J. Ramanujan Math. Soc. **34,** No.3 (2019) 271–279

Sufficient conditions for the existence of rational points on diagonal cubic surfaces

Yosuke Shimizu

Bannnai laboratory at Keio University in Japan
e-mail: yosuke.z3@keio.jp

Communicated by: Prof. Sanoli Gun

Received: December 6, 2017

Abstract. In this paper, we construct diagonal cubic surfaces over $\mathbb{Q}$ which have a $\mathbb{Q}$-rational point under the assumption that the Tate-Shafarevich group of elliptic curve $X^3 + Y^3 = AZ^3$ is finite. We can also check that there is no Brauer-Manin obstruction for these surfaces without the finiteness assumption of the Tate-Shafarevich group.

2010 Mathematics Subject Classification: 11D25 and 14G05.

0. Introduction

Let V be the smooth projective surface over $\mathbb{Q}$ defined by

$$V : a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + a_4X_4^3 = 0,$$

where $a_1a_2a_3a_4 \neq 0$. Without loss of generality we may assume that a_i are cube free integers. It is a fundamental problem of determining whether an algebraic variety has a rational point or not. If an algebraic variety over $\mathbb{Q}$ has a $\mathbb{Q}$-rational point, then obviously it has a $\mathbb{Q}_v$-rational point for every place v of $\mathbb{Q}$. If the converse is also true, then we say that it satisfies the Hasse principle. The Hasse-Minkowski theorem says the Hasse principle holds for the projective quadratic hypersurfaces [Coh, Theorem 5.3.3]. However the Hasse principle does not hold in general for V. In fact, a lot of counterexamples were constructed, for example, in [CKS], [Corn]. All these counterexamples are explained by the Brauer-Manin obstruction (See, for example, [Sko] for the Brauer-Manin obstruction). The problem here is that if there is no Brauer-Manin obstruction, then it has a rational point or not. It is conjectured that the Brauer-Manin obstruction is the only obstruction to the Hasse principle for V (It is conjectured for more general algebraic varieties. See [PV, Conjecture 3.2 and Remark 3.3] for this conjecture and its history.).

As for the existence of rational points on V, there are several results in [BF], [SD], [Sat]. They gave some sufficient conditions for V to have a rational point under the assumption that the Tate-Shafarevich group of elliptic curve $X^3 + Y^3 = AZ^3$ is finite. Note that it is known that the Brauer-Manin obstruction is empty without the finiteness assumption of the Tate-Shafarevich group under their conditions. In particular, in [Sat], Sato showed the existence of a $\mathbb{Q}$-rational point on V by showing that the curve C on V (e.g., $a_1X_1^3 + a_2X_2^3 + a_3X_3^3 = 0$) has a $\mathbb{Q}$-rational point by calculating the Selmer group of the Jacobian of C. More specifically, he showed that the Selmer groups of the elliptic curves defined by

$$X^3 + Y^3 = p_1p_2p_3^2Z^3$$

where p_i are distinct rational primes such that $(p_1, p_2, p_3) \equiv (2, 2, 5)$ or $(5, 5, 2) \mod 9$ and

$$X^3 + Y^3 = p_1^2p_2^2p_3^2Z^3$$

This research was conducted as part of the KiPAS program 2014–2019 of the Faculty of Science and Technology at Keio University. This research was supported in part by KAKENHI 26247004, as well as the JSPS Core-to-Core program "Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory and Geometry".

where p_i are distinct rational primes such that $(p_1, p_2, p_3) \equiv (2, 2, 2)$ or $(5, 5, 5) \mod 9$ are $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ [Sat, Lemma 2.5, Lemma 2.6]. In this paper, we calculate the Selmer groups of all elliptic curves defined by

$$X^3 + Y^3 = p_1^{n_1} \dots p_r^{n_r} Z^3$$

where r is a positive integer, $p_1, \dots, p_r$ are distinct rational primes such that $p_1, \dots, p_r \equiv 2 \mod 3$, and $n_1, \dots, n_r \in \{0, 1, 2\}$ and classify curves whose Selmer groups are $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Then we construct new diagonal cubic surfaces over $\mathbb{Q}$ which have a $\mathbb{Q}$-rational point under the assumption that the Tate-Shafarevich group of the elliptic curve $X^3 + Y^3 = AZ^3$ is finite (Theorem 3.1). For example, we show the following.

Theorem 0.1 (Theorem 3.1 (i)). *Let p_1, p_2, p_3 be rational primes, each congruent to either 2 or 5 modulo 9 and*

$$V : p_1 X_1^3 + p_2 X_2^3 + p_3 X_3^3 + p_1 p_2 p_3 X_4^3 = 0$$

be a cubic surface over $\mathbb{Q}$. Assume that the Tate-Shafarevich group of the elliptic curve over $\mathbb{Q}$ defined by

$$\begin{cases} X^3 + Y^3 = p_1 p_2 p_3 Z^3 & \text{if } (p_1, p_2, p_3) \equiv (2, 2, 2) \text{ or } (5, 5, 5) \mod 9 \\ X^3 + Y^3 = p_1^2 p_2^2 p_3 Z^3 & \text{if } (p_1, p_2, p_3) \equiv (2, 2, 5) \text{ or } (5, 5, 2) \mod 9 \end{cases}$$

is finite. Then $V(\mathbb{Q}) \neq \emptyset$.

Remark 0.2.

(i) The statement of Theorem 3.1 (i) is slightly different from the above statement of Theorem 0.1. However note that the above statement is also true since the defining equation of V is symmetric.
(ii) There is no Brauer-Manin obstruction for the surfaces V in Theorem 3.1 without the finiteness assumption of the Tate-Shafarevich group. See Remark 3.3 and Remark 3.5 for the details.
(iii) We can check easily that we cannot apply [SD, Theorem 1] to Theorem 3.1 (i) $\sim$ (xi) (Remark 3.2). The condition in [SD, Theorem 1] is slightly stronger than the disappearance of the Brauer-Manin obstruction.

We give an overview of this paper. In §1, we recall the argument on descent developed by Basile and Fisher [BF] and introduce some notations. Our assumption that the Tate-Shafarevich group of the elliptic curve

$$E_A : X^3 + Y^3 = AZ^3$$

is finite is needed to use their argument. In §2, we calculate the $\sqrt{-3}$-Selmer group of elliptic curve E_A for $A = p_1^{n_1} \dots p_r^{n_r}$ where r is a positive integer, $p_1, \dots, p_r$ are distinct rational primes such that $p_1, \dots, p_r \equiv 2 \mod 3$, and $n_1, \dots, n_r \in \{0, 1, 2\}$. Then we classify curves whose Selmer groups are $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. In §3, we prove Theorem 3.1 by use of the calculation results of the Selmer groups in §2.

Acknowledgements

First, I would like to thank my advisor Kenichi Bannai for his warm supports and suggestion to write this article. I'm also thankful to every member of KiPAS-AGNT group for their helpful comments and useful discussions, especially Masataka Ono who gave me significant advice in order to make this article more readable. Second, I would like to thank Tom Fisher and Kazuki Sato who answered my question about their papers [BF], [Sat]. Finally I would like to thank the referee who read this paper very carefully and gave a number of valuable comments.

1. Descent on $X^3 + Y^3 = AZ^3$

In this section, we recall the argument on descent developed in [BF]. Let ζ_3 be a primitive cube root of unity and $K = \mathbb{Q}(\zeta_3)$. For a cube free integer $A \in \mathbb{Z} \backslash \{0, \pm 1\}$, we denote by E_A the elliptic curve defined by

$$E_A : X^3 + Y^3 = AZ^3$$

with identity $O = (1, -1, 0)$. E_A admits complex multiplication, so that $\mathrm{End}_K(E_A) = \mathbb{Z}[\zeta_3]$. In fact, ζ_3 acts on E_A by $(x, y, z) \mapsto (x, y, \zeta_3 z)$, and the multiplication-by-$\sqrt{-3}$ endomorphism on E_A is given by

$$\sqrt{-3} : (x, y, z) \mapsto (\zeta_3 x^3 - \zeta_3^2 y^3, \zeta_3 y^3 - \zeta_3^2 x^3, (\zeta_3 - \zeta_3^2)xyz).$$

Fix the algebraic closure $\overline{K}$ of K and we denote by G_K the absolute Galois group of K. Then we have the following commutative diagram with exact row

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_A(K)/\sqrt{-3}E_A(K) & \longrightarrow & H^1(G_K, E_A[\sqrt{-3}]) & \longrightarrow & WC(E_A/K)[\sqrt{-3}] & \longrightarrow & 0 \\ & & & & & \searrow & \downarrow & & \\ & & & & & & \prod_v WC(E_A/K_v)[\sqrt{-3}] & & \end{array}$$

where $WC(E_A/K)$ is the Weil-Châelet group of E_A/K and v runs over all the places of K.

Lemma 1.1. *The group $E_A(\overline{K})[\sqrt{-3}]$ of $\sqrt{-3}$-torsion points is isomorphic to the group $\mu_3(\overline{K})$ of cube roots of unity as a G_K-module.*

Proof. A calculation shows that the kernel of $\sqrt{-3} : E_A \to E_A$ is $\{O, T, -T\}$ where $T = (\zeta_3, -\zeta_3^2, 0)$ and $-T = (\zeta_3^2, -\zeta_3, 0)$. An isomorphism of Galois modules $\iota : \mu_3(\overline{K}) \to E_A(\overline{K})[\sqrt{-3}]$ is given by $\iota(\zeta_3^i) = (\zeta_3^i, -\zeta_3^{2i}, 0)$ where $i = 0, 1, 2$. □

By Kummer theory and Lemma 1.1, $H^1(G_K, E_A[\sqrt{-3}])$ is isomorphic to $K^*/(K^*)^3$ and so we get the exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_A(K)/\sqrt{-3}E_A(K) & \longrightarrow & K^*/(K^*)^3 & \xrightarrow{f} & WC(E_A/K)[\sqrt{-3}] & \longrightarrow & 0\,. \\ & & & & & \searrow^{g} & \downarrow & & \\ & & & & & & \prod_v WC(E_A/K_v)[\sqrt{-3}] & & \end{array}$$

Lemma 1.2. *The above map f sends an element $\alpha(K^*)^3$ to the principal homogeneous spases*

$$C_{A,\alpha} : \alpha X^3 + \alpha^{-1} Y^3 = AZ^3$$

for E_A.

Proof. Let T and ι be the same as the proof of Lemma 1.1. The translation by T map $E_A \to E_A$, $P \mapsto P + T$ is given by $(x, y, z) \mapsto (\zeta_3 x, \zeta_3^{-1} y, z)$. Let β be a cube root of α and $\psi : C_{A,\alpha} \to E_A$ be the isomorphism $\overline{K}$ given by $(x, y, z) \mapsto (\beta x, \beta^{-1} y, z)$. Then for $\sigma \in G_K$, we have

$$\psi^\sigma \circ \psi^{-1} = \text{translation by } \iota(\sigma(\beta)/\beta) \text{ map.}$$

Therefore the class of $C_{A,\alpha}$ in $H^1(G_K, E_A)$ is represented by the cocycle $\sigma \mapsto \iota(\sigma(\beta)/\beta)$. This cocycle takes values in $E_A[\sqrt{-3}]$ and so also represents an element in $H^1(G_K, E_A[\sqrt{-3}])$. Finally we note that the identification of $K^*/(K^*)^3$ and $H^1(G_K, \mu_3(\overline{K}))$ coming from Kummer theory identifies $\alpha(K^*)^3$ with the class of $\sigma \mapsto \sigma(\beta)/\beta$. This give the description of the map f as desired. □

We denote by $S(A)$ the $\sqrt{-3}$-Selmer group $S^{(\sqrt{-3})}(E_A/K)$ (which is defined to be the kernel of the map g in the diagram above) and by $C(A)$ the kernel of the map f. Then $C(A)$ is a subgroup of $S(A)$ and by Lemma 1.2 we can write them explicitly

$$S(A) = \{\alpha(K^*)^3 \mid C_{A,\alpha} \text{ has } K_v\text{-rational points for any prime } v \text{ of } K, \alpha \in K^*\},$$

$$C(A) = \{\alpha(K^*)^3 \mid C_{A,\alpha} \text{ has } K\text{-rational points}, \alpha \in K^*\}.$$

Furthermore, we have the exact sequence

$$0 \longrightarrow C(A) \longrightarrow S(A) \longrightarrow Ш(E_A/K)[\sqrt{-3}] \longrightarrow 0$$

where $Ш(E_A/K)$ is a Tate-Shafarevich group of E_A/K. The following lemma provides the Hasse principle for the curve $C_{A,\alpha}$ when $S(A) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Lemma 1.3. *Notations are the same as above. Assume that the Tate-Shafarevich group $Ш(E_A/\mathbb{Q})$ of E_A over $\mathbb{Q}$ is finite. If $S(A) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then $C(A) = S(A)$.*

Proof. Assume that $C(A)$ is a proper subgroup of $S(A)$. Note that $C(A)$ contains a nontrivial element $A(K^*)^3$ since $C_{A,A}$ has a point $(1, 0, 1)$. Thus $C(A) \cong \mathbb{Z}/3\mathbb{Z}$. From the exact sequence

$$0 \longrightarrow C(A) \longrightarrow S(A) \longrightarrow Ш(E_A/K)[\sqrt{-3}] \longrightarrow 0$$

we have $Ш(E_A/K)[\sqrt{-3}] \cong \mathbb{Z}/3\mathbb{Z}$. However this is impossible by [BF, Lemma 5]. □

2. Calculation of Selmer groups

Let A be a cube free integer. In this section we calculate the Selmer group $S(A)$ for $A = p_1^{n_1} \dots p_r^{n_r}$ where r is a positive integer, $p_1, \dots, p_r$ are distinct rational primes such that $p_1, \dots, p_r \equiv 2 \mod 3$ and $n_1, \dots, n_r \in \{0, 1, 2\}$. Then we classify curves whose Selmer groups are $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We use this calculation results in §3. In §1, we regard $S(A)$ as a subgroup of $K^*/(K^*)^3$. In the following, we identify an element of K^* with its images in $K^*/(K^*)^3$. For a prime element q in $\mathbb{Z}[\zeta_3]$, we simply denote by K_q the (q)-adic field $K_{(q)}$.

Let $\alpha \in K^*$ be a representative of an element in $K^*/(K^*)^3$. Then we may assume that $\alpha \in \mathbb{Z}[\zeta_3]$ is a non-zero cube free integer by multiplication by an element of $(K^*)^3$. Let $A = \prod_{i=1}^r q_i^{n_i}$ be a prime factorization of A in $\mathbb{Z}[\zeta_3]$, where q_i are distinct primes in $\mathbb{Z}[\zeta_3]$ and $n_i \in \mathbb{Z}_{\geq 1}$. The condition $\alpha \in S(A)$ implies that α is of the form

$$\alpha = \zeta_3^m \prod_{i=1}^r q_i^{m_i}, \ m, m_1, \dots, m_r \in \{0, 1, 2\}$$

by [Sat, Lemma 2.1]. Conversely, if the above α satisfies $C_{A,\alpha}(K_q) \neq \emptyset$ for every prime q of K dividing $3A$, then it follows from [Sat, Lemma 2.2] that $\alpha \in S(A)$.

Before calculating the Selmer groups, we show the following three lemmas.

Lemma 2.1. *Let $p_1, \dots, p_r$ be distinct rational primes such that $p_i \equiv 2 \mod 3$ $(i = 1, \dots, r)$. Put $A = p_1^{n_1} \cdots p_r^{n_r}$ and $\alpha = \zeta_3 p_1^{m_1} \cdots p_r^{m_r}$ where $n_1, \dots, n_r \in \{1, 2\}$, $m_1, \dots, m_r \in \{0, 1, 2\}$. If there exists $i \in \{1, \dots, r\}$ such that $p_i \not\equiv 8 \mod 9$, then $\alpha \notin S(A)$.*

Proof. Since $p_i \equiv 2 \mod 3$, p_i remains prime in $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}_{p_i}^* \subset (\mathbb{Q}_{p_i}^*)^3$. Therefore the curve $C_{A,\alpha}$ is isomorphic to

$$C : \zeta_3 p_i^{m_i} X^3 + \zeta_3^{-1} p_i^{-m_i} Y^3 = p_i^{n_i} Z^3$$

over K_{p_i}. A valuation-theoretic argument yields that if C has a K_{p_i}-rational point, then we see that ζ_3 is a cube in K_{p_i}. On the other hand, as $p_i \not\equiv 8 \mod 9$, there can't be any elements of order 9 in the residue field (as the residue field has cardinality p_i^2, which is not $1 \mod 9$), and so ζ_3 can't be a perfect cube. This is contradiction. Therefore $\alpha \notin S(A)$. □

Lemma 2.2. *Let $p_1, \dots, p_r$ be distinct rational primes such that $p_i \equiv 2 \mod 3$ $(i = 1, \dots, r)$. Let $A = p_1^{n_1} \cdots p_r^{n_r}$ and $\alpha = \zeta_3^m p_1^{m_1} \cdots p_r^{m_r}$ where $n_1, \dots, n_r \in \{1, 2\}$, $m, m_1, m_r \in \{0, 1, 2\}$. If $m = 0$, then $C_{A,\alpha}(K_{p_i}) \neq \emptyset$ for all $i \in \{1, \dots, r\}$.*

Proof. Since $p_i \equiv 2 \mod 3$, the curve $C_{A,\alpha}$ is isomorphic to

$$p_i^{m_i} X^3 + p_i^{-m_i} Y^3 = p_i^{n_i} Z^3$$

over K_{p_i}. This has a K_{p_i}-rational point. □

In the following, we write $\lambda = 1 - \zeta_3$.

Lemma 2.3. *Let $A = p_1^{n_1} \dots p_r^{n_r}$ where $p_1, \dots, p_r$ are distinct rational primes and $n_1, \dots, n_r \in \{1, 2\}$. If $p_1 \equiv \cdots \equiv p_r \equiv 8 \mod 9$, then $S(A) = \langle \zeta_3, p_1, \dots, p_r \rangle \cong \prod_{i=1}^{r+1} \mathbb{Z}/3\mathbb{Z}$.*

Proof. As $p_i \equiv 8 \mod 9$, the residue field has an element of order 9 and hence ζ_3 is a cube in K_{p_i}. The curve C_{A,ζ_3} is isomorphic to

$$X^3 + Y^3 = p_i^{n_i} Z^3$$

over K_{p_i}. This has a K_{p_i}-rational point. Since $p_i \equiv 8 \mod 9$, p_i is a cube in $\mathbb{Q}_3 \subset K_\lambda$. Thus the curve C_{A,ζ_3} is isomorphic to

$$\zeta_3 X^3 + \zeta_3^2 Y^3 = Z^3$$

over K_λ. This has a K_λ-rational point $(X, Y, Z) = (1, 1, -1)$. Therefore $\zeta_3 \in S(A)$. The curve C_{A,p_i} is isomorphic to

$$p_i X^3 + p_i^2 Y^3 = p_i^{n_i} Z^3$$

over K_{p_j} for $j = i$ and

$$X^3 + Y^3 = p_j^{n_j} Z^3$$

over K_{p_j} for all $j \neq i$. These have a K_{p_j}-rational point. The curve C_{A,p_i} is isomorphic to

$$X^3 + Y^3 = Z^3$$

over K_λ. This has a K_λ-rational point. Thus $p_i \in S(A)$. Therefore we have $S(A) = \langle \zeta_3, p_1, \dots, p_r \rangle \cong \prod_{i=1}^{r+1} \mathbb{Z}/3\mathbb{Z}$. □

Let r be a positive integer and $p_1, \dots, p_r$ be distinct rational primes such that $p_i \equiv 2 \mod 3$, and $A = p_1^{n_1} \dots p_r^{n_r}$ where $n_1, \dots, n_r \in \{0, 1, 2\}$. In the following proposition, we show all calculation results of $S(A)$ which have order 9 (Even if the order is not equal to 9, we can calculate $S(A)$ in the same way.).

Proposition 2.4. *Let r be a positive integer and $p_1, \dots, p_r$ be distinct rational primes.*

(i) *Let $A = p_1$ or p_1^2. Then*

$$S(A) = \langle A, \zeta_3 \rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ if } p_1 \equiv 8 \mod 9.$$

(ii) *Let $A = p_1 p_2$. Then*

$$S(A) = \langle A, p_1 \rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ if } (p_1, p_2) \equiv (2, 2), (2, 8), (5, 5), (5, 8) \mod 9.$$

(iii) *Let $A = p_1 p_2^2$. Then*

$$S(A) = \langle A, p_1 \rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ if } (p_1, p_2) \equiv (2, 5), (2, 8), (5, 2), (5, 8), (8, 2), (8, 5) \mod 9.$$

(iv) *Let $A = p_1^2 p_2^2$. Then*

$$S(A) = \langle A, p_1 \rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ if } (p_1, p_2) \equiv (2, 2), (2, 8), (5, 5), (5, 8) \mod 9.$$

(v) *Let* $A = p_1p_2p_3$. *Then*

$$S(A) = \begin{cases} \langle A, p_1p_2^2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,2,2) \text{ or } (5,5,5) \mod 9 \\ \langle A, p_1p_2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,5,8) \mod 9. \end{cases}$$

(vi) *Let* $A = p_1p_2p_3^2$. *Then*

$$S(A) = \begin{cases} \langle A, p_1p_3^2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,8,2) \text{ or } (5,8,5) \mod 9 \\ \langle A, p_1p_2^2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,2,5) \text{ or } (5,5,2) \mod 9 \\ \langle A, p_1p_2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,5,8) \mod 9. \end{cases}$$

(vii) *Let* $A = p_1p_2^2p_3^2$. *Then*

$$S(A) = \begin{cases} \langle A, p_2p_3^2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,5,5) \text{ or } (5,2,2) \mod 9 \\ \langle A, p_1p_2^2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,2,8) \text{ or } (5,5,8) \mod 9 \\ \langle A, p_2p_3\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (8,2,5) \mod 9. \end{cases}$$

(viii) *Let* $A = p_1^2p_2^2p_3^2$. *Then*

$$S(A) = \begin{cases} \langle A, p_1p_2^2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,2,2) \text{ or } (5,5,5) \mod 9 \\ \langle A, p_1p_2\rangle \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } (p_1, p_2, p_3) \equiv (2,5,8) \mod 9. \end{cases}$$

(ix) *Assume* $p_1, \ldots, p_r \equiv 2 \mod 3$. *Put* $A = p_1^{n_1} \cdots p_r^{n_r}$ *where* $n_1, \ldots, n_r \in \{0,1,2\}$. *If* A *is not listed above (i)* $\sim$ *(ix), then the order of* $S(A)$ *is not equal to* 9. *Thus we cannot apply Lemma 1.3.*

Proof. Let $p_1, \ldots, p_r$ be rational primes such that $p_1, \ldots, p_r \equiv 2 \mod 3$ and $A = p_1^{n_1} \ldots p_r^{n_r}$ where $n_1, \ldots, n_r \in \{0,1,2\}$. If $(p_1, \ldots, p_3) \equiv (8, \ldots, 8) \mod 9$, then we have already calculated $S(A)$ in Lemma 2.3. Assume $(p_1, \ldots, p_r) \not\equiv (8, \ldots, 8) \mod 9$. By Lemma 2.1, if $\zeta_3^m p_1^{m_1} \ldots p_r^{m_r} \in S(A)$, then $m = 0$ and $C_{A, p_1^{m_1} \ldots p_r^{m_r}}$ has a K_{p_i}-rational point for $i = 1, \ldots, r$ by Lemma 2.2. Thus we only have to check whether or not $C_{A, p_1^{m_1} \ldots p_3^{m_3}}$ has a K_λ-rational point. We note from [Cora, Proposition 2.2] that since these curves are defined over $\mathbb{Q}$, they have a K_λ-rational point if and only if they have a $\mathbb{Q}_3$-rational point. As an example, we only prove (v). Put $A = p_1p_2p_3$. If $(p_1, p_2, p_3) \equiv (2,2,2)$ or $(5,5,5) \mod 9$, then it sufficient to show that $C_{A, p_1p_2^2}(\mathbb{Q}_3) \neq \emptyset$ and $C_{A,p_1}(\mathbb{Q}_3) = \emptyset$. The curve $C_{A,p_1p_2^2}$ is isomorphic to

$$p_2X^3 + p_1Y^3 = p_3Z^3$$

over $\mathbb{Q}$. Since $p_1 \equiv p_2 \mod 9$, $p_1/p_2 \in \mathbb{Z}_3^*$ is a cube in $\mathbb{Q}_3$ and this has a $\mathbb{Q}_3$-rational point. The curve C_{A,p_1} is isomorphic to

$$X^3 + p_1Y^3 = p_2p_3Z^3$$

over $\mathbb{Q}$. Modulo 9, this equation becomes

$$X^3 + 2Y^3 = 4Z^3 \text{ (resp. } X^3 + 5Y^3 = 7Z^3)$$

if $(p_1, p_2, p_3) \equiv (2,2,2) \mod 9$ (resp. $(5,5,5) \mod 9$). It has no nontrivial solution in $\mathbb{Z}/9\mathbb{Z}$. Therefore C_{A,p_1} has no $\mathbb{Q}_3$-rational points. If $(p_1, p_2, p_3) \equiv (2,5,8) \mod 9$, then it sufficient to show that $C_{A,p_1p_2}(\mathbb{Q}_3) \neq \emptyset$ and $C_{A,p_1}(\mathbb{Q}_3) = \emptyset$. The curve C_{A,p_1p_2} is isomorphic to

$$X^3 + p_1p_2Y^3 = p_3Z^3$$

over $\mathbb{Q}$. Since $p_1p_2 \equiv 1 \mod 9$, this has a $\mathbb{Q}_3$-rational point. The curve C_{A,p_1} is isomorphic to

$$X^3 + p_1Y^3 = p_2p_3Z^3$$

over $\mathbb{Q}$. Modulo 9, this equation becomes

$$X^3 + 2Y^3 = 4Z^3.$$

It has no nontrivial solution in $\mathbb{Z}/9\mathbb{Z}$. Therefore C_{A,p_1} has no $\mathbb{Q}_3$-rational point. □

Remark 2.5. The case $(p_1, p_2, p_3) \equiv (2, 2, 5)$ or $(5, 5, 2) \mod 9$ in Proposition 2.4 (vi) was proved in [Sat, Lemma 2.5] and the case $(p_1, p_2, p_3) \equiv (2, 2, 2)$ or $(5, 5, 5) \mod 9$ in Proposition 2.4 (viii) was proved in [Sat, Lemma 2.6]. On the other hand, none of the cases in the above proposition were proved in [Sat], [BF], and [SD].

Remark 2.6. In particular, if $r \geq 4$ in Proposition 2.4 (ix), the order of $S(A)$ is greater than 9. Indeed, we can easily find at least three generators of $S(A)$.

3. Proof of the main theorem

In this section, by use of the calculation results of the Selmer groups in §2 we construct diagonal cubic surfaces which have a $\mathbb{Q}$-rational point under the assumption that the Tate-Shafarevich group of the elliptic curve E_A is finite (See also Remark 3.3 and Remark 3.5).

Theorem 3.1. *Let V be the diagonal cubic surface over $\mathbb{Q}$ defined by the equation in Table 1 ① below where p_1, p_2, p_3 are rational primes satisfying the condition in Table 1 ② . Assume that the Tate-Shafarevich group of the elliptic curve E_A is finite for A in Table 1 ③. Then $V(\mathbb{Q}) \neq \emptyset$.*

	① V	② $(p_1, p_2, p_3) \mod 9$	③ A
(i)	$p_1X_1^3 + p_2X_2^3 + p_3X_3^3 + p_1p_2p_3X_4^3 = 0$	$(2, 2, 2), (5, 5, 5)$	$p_1p_2p_3$
		$(2, 2, 5), (5, 5, 2)$	$p_1^2p_2^2p_3$
(ii)	$p_1X_1^3 + p_2X_2^3 + p_3X_3^3 + p_2p_3^2X_4^3 = 0$	$(2, 2, 2), (5, 5, 5)$	$p_1p_2p_3$
		$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3^2$
(iii)	$p_1X_1^3 + p_2X_2^3 + p_3X_3^3 + p_2p_3X_4^3 = 0$	$(2, 2, 2), (5, 5, 5)$	$p_1p_2p_3$
		$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3$
(iv)	$p_1X_1^3 + p_2X_2^3 + p_1p_2p_3X_3^3 + p_1p_2p_3^2X_4^3 = 0$	$(2, 2, 5), (5, 5, 2)$	$p_1^2p_2^2p_3$
		$(2, 2, 2), (5, 5, 5)$	$p_1^2p_2^2p_3^2$
(v)	$p_1X_1^3 + p_2X_2^3 + p_2p_3^2X_3^3 + p_1p_2p_3^2X_4^3 = 0$	$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3^2$
		$(2, 2, 2), (5, 5, 5)$	$p_1^2p_2^2p_3^2$
(vi)	$p_1X_1^3 + p_2X_2^3 + p_2p_3X_3^3 + p_1p_2p_3^2X_4^3 = 0$	$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3$
		$(2, 2, 2), (5, 5, 5)$	$p_1^2p_2^2p_3^2$
(vii)	$p_1X_1^3 + p_2X_2^3 + p_3^2X_3^3 + p_2p_3^2X_4^3 = 0$	$(2, 2, 5), (5, 5, 2)$	$p_1p_2p_3^2$
		$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3^2$
(viii)	$p_1X_1^3 + p_2X_2^3 + p_3^2X_3^3 + p_2p_3X_4^3 = 0$	$(2, 2, 5), (5, 5, 2)$	$p_1p_2p_3^2$
		$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3$
(ix)	$p_1X_1^3 + p_2X_2^3 + p_2p_3^2X_3^3 + p_1p_2p_3X_4^3 = 0$	$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3^2$
		$(2, 2, 5), (5, 5, 2)$	$p_1^2p_2^2p_3$
(x)	$p_1X_1^3 + p_2X_2^3 + p_2p_3X_3^3 + p_1p_2p_3X_4^3 = 0$	$(2, 2, 8), (5, 5, 8)$	$p_1p_2^2p_3$
		$(2, 2, 5), (5, 5, 2)$	$p_1^2p_2^2p_3$
(xi)	$p_1X_1^3 + p_2X_2^3 + p_3^2X_3^3 + p_1p_2p_3^2X_4^3 = 0$	$(2, 2, 5), (5, 5, 2)$	$p_1p_2p_3^2$
		$(2, 2, 2), (5, 5, 5)$	$p_1^2p_2^2p_3^2$
(xii)	$p_1X_1^3 + p_2X_2^3 + p_3X_3^3 + p_3^2X_4^3 = 0$	$(2, 2, 2), (5, 5, 5)$	$p_1p_2p_3$
		$(2, 2, 5), (5, 5, 2)$	$p_1p_2p_3^2$

Proof. We can prove by the following way. Note that the surfaces V are of the form

$$V : p_1X_1^3 + p_2X_2^3 + p_1^{i_1}p_2^{i_2}p_3^{i_3}X_3^3 + p_1^{j_1}p_2^{j_2}p_3^{j_3}X_4^3 = 0.$$

Put $A = p_1^{i_1+1}p_2^{i_2+1}p_3^{i_3}$ or $p_1^{j_1+1}p_2^{j_2+1}p_3^{j_3}$ according to the condition of $(p_1, p_2, p_3) \mod 9$ and assume that $Ш(E_A/\mathbb{Q})$ is finite. If $p_1p_2^2 \in S(A)$ and $S(A) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then $C_{A,p_1p_2^2} \cong \{p_1X^3 + p_2Y^3 = p_1^{i_1}p_2^{i_2}p_3^{i_3}Z^3\}$ (resp. $C_{A,p_1p_2^2} \cong \{p_1X^3 + p_2Y^3 = p_1^{j_1}p_2^{j_2}p_3^{j_3}Z^3\}$) has a K-rational point if $A = p_1^{i_1+1}p_2^{i_2+1}p_3^{i_3}$ (resp. $A = p_1^{j_1+1}p_2^{j_2+1}p_3^{j_3}$) by Proposition 2.4 and Lemma 1.3. Thus the surface V clearly has a K-rational point. Then it follows from [Cora, Proposition 2.2] that V has a $\mathbb{Q}$-rational point. As an example, we only prove (i). Note that we may assume that p_1, p_2, p_3 are distinct. If $(p_1, p_2, p_3) \equiv (2, 2, 2)$ or $(5, 5, 5) \mod 9$ (in this case we assume that $Ш(E_{p_1p_2p_3}/\mathbb{Q})$ is finite), then the curve

$$C_{p_1p_2p_3,p_1p_2^2} \cong \{p_1X^3 + p_2Y^3 = p_3Z^3\}$$

has a K-rational point by Proposition 2.4 (v) and Lemma 1.3. If $(p_1, p_2, p_3) \equiv (2, 2, 5)$ or $(5, 5, 2) \mod 9$ (in this case we assume that $Ш(E_{p_1^2p_2^2p_3}/\mathbb{Q})$ is finite), then the curve

$$C_{p_1^2p_2^2p_3,p_1p_2^2} \cong \{p_1X^3 + p_2Y^3 = p_1p_2p_3Z^3\}$$

has a K-rational point by Proposition 2.4 (vii) and Lemma 1.3. Thus V has a $\mathbb{Q}$-rational point. □

Remark 3.2. Theorem 3.1 (xi) was proved in [Sat, Theorem 2.8] and we can apply [SD, Theorem 1 (i)] to Theorem 3.1 (xii). On the other hand, We can check easily that we cannot apply [SD, Theorem 1] to Theorem 3.1 (i) $\sim$ (xi).

Remark 3.3. The surfaces V in Theorem 3.1 have a $\mathbb{Q}_p$-rational point for any rational prime p (without the finiteness assumption of the Tate-Shafarevich group) by the following lemma.

Lemma 3.4. *Let V be a diagonal cubic surface over $\mathbb{Q}$ defined by*

$$V : a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + a_4X_4^3 = 0$$

where $a_1, \ldots, a_4$ are non-zero cube free integers. Assume that if $q \mid a_1a_2a_3a_4$, then $q \equiv 2 \mod 3$ for any rational prime q. Then $V(\mathbb{Q}_p) \neq \emptyset$ for any rational prime p.

Proof. Assume that $p \nmid 3a_1a_2a_3a_4$. Then $V(\mathbb{Q}_p) \neq \emptyset$ by Chevalley-Warning theorem and Hensel's lemma. Assume that $p \mid a_1a_2a_3a_4$. Since $p \equiv 2 \mod 3$, V is isomorphic to

$$p^{i_1}X_1^3 + p^{i_2}X_2^3 + p^{i_3}X_3^3 + p^{i_4}X_4^3 = 0$$

over $\mathbb{Q}_p$ where $i_1, i_2, i_3, i_4 \in \{0, 1, 2\}$. This has a $\mathbb{Q}_p$-rational point. Assume that $p = 3$. Since $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^3$ is generated by the image of 3 and 2 as a group, at least two of the coefficient in $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^3$ are the same. Therefore V has a $\mathbb{Q}_3$-rational point. □

Remark 3.5. For the surfaces V in Theorem 3.1, there is no Brauer-Manin obstruction to the Hasse principle (without the finiteness assumption of the Tate-Shafarevich group). In fact, the surfaces V in Theorem 3.1 (ii), (iii), (vii), (viii) are not birationally equivalent to a plane over $\mathbb{Q}_{p_1}$, the surfaces V in Theorem 3.1 (v), (vi), (ix), (x) are not birationally equivalent to a plane over $\mathbb{Q}_{p_2}$, the surfaces V in Theorem 3.1 (i), (xi) are not birationally equivalent to a plane over $\mathbb{Q}_3$ and the surfaces V in Theorem 3.1 (iv), (xii) are not birationally equivalent to a plane over $\mathbb{Q}_{p_1}$ and $\mathbb{Q}_{p_2}$ by use of [CKS, Lemma 8]. Thus it follows from [CKS, Proposition 2] that there is no Brauer-Manin obstruction to the Hasse principle.

References

[BF] C. L. Basile and T. A. Fisher, Diagonal cubic equations in four variables with prime coefficients, *Rational points on algebraic varieties, Progr. Math.*, Birkhäuser, Basel, **199** (2001) 1–12.

[Coh] H. Cohen, Number theory, Vol. I. Tools and Diophantine equations, Graduate Texts in Mathematics, Springer, New York, **239** (2007).

[Cora] D. F. Coray, Algebraic points on cubic hypersurfaces, *Acta Arith.*, **30** no. 3, (1976) 267–296.

[Corn] Patrick Corn, Del Pezzo surfaces and the Brauer-Manin obstruction, PhD thesis, University of California, Berkeley (2005).

[CKS] Jean-Louis Colliot-Thélène, Dimitri Kanevsky and Jean-Jacques Sansuc, Arithmétique des surfaces cubiques diagonales, Diophantine Approximation and Transcendence Theory (Bonn 1985), Lecture Notes in Math., Springer, Berlin, **1290** (1987) 1–108.

[PV] Bjorn Poonen and José Felipe Voloch, Random Diophantine equations, Arithmetic of higher dimensional algebraic varieties (Palo Alto, CA, 2002), 2004, 175–184. With appendices by Jean-Louis Colliot-Théléne and Nicholas M. Katz.

[Sat] Kazuki Sato, Rational points on diagonal cubic surfaces, *J. Ramanujan Math. Soc.*, **30** no. 3, (2015) 295–308.

[SD] P. Swinnerton-Dyer, The solubility of diagonal cubic surfaces, *Ann. Sci. École Norm. Sup. (4)*, **34** no. 6, (2001) 891–912.

[Sko] A. N. Skorobogatov, Torsors and rational points, Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, **144** (2001).