On the Distribution of Rational Points on Certain Kummer Surfaces *

Atsushi Sato

1 Introduction

We study the distribution of rational points on certain $K3$ surfaces defined over an algebraic number field k of finite degree, namely the Kummer surfaces S/k attached to abelian surfaces A/k which are k-isogenous to $E \times E$, the product of an elliptic curve with itself. (We will also make some minor simplifying assumptions, such as $A[2] \subset A(k)$, and if E has CM, then k contains the CM field.) These are precisely the abelian surfaces which contain infinitely many abelian subvarieties of dimension one. The image of these abelian subvarieties of A in the Kummer surface S gives infinitely many rational curves on S.

Our main results (see Theorems 3.2 and 3.6 for details) describe the height counting function for the rational points on S which lie on the rational curves just described. Our results are compatible with one of the conjectures of Batyrev and Manin, but do not provide a proof of the conjecture because $S(k)$ may contain points not lying on these rational curves.

1.1 Distribution of rational points on a variety

Let k be an algebraic number field of finite degree and V/k a nonsingular projective variety. It is one of the most important problems in number theory to study the set $V(k)$ of k-rational points on V.

*1991 *Mathematics Subject Classification*: Primary 11G35; Secondary 14G25, 14J28.

One can study the structure of $V(k)$, especially the distribution of k-rational points on V, by using height functions in the following way:

Let $h_D : V(\bar{k}) \to \mathbb{R}$ be an absolute logarithmic height function associated with an ample k-rational divisor D on V. We define the counting function $\mathcal{N}(V(k), h_D; T)$ for $T \in \mathbb{R}_+$ by

$$\mathcal{N}(V(k), h_D; T) = \sharp\{P \in V(k) \ ; \ h_D(P) \leq T\}.$$

For varieties V of certain type, one can obtain very important information on $V(k)$ by investigating the asymptotic behavior of $\mathcal{N}(V(k), h_D; T)$ as $T \to \infty$. We quote two classical results.

EXAMPLE 1.1 (Schanuel [Sc]) For the $(n-1)$-dimensional projective space $\mathbb{P}^{n-1}$, we have the following asymptotic formula:

$$\mathcal{N}(\mathbb{P}^{n-1}(k), h_{\mathbb{P}^{n-1}}; T) = ce^{ndT} + \begin{cases} O(Te^T) & \text{if } \ n = 2, \ d = 1, \\ O(e^{(nd-1)T}) & \text{otherwise,} \end{cases} \quad \text{as } T \to \infty,$$

where $h_{\mathbb{P}^{n-1}} : \mathbb{P}^{n-1}(\bar{k}) \to \mathbb{R}$ denotes the standard *absolute logarithmic height function* on $\mathbb{P}^{n-1}$, which is a height function associated with a hyperplane H, d denotes the degree of k, and c is a positive number which can be expressed in terms of the class number of k, special values of the Dedekind zeta function of k, etc.

EXAMPLE 1.2 (Néron [N]) For an abelian variety A/k, we have the following asymptotic formula:

$$\mathcal{N}(A(k), h_D; T) = cT^{r/2} + O(T^{(r-1)/2}) \quad \text{as } T \to \infty,$$

where r denotes the rank of the Mordell-Weil group $A(k)$ and c is a positive number which depends on the algebraic equivalence class of D. This is a consequence of the Mordell-Weil Theorem and the theory of the canonical height functions.

REMARK 1.3 We can show a similar formula to Example 1.2 for a variety which has an abelian variety as an unramified covering, say a hyperelliptic surface (see [MS]).

We note that these formulas have the form "main term + error term", and that the growth order and the leading coefficient c of the main term are closely related to geometric invariants of V and arithmetic invariants of k.

In view of these results, an optimist might have a dream that, for *any* variety V, investigating the asymptotic behavior of the counting function $\mathcal{N}(V(k), h_D; T)$ as $T \to \infty$ presents something which is related to geometric invariants of V and arithmetic invariants of k.

However, after a short study on some other varieties, we have to realize that the dream is just a dream. For example, let A/k be an abelian surface and $V \to A$ the blow-up of a k-rational point on A. For such a variety V, we cannot expect that investigating the asymptotic behavior of $\mathcal{N}(V(k), h_D; T)$ would work for studying the geometry of V. Indeed, Example 1.1 combined with Example 1.2 tells us that the counting function presents the information only on the exceptional curve. In other words, the exceptional curve has too many rational points than its complement does. We cannot view the whole shape of V through the counting function without removing the exceptional curve.

It sometimes happens that rational points on a variety concentrate on closed subvarieties of lower dimension. Accordingly, studying the distribution of rational points on a variety V/k, we have to investigate the asymptotic behavior of the counting function $\mathcal{N}(U(k), h_D; T)$ for a suitable non-empty Zariski open subset U/k of V.

1.2 A conjecture of Batyrev and Manin

Recently, Batyrev and Manin [BM] introduced geometric and arithmetic invariants for ample divisors on a variety, and described a conjecture about their relation (cf. also, [Mo] and [S3]).

Let k be an algebraic number field of finite degree and V/k a nonsingular projective variety. Let $NS(V)$ denote the Néron-Severi group of V, and let $N^1_{\mathrm{eff}}(V)$ be the closed cone in $NS(V) \otimes_{\mathbb{Z}} \mathbb{R}$ generated by effective divisors on V.

For an ample k-rational divisor D on V, we define a *geometric invariant* $\alpha(D) \in \mathbb{R}$ of D by

$$\alpha(D) = \inf\{\gamma \in \mathbb{R} \ ; \ D \otimes \gamma + K_V \otimes 1 \in N^1_{\mathrm{eff}}(V)\},$$

where K_V is a canonical divisor on V. For an ample k-rational divisor D on V and a non-empty Zariski open subset U/k of V, we define an *arithmetic invariant* $\beta_U(D) \in \mathbb{R} \cup \{-\infty\}$

of D and U by

$$\beta_U(D) = \frac{1}{[k:\mathbb{Q}]} \inf\Big\{ s \in \mathbb{R} \ ; \ \sum_{P \in U(k)} H_D(P)^{-s} < \infty \Big\},$$

where $H_D : V(\bar{k}) \to \mathbb{R}_+$ is an *absolute exponential height function* associated with D. Since the height function H_D is defined up to multiplying by bounded functions, $\beta_U(D)$ does not depend on the choice of H_D. It is easy to see that $\alpha(D)$ and $\beta_U(D)$ depend only on the algebraic equivalence class of D, and that

$$\alpha(mD) = \frac{1}{m}\,\alpha(D) \quad \text{and} \quad \beta_U(mD) = \frac{1}{m}\,\beta_U(D)$$

for $m \in \mathbb{Z}_+$.

Remark 1.4 (i) It is known that the signature of $\alpha(D)$ and $\beta_U(D)$ are independent of the choice of D.

(ii) One easily observes that either $\beta_U(D) = -\infty$ or $\beta_U(D) \geq 0$. The former case holds if and only if $U(k)$ is a finite set. In the latter case, $\beta_U(D)$ can be expressed with the counting function as follows:

$$\beta_U(D) = \frac{1}{[k:\mathbb{Q}]} \inf\{\delta \in \mathbb{R}_+ \ ; \ \mathcal{N}(U(k), h_D; T) \ll e^{\delta T} \text{ as } T \to \infty\}.$$

Conjecture 1.5 (Batyrev-Manin [BM]) *For any $\varepsilon > 0$, there is a non-empty Zariski open subset U/k of V such that*

$$\beta_U(D) \leq \alpha(D) + \varepsilon.$$

We have $\alpha(H) = \beta_{\mathbb{P}^{n-1}}(H) = n$ in Example 1.1, and $\alpha(D) = \beta_A(D) = 0$ in Example 1.2. Thus the conjecture holds for these varieties. We note that, in the case $\alpha(D) \leq 0$, the conjecture for a field k immediately implies the conjecture for any subfield of k.

Example 1.6 If $V = C$ is a curve of genus g, we easily see

$$\alpha(D) = \frac{2-2g}{\deg D}$$

for an ample divisor D on C. Thus we have:

(i) $\alpha(D) > 0$ if $g = 0$.

(ii) $\alpha(D) = 0$ if $g = 1$.

(iii) $\alpha(D) < 0$ if $g \geq 2$.

Note that the conjecture for the case $g \geq 2$ is nothing but the Mordell-Faltings Theorem.

EXAMPLE 1.7 (Morita [Mo]) If $V = S$ is a surface, then the Kodaira dimension $\kappa(S)$ and the geometric invariant $\alpha(D)$ satisfy the following:

(i) $\alpha(D) > 0$ if $\kappa(S) = -\infty$.

(ii) $\alpha(D) = 0$ if $\kappa(S) = 0$ or 1.

(iii) $\alpha(D) < 0$ if $\kappa(S) = 2$.

Let S/k be a nonsingular projective surface without (-1)-curves and of Kodaira dimension zero. For such a surface S, Conjecture 1.5 asserts: *For any $\varepsilon > 0$, there exists a non-empty Zariski open subset U/k of S such that $\beta_U(D) \leq \varepsilon$.*

In cases where S is an abelian surface or a hyperelliptic surface, we have $\beta_S(D) = 0$ (see Example 1.2 and Remark 1.3). Moreover, it is known that the conjecture for Enriques surfaces can be reduced to the conjecture for $K3$ surfaces (cf. [Mo]).

If there exists a rational curve (i.e., a curve of genus zero with a rational point) L/k lying on S, one easily observes that there exists a positive constant δ such that

$$\mathcal{N}(L(k), h_D; T) \gg e^{\delta T} \quad \text{as } T \to \infty$$

(cf. Proposition 3.4). Therefore, if there exist infinitely many rational curves L/k lying on S and if the conjecture for S holds, we must take the subvariety U again and again infinitely many times as ε tends to zero. Thus, we have to estimate the distribution of rational points on such rational curves in order to show the conjecture for S.

In the past several years, rational points on certain classes of $K3$ surfaces have been studied in a number of papers. In 1991, Silverman [S2] constructed the canonical height functions with respect to certain automorphisms of a $K3$ surface and applied them to study the distribution of rational points (see also [CS1]). This work has been generalized and studied precisely in [Ba], [Bi], [CS2] and in [W]. Some of these papers showed that their results are compatible with Conjecture 1.5, but did not provide the proof of

the conjecture. It seems that studying rational points on $K3$ surfaces is still difficult. However, for the class of $K3$ surfaces called *Kummer surfaces*, one can say a bit by applying the theory of abelian varieties (cf., e.g., [S1, Example 4.4]).

ACKNOWLEDGEMENTS The author would like to express his thanks to Professor Yasuo Morita for wonderful suggestions.

2 Notation and definitions

Let k be an algebraic number field of finite degree, A/k an abelian surface, and let S be the Kummer surface of A. Then we have the following commutative diagram:

$$\begin{array}{ccc} \hat{A} & & \\ {\scriptstyle\rho}\downarrow & \searrow^{\pi} & \\ A & \overset{\varpi}{\dashrightarrow} & S, \end{array}$$

where $\rho : \hat{A} \to A$ denotes the blow-up of the sixteen points $A[2]$ of order two on A and $\pi : \hat{A} \to S$ the natural projection. Let $\tilde{A}$ denote the open subvariety $A - A[2]/k$ of A, on which the rational map ϖ is regular. For each $Q \in A[2]$, we have a (-1)-curve $\rho^{-1}(Q)/\bar{k}$ lying on $\hat{A}$, which provides a rational curve (defined over $\bar{k}$) lying on S. We denote by L_Q the rational curve and by $\tilde{S}$ the open subvariety $S - \bigcup_{Q \in A[2]} L_Q/k$ of S. Then we have

$$\varpi^{-1}(\tilde{S}(k)) = A\langle k \rangle \cap \tilde{A}(\bar{k}),$$

where $A\langle k \rangle$ denotes the set of points P on A that $\{P, -P\}$ is stable under the action of $\mathrm{Gal}(\bar{k}/k)$:

$$A\langle k \rangle = \{P \in A(\bar{k}) \ ; \ \{P, -P\} \text{ is } \mathrm{Gal}(\bar{k}/k)\text{-stable}\}.$$

REMARK 2.1 (i) For $P \in A\langle k \rangle$, one of the following holds:

(a) P is defined over k.

(b) P is defined over a quadratic extension K/k and satisfies $P^{\sigma(K)} = -P$.

Here $\sigma(K)$ denotes the generator of $\mathrm{Gal}(K/k)$. Thus we have

$$A\langle k \rangle = A(k) \cup \bigcup_{[K:k]=2} \{P \in A(K) \ ; \ P^{\sigma(K)} = -P\}.$$

(ii) Each set $\{P \in A(K)\ ;\ P^{\sigma(K)} = -P\}$ can be identified with the set of k-rational points on the twist of A with respect to the 1-cocycle

$$\mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(A), \qquad \sigma \longmapsto \begin{cases} 1 & \text{if } \sigma|_K = 1, \\ [-1] & \text{if } \sigma|_K = \sigma(K). \end{cases}$$

We note that the sets $A(k)$ and $\{P \in A(K)\ ;\ P^{\sigma(K)} = -P\}$ are *almost disjoint*. More precisely, we have

$$A(k) \cap \{P \in A(K)\ ;\ P^{\sigma(K)} = -P\} \subset A[2]$$

and

$$\{P \in A(K)\ ;\ P^{\sigma(K)} = -P\} \cap \{P \in A(K')\ ;\ P^{\sigma(K')} = -P\} \subset A[2]$$

for distinct quadratic extensions K and K' of k.

(iii) We can describe the distribution of k-rational points on A and on each twist of A. However, that does not help us to study the set $A\langle k\rangle$, for k has infinitely many quadratic extensions.

Suppose that there exists an elliptic curve (i.e., a one-dimensional abelian subvariety) $C/\bar{k}$ lying on A. Then, for each $Q \in A[2]$, the curve $\tau_Q(C)/\bar{k}$ lying on A is stable under $[-1] \in \mathrm{Aut}(A)$, and hence it provides a rational curve (defined over $\bar{k}$) lying on S. Here τ_Q denotes the translation-by-Q map on A. We denote by $L_{Q,C}$ the rational curve.

Let $\mathcal{C}$ denote the set of all elliptic curves (defined over $\bar{k}$) on A, and $\mathcal{L}$ the set of rational curves on S obtained as described above. For each $L \in \mathcal{L}$, we denote the open subvariety $L \cap \tilde{S}$ of L by $\tilde{L}$. Note that the surjection

$$A[2] \times \mathcal{C} \longrightarrow \mathcal{L}, \qquad (Q, C) \longmapsto L_{Q,C}$$

gives four-to-one correspondence between $A[2] \times \mathcal{C}$ and $\mathcal{L}$. More precisely, one easily shows:

LEMMA 2.2 *For (Q, C), $(Q', C') \in A[2] \times \mathcal{C}$, the following conditions are equivalent*:
(a) $L_{Q,C} = L_{Q',C'}$.
(b) $C = C'$ *and* $Q \equiv Q' \pmod{C[2]}$.

For a projective variety V/k, a "height" function $h : V(\bar{k}) \to \mathbb{R}$ and a subset $\mathcal{V} \subset V(\bar{k})$, we define two counting functions $\mathcal{N}(\mathcal{V}, h; T)$ and $\mathcal{N}_+(\mathcal{V}, h; T)$ of $T \in \mathbb{R}_+$ by

$$\mathcal{N}(\mathcal{V}, h; T) = \sharp\{P \in \mathcal{V} \ ; \ h(P) \leq T\},$$
$$\mathcal{N}_+(\mathcal{V}, h; T) = \sharp\{P \in \mathcal{V} \ ; \ 0 < h(P) \leq T\}.$$

3 Main results

The purpose of this paper is to study the distribution of rational points on rational curves $L \in \mathcal{L}$ in the case where the set $\mathcal{L}$ consists of *infinitely many* rational curves. This condition, $\sharp\mathcal{L} = \infty$, is equivalent to the following (see Proposition 4.1):

(C0) *The endomorphism algebra* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is isomorphic to* $\mathrm{M}_2(F)$ *over a field* F.

We note that the field F in (C0) is isomorphic to the field $\mathbb{Q}$ of rational numbers or an imaginary quadratic field.

Until the end of this section, we assume the condition (C0). Then there exists an elliptic curve $E/\bar{k}$ satisfying the following two conditions (see Remark 4.2):

(i) A is isogenous to $E \times E$ (over $\bar{k}$).

(ii) $\mathrm{End}(E)$ is isomorphic to the maximal order R of F.

We fix such an elliptic curve E and an isogeny $\phi : A \to E \times E$. Then the map $C \mapsto \phi(C)$ gives one-to-one correspondence between $\mathcal{C}$ and the set of all elliptic curves lying on $E \times E$, and its inverse is given by $E' \mapsto \hat{\phi}(E')$, where $\hat{\phi} : E \times E \to A$ denotes the dual isogeny of ϕ.

We shall partially order the elliptic curves lying on $E \times E$ (or the elliptic curves lying on A) according to their degrees, and study the asymptotic behavior of the number of elliptic curves $C \in \mathcal{C}$ of bounded degrees (cf. [K, Corollary 1.3]). We fix $\{O\} \times E + E \times \{O\}$ as an ample divisor on $E \times E$ and define the *degree* of E' (with respect to $\{O\} \times E + E \times \{O\}$) by

$$\deg E' = E'.(\{O\} \times E + E \times \{O\})$$

for elliptic curves E' lying on $E \times E$. Then we obtain the following asymptotic formula which will be shown in Section 4.2:

PROPOSITION 3.1 *We have*

$$\sharp\{C \in \mathcal{C} \ ; \ \deg \phi(C) \leq T\} \ll T^{[F:\mathbb{Q}]} \quad \text{as } T \to \infty.$$

For simplicity, we assume that the field k is sufficiently large so that the following conditions are satisfied:

(C1) *Every two-torsion point on A is k-rational.*

(C2) *The elliptic curve E is defined over k.*

(C3) *Any element of* $\mathrm{End}(E)$ *is defined over k.*

(C4) *The isogeny $\phi : A \to E \times E$ is defined over k.*

Then each $L \in \mathcal{L}$ is defined over k (see Proposition 4.9, (iii)). Moreover, the rational curves $L \in \mathcal{L}$ are *almost disjoint*. More precisely, we have

$$\varpi^{-1}(\tilde{L}(k) \cap \tilde{L}'(k)) \subset A\langle k \rangle \cap A(\bar{k})_{\mathrm{tor}}$$

if $L \neq L'$ (see Remark 4.11). Note that the set $A\langle k \rangle \cap A(\bar{k})_{\mathrm{tor}}$ is finite (cf. Remark 2.1).

Let D be an ample k-rational divisor on S, and let $h_D : S(\bar{k}) \to \mathbb{R}$ (resp. $H_D : S(\bar{k}) \to \mathbb{R}_+$) be an absolute logarithmic (resp. exponential) height function associated with D. To state the main results, we need three positive constants m_0, c_0, c_0'. We will give their definitions later (see Lemma 4.7 and Lemma 5.1, (i)), and just mention their dependencies for the present. The constant m_0 is an analogue of the class number of F and depends only on F, while the constants c_0 and c_0' are used to compare two different height functions on $\tilde{A}$ and depend on the choice of E, ϕ and D.

The following theorem, which will be shown in Section 5.2, shows that the distribution of rational points on $\bigcup_{L \in \mathcal{L}} L$ is compatible with Conjecture 1.5:

THEOREM 3.2 *For each $M > 0$, we define a finite subset $\mathcal{L}_M \subset \mathcal{L}$ by*

$$\mathcal{L}_M = \{L_{Q,C} \ ; \ Q \in A[2], \ C \in \mathcal{C}, \ \deg \phi(C) \leq M\}.$$

Then

$$\mathcal{N}((\mathcal{L} - \mathcal{L}_M)[k], h_D; T) \ll T^{[F:\mathbb{Q}]} \exp\Big(\frac{4[k:\mathbb{Q}]m_0c_0}{M}\, T\Big) \quad \text{uniformly in } M \text{ as } T \to \infty,$$

where

$$(\mathcal{L}-\mathcal{L}_M)[k]=\bigcup_{L\in\mathcal{L}-\mathcal{L}_M}\tilde{L}(k).$$

COROLLARY 3.3 *The Dirichlet series*

$$\sum_{P\in(\mathcal{L}-\mathcal{L}_M)[k]}H_D(P)^{-s}$$

converges for $s>4[k:\mathbb{Q}]m_0c_0/M$.

In a similar fashion to the proof of Theorem 3.2, we can prove:

PROPOSITION 3.4 *For each* $(Q,C)\in A[2]\times\mathcal{C}$, *we have*

$$\mathcal{N}(L_{Q,C}(k),h_D;T)\gg\exp\Big(\frac{4[k:\mathbb{Q}]}{m_0c_0'\deg\phi(C)}\,T\Big)\quad\textit{uniformly in }(Q,C)\textit{ as }T\to\infty.$$

COROLLARY 3.5 *The Dirichlet series*

$$\sum_{P\in L_{Q,C}(k)}H_D(P)^{-s}$$

diverges for $0<s\le 4[k:\mathbb{Q}]/(m_0c_0'\deg\phi(C))$.

From Theorem 3.2 and Proposition 3.4, we conclude:

THEOREM 3.6 *For each* $M>0$, *take* $N>M$ *sufficiently large so that*

$$\{C\in\mathcal{C}\ ;\ M<\deg\phi(C)<N/(m_0^2c_0c_0')\}\neq\emptyset.$$

Then

$$\mathcal{N}((\mathcal{L}-\mathcal{L}_M)[k],h_D;T)\sim\mathcal{N}((\mathcal{L}_N-\mathcal{L}_M)[k],h_D;T)\quad\textit{as }T\to\infty,$$

where

$$(\mathcal{L}_N-\mathcal{L}_M)[k]=\bigcup_{L\in\mathcal{L}_N-\mathcal{L}_M}\tilde{L}(k).$$

From the last theorem, we see that, for *any* subset $\mathcal{L}'\subset\mathcal{L}$, almost all rational points on $\bigcup_{L\in\mathcal{L}'}L$ concentrate on finitely many rational curves $L\in\mathcal{L}'$ of lower degree (note that $\mathcal{L}_N-\mathcal{L}_M$ consists of finitely many rational curves).

Although $\bigcup_{L\in\mathcal{L}} L$ is a dense subset of S, the set $\bigcup_{L\in\mathcal{L}} L(k)$ of rational points might be tiny as compared with $S(k)$. Therefore we have not proved Conjecture 1.5 for S. However, we have seen that $\bigcup_{L\in\mathcal{L}} L$ has a large amount of rational points at the same time. Theorem 3.6 suggests: *Whatever non-empty Zariski open subset U/k of S we take, the counting function $\mathcal{N}(U(k), h_D; T)$ will not be able to describe the whole shape of S.* Thus, we cannot expect an asymptotic formula for S as in Examples 1.1 or 1.2. It seems that these results present an evidence of difficulty inherent in the study of the distribution of rational points on a $K3$ surface.

4 Elliptic curves lying on abelian surfaces

In this section, we study the set $\mathcal{C}$ in a different way from [K] and give the proof of Proposition 3.1. Until the end of Section 4.2, *all varieties and morphisms are assumed to be defined over $\bar{k}$.*

4.1 Elliptic curves lying on A

First, we show that the condition (C0) in Section 3 can be rephrased in terms of the endomorphism algebra of A as follows:

PROPOSITION 4.1 *The set $\mathcal{C}$ consists of infinitely many elliptic curves if and only if the endomorphism algebra* $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ *is isomorphic to the total matrix algebra* $\mathrm{M}_2(F)$ *over a field F.*

PROOF For an abelian surface A, one (and the only one) of the following holds (cf., e.g., [Mi, Proposition 12.1]):

(a) A is simple.

(b) A is isogenous to $E_1\times E_2$ for non-isogenous two elliptic curves E_1 and E_2.

(c) A is isogenous to $E\times E$ for an elliptic curve E.

Moreover, each of these conditions implies the following, respectively:

(a)* $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ is a skew field.

(b)* $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ is isomorphic to $(\mathrm{End}(E_1)\otimes_{\mathbb{Z}}\mathbb{Q})\oplus(\mathrm{End}(E_2)\otimes_{\mathbb{Z}}\mathbb{Q})$.

(c)* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to $\mathrm{M}_2(\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q})$.

In case (a) or (b), one easily shows that the set $\mathcal{C}$ consists of finitely many elliptic curves:

$$\sharp\mathcal{C} = \begin{cases} 0 & \text{in case (a),} \\ 2 & \text{in case (b).} \end{cases}$$

In case (c), the set $\mathcal{C}$ consists of infinitely many elliptic curves as we will observe below. □

REMARK 4.2 In case (c) in the proof above, we can take the elliptic curve E so that $\mathrm{End}(E)$ is isomorphic to the maximal order of F.

In the rest of this section, we assume the condition (C0), and we fix an elliptic curve E satisfying the following two conditions:

(i) A is isogenous to $E \times E$.

(ii) $\mathrm{End}(E)$ is isomorphic to the maximal order R of F.

Moreover, we fix an isogeny $\phi : A \to E \times E$.

4.2 Elliptic curves lying on $E \times E$

Let p (resp. q) denote the first (resp. the second) projection from $E \times E$ to E, and we fix a ring isomorphism

$$[\,\cdot\,] : R \longrightarrow \mathrm{End}(E), \qquad \alpha \longmapsto [\alpha].$$

Then each $(\alpha, \beta) \in R^2 - \{(0,0)\}$ induces a morphism

$$E \longrightarrow E \times E, \qquad P \longmapsto ([\alpha]P,\ [\beta]P),$$

which gives an isogeny $\psi_{\alpha,\beta}$ from E to an elliptic curve $E_{\alpha,\beta}$ lying on $E \times E$.

REMARK 4.3 If F is an imaginary quadratic field (i.e., E has complex multiplication), then $\mathrm{Ker}\,\psi_{\alpha,\beta}$ is isomorphic to $\mathfrak{m}_{\alpha,\beta}^{-1}/R$ and hence $\deg \psi_{\alpha,\beta} = N\mathfrak{m}_{\alpha,\beta}$ holds. Here, $\mathfrak{m}_{\alpha,\beta}$ denotes the (integral) ideal in F generated by α and β, and $N\mathfrak{m}_{\alpha,\beta}$ its norm.

LEMMA 4.4 *For* $(\alpha, \beta),\ (\alpha', \beta') \in R^2 - \{(0,0)\}$, *we have*:

(i) $E_{\alpha,\beta} = E_{\alpha',\beta'}$ *if* $\alpha\beta' = \alpha'\beta$.

(ii) $E_{\alpha,\beta} \cap E_{\alpha',\beta'} \subset (E \times E)_{\mathrm{tor}}$, *therefore* $E_{\alpha,\beta} \neq E_{\alpha',\beta'}$ *if* $\alpha\beta' \neq \alpha'\beta$.

PROOF (i) Clear.

(ii) Suppose that

$$([\alpha]P,\ [\beta]P) = ([\alpha']P',\ [\beta']P')$$

for some $P, P' \in E(\bar{k})$. Then

$$[\alpha\beta' - \alpha'\beta]P = [\alpha\beta' - \alpha'\beta]P' = O,$$

which implies $P, P' \in E_{\mathrm{tor}}$. □

The proof of Proposition 4.1 is completed by the following proposition and corollary:

PROPOSITION 4.5 *The map* $(\alpha, \beta) \mapsto E_{\alpha,\beta}$ *induces one-to-one correspondence between the set* $\mathbb{P}^1(F)$ *of* F*-rational points on the projective line and the set of all elliptic curves lying on* $E \times E$.

COROLLARY 4.6 *There exists one-to-one correspondence between* $\mathbb{P}^1(F)$ *and* $\mathcal{C}$.

PROOF OF PROPOSITION 4.5 It suffices to show that any elliptic curve lying on $E \times E$ can be expressed as $E_{\alpha,\beta}$ for some $(\alpha, \beta) \in R^2 - \{(0,0)\}$. Let E' be such an elliptic curve. Then $p|_{E'}$ and $q|_{E'}$ are morphisms of abelian varieties from E' to E. Since either $p|_{E'} \neq 0$ or $q|_{E'} \neq 0$ holds, E' must be isogenous to E. By taking an isogeny $\lambda : E \to E'$, we have $E' = E_{\alpha,\beta}$ for $[\alpha] = p|_{E'} \circ \lambda,\ [\beta] = q|_{E'} \circ \lambda \in \mathrm{End}(E)$. □

Before giving the proof of Proposition 3.1, we show the following lemma:

LEMMA 4.7 *There exists a positive constant* m_0 *for which the following holds*: *Any element of* $\mathbb{P}^1(F)$ *can be represented by some* $(\alpha, \beta) \in R^2 - \{(0,0)\}$ *satisfying* $\deg \psi_{\alpha,\beta} \leq m_0$.

REMARK 4.8 If F is of class number one, the lemma above clearly holds for $m_0 = 1$.

PROOF OF LEMMA 4.7 It suffices to show the lemma in the case where F is an imaginary quadratic field of class number greater than one. Let $\mathfrak{m}^{(1)}, \dots, \mathfrak{m}^{(h)}$ be integral ideals in F so that any ideal class of F is represented by one of these, and we fix a nonzero integer $\mu \in \bigcap_{i=1}^{h} \mathfrak{m}^{(i)}$.

For any $(\alpha', \beta') \in F^2 - \{(0,0)\}$, there exists $\gamma \in F^\times$ such that $\mathfrak{m}_{\alpha',\beta'}^{-1} = \gamma \mathfrak{m}^{(i)}$ for some i. By putting $\alpha = \gamma\mu\alpha'$ and $\beta = \gamma\mu\beta'$, we have $(\alpha, \beta) \in R^2 - \{(0,0)\}$, $\alpha\beta' = \alpha'\beta$ and

$$N\mathfrak{m}_{\alpha,\beta} = N(\gamma\mu\mathfrak{m}_{\alpha',\beta'}) = \frac{|N_{F/\mathbb{Q}}(\mu)|}{N\mathfrak{m}^{(i)}}.$$

Hence the inequality holds for $m_0 = |N_{F/\mathbb{Q}}(\mu)|$ (cf. Remark 4.3). □

PROOF OF PROPOSITION 3.1 For any $(\alpha, \beta) \in R^2 - \{(0,0)\}$, the degree (with respect to $\{O\} \times E + E \times \{O\} = E_{0,1} + E_{1,0}$) of $E_{\alpha,\beta}$ can be expressed as

$$\deg E_{\alpha,\beta} = \frac{\deg[\alpha] + \deg[\beta]}{\deg \psi_{\alpha,\beta}}.$$

Hence it follows from Proposition 4.5 and Lemma 4.7 that

$$\sharp\{C \in \mathcal{C} \ ; \ \deg \phi(C) \le T\} \le \sharp\{(\alpha, \beta) \in R^2 \ ; \ \deg[\alpha] + \deg[\beta] \le m_0 T\}.$$

On the other hand, one easily shows that

$$\sharp\{(\alpha, \beta) \in R^2 \ ; \ \deg[\alpha] + \deg[\beta] \le m_0 T\} \asymp T^{[F:\mathbb{Q}]} \quad \text{as } T \to \infty.$$

Hence we obtain the desired asymptotic formula. □

4.3 Some remarks on k-rationality

Now we assume the conditions (C1)–(C4) of Section 3. These conditions imply:

PROPOSITION 4.9 (i) *For any $(\alpha, \beta) \in R^2 - \{(0,0)\}$, the elliptic curve $E_{\alpha,\beta}$, the isogeny $\psi_{\alpha,\beta} : E \to E_{\alpha,\beta}$ and its dual isogeny $\hat{\psi}_{\alpha,\beta} : E_{\alpha,\beta} \to E$ are defined over k. Therefore any elliptic curve lying on $E \times E$ is defined over k.*

(ii) *The dual isogeny $\hat{\phi} : E \times E \to A$ of ϕ is defined over k. Therefore any $C \in \mathcal{C}$ is defined over k.*

(iii) *For any $(Q, C) \in A[2] \times \mathcal{C}$, the rational curve $L_{Q,C}$ is defined over k. Therefore any $L \in \mathcal{L}$ is defined over k.*

Since the elliptic curve E is defined over k, we can define $E\langle k\rangle$ in the same fashion as $A\langle k\rangle$. We can also define $E_{\alpha,\beta}\langle k\rangle$ and $C\langle k\rangle$ because of the proposition above.

COROLLARY 4.10 (i) *For any* $(\alpha,\beta)\in R^2-\{(0,0)\}$, *we have*

$$\psi_{\alpha,\beta}(E\langle k\rangle)\subset E_{\alpha,\beta}\langle k\rangle,\qquad \hat{\psi}_{\alpha,\beta}(E_{\alpha,\beta}\langle k\rangle)\subset E\langle k\rangle.$$

(ii) *For any* $C\in\mathcal{C}$, *we have*

$$\phi(C\langle k\rangle)\subset\phi(C)\langle k\rangle,\qquad \hat{\phi}(\phi(C)\langle k\rangle)\subset C\langle k\rangle.$$

(iii) *For any* $(Q,C)\in A[2]\times\mathcal{C}$, *we have*

$$\varpi^{-1}(\tilde{L}_{Q,C}(k))=\tau_Q(C\langle k\rangle)\cap\tilde{A}(\bar{k}).$$

REMARK 4.11 We recall that the rational curves $L\in\mathcal{L}$ are *almost disjoint*. More precisely, we have

$$\varpi^{-1}(\tilde{L}_{Q,C}(k)\cap\tilde{L}_{Q',C'}(k))\subset\tau_Q(C\langle k\rangle)\cap\tau_{Q'}(C'\langle k\rangle)\subset A\langle k\rangle\cap A(\bar{k})_{\mathrm{tor}}$$

if $L_{Q,C}\neq L_{Q',C'}$ (cf. Lemma 2.2 and Lemma 4.4, (ii)).

5 Number of rational points of bounded heights

In this section, we give the proof of Theorem 3.2. Notation and assumptions are the same as in Section 3.

5.1 Reduction of the problem

Let d_0 denote the degree of the isogeny $\phi: A\to E\times E$. For convenience, we fix the canonical absolute logarithmic height functions on E, $E\times E$ and on A as follows:

$$\begin{aligned}
\hat{h}_E &: E(\bar{k})\to\mathbb{R} && \text{the height associated with } (O),\\
\hat{h}_{E\times E} &: (E\times E)(\bar{k})\to\mathbb{R} && \text{the height associated with } E_{0,1}+E_{1,0},\\
\hat{h}_A &: A(\bar{k})\to\mathbb{R} && \text{the height associated with } \hat{\phi}(E_{0,1})+\hat{\phi}(E_{1,0}).
\end{aligned}$$

We recall that (O), $E_{0,1}+E_{1,0}$ and $\hat{\phi}(E_{0,1})+\hat{\phi}(E_{1,0})$ are ample (and even) k-rational divisors on E, $E\times E$ and on A, respectively.

LEMMA 5.1 (i) *There exist positive constants* c_0, c_1, c_0', c_1' *such that*

$$d_0\hat{h}_A \leq c_0 h_D \circ \varpi + c_1 \quad \textit{on } \tilde{A}(\bar{k})$$

and

$$d_0 h_D \circ \varpi \leq c_0'\hat{h}_A + c_1' \quad \textit{on } \tilde{A}(\bar{k}).$$

(ii) *We have*

$$d_0\hat{h}_A = \hat{h}_{E\times E} \circ \phi \quad \textit{on } A(\bar{k}).$$

(iii) *For each* $(\alpha, \beta) \in R^2 - \{(0,0)\}$, *we have*

$$\hat{h}_{E\times E} = \frac{\deg E_{\alpha,\beta}}{\deg \psi_{\alpha,\beta}}\, \hat{h}_E \circ \hat{\psi}_{\alpha,\beta} \quad \textit{on } E_{\alpha,\beta}(\bar{k}).$$

PROOF (i) Since the natural projection $\pi : \hat{A} \to S$ is finite and surjective, the pull-back π^*D is an ample divisor on $\hat{A}$. Let $h_{\pi^*D} : \hat{A}(\bar{k}) \to \mathbb{R}$ be an absolute logarithmic height function associated with π^*D. Then

$$h_{\pi^*D} = h_D \circ \pi + O(1) \quad \text{on } \hat{A}(\bar{k})$$

(see, e.g., [L, Chapter 4, Theorem 5.1]). On the one hand, there exist positive constants c_0 and c_0' such that

$$d_0\hat{h}_A \circ \rho \leq c_0 h_{\pi^*D} + O(1) \quad \text{on } \Big(\hat{A} - \bigcup_{Q\in A[2]} \rho^{-1}(Q)\Big)(\bar{k})$$

and

$$d_0 h_{\pi^*D} \leq c_0'\hat{h}_A \circ \rho + O(1) \quad \text{on } \Big(\hat{A} - \bigcup_{Q\in A[2]} \rho^{-1}(Q)\Big)(\bar{k})$$

(see, e.g., [L, Chapter 4, Propositions 1.7 and 5.4]). Hence we obtain the assertion.

(ii) Immediate from

$$\phi^*(E_{0,1} + E_{1,0}) = d_0(\hat{\phi}(E_{0,1}) + \hat{\phi}(E_{1,0}))$$

(see, e.g., [L, Chapter 5, Proposition 3.3]).

(iii) Since the pull-back of $E_{0,1} + E_{1,0}$ by the morphism

$$E \longrightarrow E \times E, \qquad P \longmapsto ([\alpha]P,\ [\beta]P)$$

is algebraically equivalent to $(\deg[\alpha]+\deg[\beta])(O)$, we have

$$\hat{h}_{E\times E}\circ\psi_{\alpha,\beta}=(\deg[\alpha]+\deg[\beta])\hat{h}_E \quad \text{on } E(\bar{k}),$$

which implies the desired equality. □

LEMMA 5.2 (i) *Let c_0 and c_1 be the positive constants as in Lemma* 5.1. *For a subset $\mathcal{C}'\subset\mathcal{C}$, define a subset $\mathcal{L}'\subset\mathcal{L}$ by $\mathcal{L}'=\{L_{Q,C}\ ;\ Q\in A[2],\ C\in\mathcal{C}'\}$. Then*

$$\mathcal{N}\Big(\bigcup_{L\in\mathcal{L}'}\tilde{L}(k),h_D;T\Big)\le 2\sum_{C\in\mathcal{C}'}\mathcal{N}_+\Big(C\langle k\rangle,\hat{h}_A;\frac{c_0T+c_1}{d_0}\Big)+\frac{1}{2}\sharp(A\langle k\rangle\cap A(\bar{k})_{\rm tor}).$$

(ii) *Let m_0 be the positive constant as in Lemma* 4.7. *Then, for each $C\in\mathcal{C}$, we have*

$$\mathcal{N}_+(C\langle k\rangle,\hat{h}_A;T)\le m_0d_0\,\mathcal{N}_+\Big(E\langle k\rangle,\hat{h}_E;\frac{m_0d_0}{\deg\phi(C)}\,T\Big).$$

PROOF (i) It follows from Lemma 2.2, Corollary 4.10, (iii) and Lemma 5.1, (i) that

$$\mathcal{N}\Big(\bigcup_{L\in\mathcal{L}'}\tilde{L}(k),h_D;T\Big)\le\frac{1}{2}\mathcal{N}\Big(\bigcup_{C\in\mathcal{C}'}\bigcup_{Q\in A[2]/C[2]}\tau_Q(C\langle k\rangle),\hat{h}_A;T'\Big),$$

where $T'=(c_0T+c_1)/d_0$. As we mentioned in Remark 4.11, we have

$$\begin{aligned}&\mathcal{N}\Big(\bigcup_{C\in\mathcal{C}'}\bigcup_{Q\in A[2]/C[2]}\tau_Q(C\langle k\rangle),\hat{h}_A;T'\Big)\\&\quad\le\mathcal{N}_+\Big(\bigcup_{C\in\mathcal{C}'}\bigcup_{Q\in A[2]/C[2]}\tau_Q(C\langle k\rangle),\hat{h}_A;T'\Big)+\sharp(A\langle k\rangle\cap A(\bar{k})_{\rm tor})\end{aligned}$$

and

$$\begin{aligned}\mathcal{N}_+\Big(\bigcup_{C\in\mathcal{C}'}\bigcup_{Q\in A[2]/C[2]}\tau_Q(C\langle k\rangle),\hat{h}_A;T'\Big)&=\sum_{C\in\mathcal{C}'}\sum_{Q\in A[2]/C[2]}\mathcal{N}_+\Big(\tau_Q(C\langle k\rangle),\hat{h}_A;T'\Big)\\&=4\sum_{C\in\mathcal{C}'}\mathcal{N}_+\Big(C\langle k\rangle,\hat{h}_A;T'\Big)\end{aligned}$$

(note that $\hat{h}_A\circ\tau_Q=\hat{h}_A$ on $A(\bar{k})$). Therefore we obtain the desired inequality.

(ii) It follows from Corollary 4.10, (ii) and Lemma 5.1, (ii) that

$$\mathcal{N}_+(C\langle k\rangle,\hat{h}_A;T)\le d_0\,\mathcal{N}_+(\phi(C)\langle k\rangle,\hat{h}_{E\times E};d_0T).$$

By Proposition 4.5 and Lemma 4.7, we can take $(\alpha,\beta)\in R^2-\{(0,0)\}$ so that $\phi(C)=E_{\alpha,\beta}$ and $\deg\psi_{\alpha,\beta}\le m_0$. Then it follows from Corollary 4.10, (i) and Lemma 5.1, (iii) that

$$\mathcal{N}_+(E_{\alpha,\beta}\langle k\rangle,\hat{h}_{E\times E};d_0T)\le m_0\,\mathcal{N}_+\Big(E\langle k\rangle,\hat{h}_E;\frac{m_0d_0}{\deg E_{\alpha,\beta}}\,T\Big).$$

Therefore we obtain the desired inequality. □

5.2 Distribution of rational points on $\bigcup_{L\in\mathcal{L}} L$

Now, we fix a Weierstrass equation for E/k of the form

$$E: \quad y^2 = x^3 + ax + b \qquad (a, b \in k,\ 4a^3 + 27b^2 \neq 0).$$

Then $E\langle k\rangle = x^{-1}(\mathbb{P}^1(k))$ and

$$\hat{h}_E = \frac{1}{2}\, h_{\mathbb{P}^1} \circ x + O(1) \quad \text{on } E(\bar{k}),$$

where $h_{\mathbb{P}^1} : \mathbb{P}^1(\bar{k}) \to \mathbb{R}$ denotes the standard absolute logarithmic height function on $\mathbb{P}^1$. On the one hand, it follows from Example 1.1 that

$$\mathcal{N}(\mathbb{P}^1(k), h_{\mathbb{P}^1}; T) \asymp \exp(2[k:\mathbb{Q}]T) \quad \text{as } T \to \infty.$$

These formulas imply:

Lemma 5.3 *We have*

$$\mathcal{N}(E\langle k\rangle, \hat{h}_E; T) \asymp \exp(4[k:\mathbb{Q}]T) \quad \textit{as } T \to \infty.$$

Corollary 5.4 *The infimum*

$$h_0 = \inf\{\hat{h}_E(P)\ ;\ P \in E\langle k\rangle,\ \hat{h}_E(P) > 0\}$$

is positive.

By the corollary above, we obtain:

Corollary 5.5 *Let m_0 and h_0 be the positive constants as in Lemma 4.7 and Corollary 5.4, respectively. Then, for $C \in \mathcal{C}$,*

$$\mathcal{N}_+(C\langle k\rangle, \hat{h}_A; T) = 0 \quad \textit{if } \deg\phi(C) > \frac{m_0 d_0}{h_0}\, T.$$

Proof of Theorem 3.2 It follows from Lemma 5.2 that

$$\begin{aligned}
&\mathcal{N}((\mathcal{L} - \mathcal{L}_M)[k], h_D; T) \\
&\quad \le 2m_0 d_0 \sum_{C\in\mathcal{C}-\mathcal{C}_M} \mathcal{N}_+\Big(E\langle k\rangle, \hat{h}_E; \frac{m_0}{\deg\phi(C)}\,(c_0T + c_1)\Big) + \frac{1}{2}\,\sharp(A\langle k\rangle \cap A(\bar{k})_{\mathrm{tor}}),
\end{aligned}$$

where $\mathcal{C}_M = \{C \in \mathcal{C}\ ;\ \deg\phi(C) \le M\}$. Moreover, it follows from Corollary 5.5 that

$$\begin{aligned}
&\sum_{C\in\mathcal{C}-\mathcal{C}_M} \mathcal{N}_+\Big(E\langle k\rangle, \hat{h}_E; \frac{m_0}{\deg\phi(C)}\,(c_0T + c_1)\Big) \\
&\quad \le \sharp\Big\{C \in \mathcal{C}\ ;\ \deg\phi(C) \le \frac{m_0 d_0}{h_0}\,(c_0T + c_1)\Big\}\mathcal{N}\Big(E\langle k\rangle, \hat{h}_E; \frac{m_0}{M}\,(c_0T + c_1)\Big).
\end{aligned}$$

Hence we obtain the desired asymptotic formula by Proposition 3.1 and Lemma 5.3. □

References

[Ba] A. Baragar, Rational points on $K3$ surfaces in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$, Math. Ann. **305** (1996), 541–558.

[BM] V. V. Batyrev and Yu. I. Manin, Sur le nombre des points rationnels de hauteur borné des variétés algébriques, ibid. **286** (1990), 27–43.

[Bi] H. Billard, Propriétés arithmétiques d'une famille de surfaces $K3$, Compositio Math. **108** (1997), 247–275.

[CS1] G. S. Call and J. H. Silverman, Canonical heights on varieties with morphisms, ibid. **89** (1993), 163–205.

[CS2] ——, ——, Computing the canonical height on $K3$ surfaces, Math. Comp. **65** (1996), 259–290.

[K] E. Kani, Elliptic curves on abelian surfaces, Manuscripta Math. **84** (1994), 199–223.

[L] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.

[Mi] J. S. Milne, Abelian varieties, in *Arithmetic Geometry* (G. Cornell and J. H. Silverman eds.), Springer, New York, 1986, pp. 103–150.

[Mo] Y. Morita, Remarks on a conjecture of Batyrev and Manin, Tôhoku Math. J. **49** (1997), 437–448.

[MS] Y. Morita and A. Sato, Distribution of rational points on hyperelliptic surfaces, ibid. **44** (1992), 345–358.

[N] A. Néron, Quasi-fonctions et hauteurs sur les variétés abéliennes, Ann. of Math. **82** (1965), 249–331.

[Sc] S. H. Schanuel, Heights in number fields, Bull. Soc. Math. France **107** (1979), 433–449.

[S1] J. H. Silverman, Integral points on curves and surfaces, in *Number Theory, Ulm* 1987 (H. P. Schlickewei and E. Wirsing eds.), Lecture Notes in Math. **1380**, Springer, New York, 1989, pp. 202–241.

[S2] ——, Rational points on $K3$ surfaces: A new canonical height, Invent. Math. **105** (1991), 347–373.

[S3] ——, Counting integer and rational points on varieties, Astérisque **228** (1995), 223–236.

[W] L. Wang, Rational points and canonical heights on $K3$-surfaces in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$, in *Recent Developments in the Inverse Galois Problem* (M. D. Fried et al. eds.), Contemp. Math. **186**, Amer. Math. Soc., Providence, RI, 1995, pp. 273–289.

Mathematical Institute
Tohoku University
Sendai 980-8578
Japan
E-mail: atsushi@math.tohoku.ac.jp