/2 < 1 + \mathbb{F}_v$. So $\mathbb{P}^1(\mathbb{F}_v) \setminus \alpha(C(\mathbb{F}_v)) \neq \emptyset$. In this case, there exists an element $\overline{\pi}_v \in \mathbb{F}_v$ such that $\overline{\pi}_v^4 - p \notin \mathbb{F}_v^2$. For $q \notin K_v^{\times 2}$, the equation $qy^2 = x^4 - p$ with affine coordinates $(x, y)$ has a $\mathbb{F}_v$-solution with $x = \overline{\pi}_v$. So in each case, we have $\overline{C}(\mathbb{F}_v) \neq \emptyset$. So $C^0(K_v) \neq \emptyset$. 

We put some additional conditions for the parameters $p$, $q$ so that the curve in Proposition 4.0.1 has local points for all places.

Corollary 4.0.2. Given a number field $K$, let $C^0$ be the plane curve defined by the equation $y^2 = x^4 - p$ in $K[x, y]$ such that $p, q$ are coprime integers in $K$. Let $S_1 = \infty_K \cup 2K \cup \{v \in \Omega_K \mid v(q) \neq 0\}$. Additionally, we assume that $p$ is a prime element, and $p \in K_v^{\times 2}$ for all $v \in S_1$. Then $C^0(K_v) \neq \emptyset$ for all $v \in \Omega_K$.

Proof. By Proposition 4.0.1 we only need to check the case that $v \in S_1 \cup \{v_p\}$.

Suppose that $v \in S_1$. By assumption that $p \in K_v^{\times 4}$, then the equation $y^2 = x^4 - p$ with affine coordinates $(x, y)$ has a $K_v$-solution with $y = 0$. Suppose that $v = v_p$, then $v$ is an odd place. By the product formula $\prod_{v \in \Omega_K}(p, q)_v = 1$, we have $q \notin K_v^{\times 2}$. By Hensel’s lemma, the curve $C^0$ admits a $K_v$-point with $v(x) < 0$.

So $C^0(K_v) \neq \emptyset$ for all $v \in \Omega_K$.

5. The local-global principle for genus one curves

5.1. The Brauer-Manin obstruction. Let $C^0$ be a curve defined over a number field $K$ as in Proposition 4.0.1 and let $C$ be its smooth compactification. Let $K(C^0)$ be the function field of $C^0$. According to [Gro85, Cor. 1.8], we have an inclusion $\text{Br}(C) \hookrightarrow \text{Br}(K(C^0))$. Next, we consider the quaternion algebra class $(y, p) \in \text{Br}(K(C^0)[2])$. It is proved in [CTS21, Example 6.3.3] that this quaternion algebra class indeed belongs to $\text{Br}(C)[2]$. They proved it in a purely algebraic way. To fit into the context of this paper, we will give another proof by explicit calculations of local invariants.

Lemma 5.1.1. Given a number field $K$, let $C^0$ be the plane curve defined by the equation $y^2 = x^4 - p$ in $K[x, y]$ such that $p, q$ are coprime integers in $K$. Then the quaternion algebra class $A = (y, p) \in \text{Br}(K(C^0)[2])$ belongs to $\text{Br}(C)[2]$.

Proof. By Harari’s formal lemma [Har94, Théorème 2.1.1], it will be sufficient to prove that for almost all $v \in \Omega_K$, the local invariant $\text{inv}_v(A(P_v)) = 0$ for all $P_v \in C^0(K_v)$ with $y(P_v) \neq 0$.

Let $S = \infty_K \cup 2K \cup \{v \in \Omega_K \mid v(pq) \neq 0\}$ be a finite set. Suppose that $v \in \Omega_K \setminus S$, then $v$ is an odd place. Take an arbitrary $P_v \in C^0(K_v)$ with $y(P_v) \neq 0$. If $\text{inv}_v(A(P_v)) = 1/2$, then $(y, p)_v = -1$ at $P_v$. By Chevalley-Warning theorem [Ser73, Chapter I §2, Corollary 2], the valuation $y$ is odd at $P_v$, which implies $y(v) > 0$. So the polynomial $x^4 - p$ has a $\mathbb{F}_v$-root. By Hensel’s lemma, we have $p \in K_v^{\times 2}$, which contradicts $(y, p)_v = -1$. So $\text{inv}_v(A(P_v)) = 0$.

We make the following assumption on the base field and the parameters of the equation (1) so that the curve given by this equation violates the local-global principle.
5.2. Assumption on a number field. Let $K$ be a number field. For the ideal class group of $K$ is finite, we take a positive integer $N$ such that $\mathcal{O}_K[1/N]$ is a principal ideal domain. Let $S_2 = \infty'_K \cup 2_K \cup \{v \in \Omega_K^f|v(N) \neq 0\}$ be a finite set. We make the following assumption on the number field $K$.

Assumption 5.2.1. For a number field $K$, we assume that there exist a pair of coprime integers $(p, q)$ and an odd place $v_0 \in \Omega_K$ satisfying the following assumption.

1. $p$ is a prime element,
2. $p \in K_v^{\times 4}$ for all $v \in S_2$,
3. $q \in K_v^{\times 2}\setminus K_v^{\times 4}$,
4. $\mathbb{F}_v \equiv 3 \pmod{4}$,
5. $v_0(q) = 1$,
6. $\{v \in \Omega_K^f|v(q) \neq 0\}\setminus \{v_0\} \subset \{v \in \Omega_K^f|v(N) \neq 0\}$.

5.3. The local-global principle. The following proposition states that the curve given by the equation (1) with parameters satisfying Assumption 5.2.1 let $C^0$ be the plane curve defined by the equation $yy^2 = x^4 - p$ in $K[x, y]$. Then $C^0(K_v) \neq \emptyset$ for all $v \in \Omega_K$.

Proof. We will check that the parameters satisfy all conditions of Corollary 4.10.2. Let $S_1 = \infty'_K \cup 2_K \cup \{v \in \Omega_K^f|v(q) \neq 0\}$ as in Corollary 4.10.2 and let $S_2 = \infty'_K \cup 2_K \cup \{v \in \Omega_K^f|v(N) \neq 0\}$ as in Subsection 5.2.1. Then $S_1 \setminus \{v_0\} \subset S_2$. By the choice of $p$ and Corollary 4.10.2, we only need to prove that $p \in K_v^{\times 4}$. By the product formula $\prod_{v \in \Omega_K} (p, q)_v = 1$ and $q \in K_v^{\times 2}$, we have $(p, q)_v = 1$. By Assumption (5), the reduction $\bar{p} \in \mathbb{F}_v^{\times 2}$. By Assumption (4) that $\mathbb{F}_v \equiv 3 \pmod{4}$, we have $\bar{p}^{v_0} = \mathbb{F}_v^{\times 4}$, so $\bar{p} \in \mathbb{F}_q^\times$. By Hensel’s lemma, we have $p \in K_v^{\times 4}$. \hfill \Box

By Lemma 5.1.1 the quaternion algebra class $A = (y, p) \in \text{Br}(K(C^0))[2]$ belongs to $\text{Br}(C)[2]$. For the curve given in Proposition 5.3.1, we calculate the local invariant $\text{inv}_v(A(P_v))$ for all $P_v \in C(K_v)$ and any $v \in \Omega_K$.

Lemma 5.3.2. For a number field $K$, we assume that there exist a pair of coprime integers $(p, q)$ and an odd place $v_0 \in \Omega_K$ satisfying Assumption 5.2.1. Let $C$ be the smooth projective model of the plane curve defined by the equation $yy^2 = x^4 - p$ in $K[x, y]$. Let $A = (y, p) \in \text{Br}(C)[2]$. Then, for any $v \in \Omega_K$, and any $P_v \in C(K_v)$,

$$\text{inv}_v(A(P_v)) = \begin{cases} 0 & \text{if } v \neq v_0, \\ 1/2 & \text{if } v = v_0. \end{cases}$$

Proof. For the evaluation of $A$ on $C(K_v)$ is locally constant, the implicit function theorem implies that we only need to calculate $\text{inv}_v(A(P_v))$ for all $P_v \in C^0(K_v)$ with $y(P_v) \neq 0$.

Let $S = \infty'_K \cup 2_K \cup \{v \in \Omega_K^f|v(pq) \neq 0\}$ be a finite set. As in the proof of Lemma 5.1.1 for any $v \in \Omega_K \setminus S$, and any $P_v \in C^0(K_v)$ with $y(P_v) \neq 0$, we have $\text{inv}_v(A(P_v)) = 0$. Suppose that $v \in S \setminus v_0, v_p$. Let $S_2 = \infty'_K \cup 2_K \cup \{v \in \Omega_K^f|v(N) \neq 0\}$ as in Subsection 5.2.1 then $v \in S_2$. By Assumption (2), we have $\text{inv}_v(A(P_v)) = 0$ for all $P_v \in C^0(K_v)$ with $y(P_v) \neq 0$.

Suppose that $v = v_0$. By the same argument as in the proof of Proposition 5.3.1 we have $p \in K_v^{\times 4}$, which implies $\text{inv}_v(A(P_v)) = 0$ for all $P_v \in C^0(K_v)$ with $y(P_v) \neq 0$.

Suppose that $v = v_p$. Take an arbitrary $P_v \in C^0(K_v)$. By comparing the valuation of the equation (1), we have $v(x) \leq 0$ and $x^4 - p \in K_v^{\times 4}$ at $P_v$. By Assumption (3), we have $q \in K_v^{\times 2}\setminus K_v^{\times 4}$. Then $y \not\in K_v^{\times 2}$, so $\text{inv}_v(A(P_v)) = 1/2$ at $P_v$. \hfill \Box

Combining Lemma 5.3.2 with the global reciprocity law, we have the following proposition that the curve given by the equation (1) with parameters satisfying Assumption 5.2.1 has no $K$-rational point.
Proposition 5.3.3. For a number field $K$, we assume that there exist a pair of coprime integers $(p, q)$ and an odd place $v_0 \in \Omega_K$ satisfying Assumption 5.2.1. Let $C$ be the smooth projective model of the plane curve defined by the equation $qy^2 = x^4 - p$ in $K[x, y]$. Then $C(K) = \emptyset$.

Proof. If the curve $C$ has a $K$-rational point, then by the global reciprocity law, the sum $\sum_{v \in \Omega_K} \nu_v(A(P)) = 0$ in $\mathbb{Q}/\mathbb{Z}$. By Lemma [5.3.2] the sum is 1/2, which is nonzero in $\mathbb{Q}/\mathbb{Z}$.

Applying Proposition 5.3.3, the Jacobian of $C$ will have the following proposition.

Proposition 5.3.4. For a number field $K$, we assume that there exist a pair of coprime integers $(p, q)$ and an odd place $v_0 \in \Omega_K$ satisfying Assumption 5.2.1. Then there exists an elliptic curve $E$ defined over $K$ such that $\mathbb{III}(K, E)[2] \neq \emptyset$.

Proof. Let $C$ be the smooth projective model of the plane curve defined by the equation $qy^2 = x^4 - p$ in $K[x, y]$. Let $E$ be the Jacobian of $C$. By Corollary 4.0.2, the curve $E$ is an elliptic curve. Consider the class $[C] \in H^1(K, E)$. By Proposition 5.3.1, the set $C(K_v) \neq \emptyset$ for every $v \in \Omega_K$, which implies $[C] \in \mathbb{III}(K, E)$. By Proposition 5.3.3, the set $C(K) = \emptyset$, which implies $[C] \neq 0$. For $C(K, \mathbb{Z}[\eta]) \neq 0$, the standard restriction-corestriction argument implies $2[C] = 0$, so $[C] \in \mathbb{III}(K, E)[2]$ is a nonzero element. □

6. Assumption 5.2.1 holds for number fields not containing $\mathbb{Q}(i)$

Let $K$ be a number field not containing $\mathbb{Q}(i)$. In this section, we will find a pair of coprime integers $(p, q)$ and an odd place $v_0 \in \Omega_K$ satisfying Assumption 5.2.1.

The following lemma is a consequence of the Čebotarev density theorem.

Lemma 6.0.1. Let $K$ be a number field not containing $\mathbb{Q}(i)$. Let $P_K$ be the set of prime numbers $p$ such that

- $p$ splits over $K$, i.e. there exists a place $v \in \Omega_K$ such that $K_v \cong \mathbb{Q}_p$.
- $p \equiv 3 \mod 4$.

Then the set $P_K$ is an infinite set.

Proof. Let $\overline{K}$ be an algebraic closure field of $K$. Let $L$ be the Galois closure of $K/\mathbb{Q}$ in $\overline{K}$. For $\mathbb{Q}(i) \notin \overline{K}$, the extension $L(i)/K$ is a nontrivial Galois extension. Take an element $\sigma \in \text{Gal}(L(i)/K)$ such that the restriction of $\sigma$ on $K(i)$ is nontrivial. Let $P_{L(i)}$ be the set of all prime numbers $p$ such that there exists a place $v/p \in \Omega_{L(i)}$ satisfying that the subgroup $\text{Gal}(L(i)/\mathbb{Q}_p) \subset \text{Gal}(L(i)/\mathbb{Q})$ is generated by $\sigma$. Similar to the proof of [Neu99] Chapt. VII Theorem 13.4, the set $P_{L(i)}$ has positive density. Take an arbitrary prime number $p_0 \in P_{L(i)}$ unramified over $L(i)$. Then there exists a place $v_0|p_0$ in $\Omega_{L(i)}$ such that $\text{Gal}(L(i)/\mathbb{Q}_{p_0})$ is generated by $\sigma$. Let $v_0'$, $w_0$ be the restriction of $v_0$ on $K(i)$ and $K$ respectively. Then $K_{w_0} \cong \mathbb{Q}_{p_0}$, and $K(i)_{w_0}/K_{w_0}$ is a nontrivial unramified extension. So $p_0$ splits over $K$, and $p_0 \equiv 3 \mod 4$. So the set $P_K$ is an infinite set. □

Remark 6.0.2. One can calculate that the density $d(P_K) \geq \frac{1}{2[K: \mathbb{Q}]}$. Here $[K : \mathbb{Q}]$ is the degree of the extension $K/\mathbb{Q}$.

Given a number field $K$ not containing $\mathbb{Q}(i)$, let $N$ and $S_2 = \infty_K \cup 2K \cup \{v \in \Omega_K | v(N) \neq 0\}$ be as in Subsection 5.2.2. We will choose $(p, q)$ and an odd place $v_0 \in \Omega_K$ satisfying Assumption 5.2.1.

Proposition 6.0.3. Let $K$ be a number field not containing $\mathbb{Q}(i)$. Then there exist a pair of coprime integers $(p, q)$ and an odd place $v_0 \in \Omega_K$ satisfying Assumption 5.2.1.

Proof. Let $m_\infty$ be the product of all places in $\infty_K$, and let $m = 16N^2m_\infty$ be a modulus of $K$. Let $K_m$ be the ray class field of modulus $m$, then $\mathbb{Q}(i) \subset K_m$. Let $I_m$ be the subgroup of fractional ideals that are prime to $16N^2$. Let $P_m \subset I_m$ be the subgroup of principal ideals
generated by some $a \in K^\times$ with $a \equiv 1 \mod 16N^2$ and $\tau_v(a) > 0$ for all $v \in \infty^r_K$. Then by Artin reciprocity law (cf. [Neu99] Chapter VI Theorem 7.1 and Corollary 7.2)), the classical Artin homomorphism $\theta$ gives an exact sequence:

$$(2) \quad 0 \to P_m \to I_m \to \Gal(K_m/K) \to 0.$$

By Lemma 6.0.1, we take a place $v_0 \in \Omega_K$ such that $\mathfrak{p}P_{v_0} \equiv 3 \mod 4$, and $v_0$ unramified over $K_m$. For $\mathcal{O}_K[1/N]$ is a principle ideal domain, we can take $q \in \mathcal{O}_K$ satisfying Assumption (3) and Assumption (4). For $v_0$ is unramified over $K_m$ and $v_0(q) = 1$, the Galois group $\Gal(K_m(\sqrt{q})/K_m) \cong \mathbb{Z}/4\mathbb{Z}$ denoted a generator by $\sigma$. By Čebotarev density theorem [Neu99] Chapt. VII Theorem 13.4], there exist a place $v'_1$ in $\Omega_{K_m}(\sqrt{q})$ and its restriction $v_1 \in \Omega_K$ such that $\Gal(K_m(\sqrt{q})v'_1/K_{v_1})$ is generated by $\sigma^2$. Then $v_1$ splits completely in $K_m$. By [Neu99] Chapt. VI Corollary 7.4 and the exact sequence (2), the place $v_1$ is associated to a prime element $p \in P_m$. So Assumption (1) and Assumption (2) hold. By the choice of $v_1$, the assumption $q \in K^\times 2\setminus K^\times 4$ holds.

Combining Proposition 5.3.4 and Proposition 6.0.3 we get our theorem.

**Theorem 6.0.0.1.** For any number field $K$ not containing $\mathbb{Q}(i)$, there exists an elliptic curve $E$ defined over $K$ such that $\text{III}(K,E)[2] \neq 0$.

**Acknowledgements.** The author would like to thank D.S. Wei, Y. Xu and C. Lv for many fruitful discussions. The author is grateful to B. Poonen and anonymous referees for their valuable suggestions. The author was partially supported by NSFC Grant No. 12071448.

**References**

[Cla09] P. L. Clark, *Curves over global fields violating the hasse principle*, Preprint, arXiv:0905.3459 [math.NT] (2009).

[CTS21] J.-L. Colliot-Thélène and A.N. Skorobogatov, *The Brauer-Grothendieck group*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 3. Folge, 71, Springer-Verlag, 2021.

[Gro68] A. Grothendieck, *Le groupe de Brauer II: Exemples et compléments*. In: *Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics, vol. 3, North-Holland, 1968 (French). pp. 66-87.

[Har94] D. Harari, *Méthode des fibrations et obstruction de manin*, Duke Math. J. 75 (1994), 221-260.

[Har97] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, 1997.

[Lin40] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppsala 1940 (1940), 97 (German).

[LV54] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. 76 (1954), 819-827.

[Neu99] J. Neukirch, *Algebraic number theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 3. Folge, 71, Springer-Verlag, 1999.

[Poo10] B. Poonen, *Curves over every global field violating the local-global principle*, J. Math. Sci. 171 (2010), no. 6, 782-785.

[Rei42] H. Reichardt, *Einige im Kleeen überall lösbare, im Grossen unlösbare diophantische Gleichen*, J. reine angew. Math. 184 (1942), 12-18 (German).

[Sel51] E.S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. 85 (1951), 203-362.

[Ser73] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag, 1973.

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 2009.