Distribution of Rational Points on Hyperelliptic Surfaces

Yasuo Morita* and Atsushi Sato

Abstract

In this paper, we study distribution of rational points on a hyperelliptic surface defined over an algebraic number field, and show that this distribution is very similar to the distribution of rational points on an abelian surface. As an application, we show that a conjecture of Batyrev-Manin holds for such a surface.

1 Introduction

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

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 $\mathcal{L}$ be an ample invertible sheaf on the k–variety V and let $h_{\mathcal{L}}$ be the (absolute) logarithmic height function associated to $\mathcal{L}$. Then, for any positive number M, $\{P \in V(k)\ ;\ h_{\mathcal{L}}(P) \leq M\}$ is a finite set. We define a function $N_{\mathcal{L}}(V(k); M)$ of M by

$$N_{\mathcal{L}}(V(k); M) = \#\{P \in V(k)\ ;\ h_{\mathcal{L}}(P) \leq M\}.$$

One can obtain very important information on $V(k)$ by investigating the asymptotic behavior of $N_{\mathcal{L}}(V(k); M)$ as $M \to \infty$.

Let A be an abelian variety defined over k. Then the set $A(k)$ of k–rational points on A is a finitely generated abelian group (the Mordell-Weil theorem). In 1965, Néron [7]

1980 *Mathematics Subject Classification.* Primary 11G35; Secondary 14J20. *Key Words and phrases.* Hyperelliptic surfaces, heights, rational points.

*A part of this work was done when the first author was a member of the Sonderforschungsbereich 170, in Göttingen. He was also supported by the Grant-in-Aid for Scientific Research (No. 02640006) of the Ministry of Education, Science and Culture, Japan.

obtained the following asymptotic formula by using the canonical height:

$$N_{\mathcal{L}}(A(k);M) = cM^{r/2} + O(M^{(r-1)/2}) \quad \text{as} \quad M \to \infty,$$

where r is the rank of the abelian group $A(k)$ and c is a positive number which depends only on the algebraic equivalence class of $\mathcal{L}$.

For the n–dimensional projective space $\mathbf{P}^n$, Schanuel [8] obtained the following asymptotic formula:

$$N_{\mathcal{O}(1)}(\mathbf{P}^n(k);M) = c\exp((n+1)M) + \begin{cases} O(M\exp(M)) & \text{if } \ n=d=1 \\ O(\exp((n+1-(1/d))M)) & \text{otherwise} \end{cases}$$

as $M \to \infty$, where $d = [k : \mathbf{Q}]$ 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.

The main purpose of this paper is to investigate the set $S(k)$ of k–rational points on a hyperelliptic surface S defined over k, especially to investigate the asymptotic behavior of $N_{\mathcal{L}}(S(k);M)$ as $M \to \infty$.

Let S be a hyperelliptic surface defined over k. Then S can be expressed as a quotient space of an abelian variety A by a finite group of automorphisms. We study the set of k–rational points on S by using this covering structure and by reducing the problem to the corresponding problem on abelian varieties. Under a minor assumption, we can express the set $S(k)$ in terms of the abelian variety A and *a finite number* of twists of A (cf. Theorem 3.9 and Remark 3.11). Then, by applying the theory of height functions, we obtain the following theorem, which implies that the distribution of rational points on a hyperelliptic surface is very similar to the distribution of rational points on an abelian variety.

Theorem A *Let k be an algebraic number field of finite degree and let S be a hyperelliptic surface defined over k. Then there exists a finite extension k' of k satisfying the following property*:

Let K be any finite extension of k'. Then, for any ample invertible sheaf $\mathcal{L}$ on S/K, we have

$$N_{\mathcal{L}}(S(K);M) = cM^{r/2} + O(M^{(r-1)/2}) \quad \textit{as} \quad M \to \infty,$$

where r is a non-negative integer which depends on K but not on $\mathcal{L}$, while c is a positive number which depends on K and the algebraic equivalence class of $\mathcal{L}$.

We say that the ground field k is *sufficiently large* if k' and k coincide. We give in §3 a sufficient condition for k to be sufficiently large. If k is sufficiently large, the above theorem can be simplified:

Theorem A′ *Let k and S be as above. Suppose that k is sufficiently large. Then, for any ample invertible sheaf $\mathcal{L}$ on the k–variety S, the above asymptotic formula for $N_{\mathcal{L}}(S(k); M)$ holds.*

Throughout this paper, *all varieties, morphisms, sheaves, etc. are assumed to be defined over the algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$*, and we use the following notation:

If A is an abelian variety, we denote by O the unit element, and by $\mathrm{Aut}(A)$ (resp. $\mathrm{Aut}(A, O)$) the automorphism group of A as an algebraic variety (resp. as a group variety). If A is defined over a field k, we denote by $\mathrm{Aut}_k(A)$ (resp. $\mathrm{Aut}_k(A, O)$) the group consisting of all elements of $\mathrm{Aut}(A)$ (resp. $\mathrm{Aut}(A, O)$) which are defined over k.

For any abelian group $\mathcal{A}$, we denote by $\mathcal{A}_{\mathtt{tor}}$ the torsion subgroup of $\mathcal{A}$. If $\mathcal{A}$ is finitely generated, we denote by $\mathcal{A}_{\mathtt{free}}$ and $\mathcal{A}_{\mathbf{R}}$ the quotient group $\mathcal{A}/\mathcal{A}_{\mathtt{tor}}$ and the $\mathbf{R}$–vector space $\mathcal{A} \otimes_{\mathbf{Z}} \mathbf{R}$, respectively.

If $\mathcal{G}$ is a group, and if g, g' are elements of $\mathcal{G}$, we denote by $\langle g \rangle$ (resp. $\langle g, g' \rangle$) the subgroup of $\mathcal{G}$ generated by g (resp. g and g').

2 Hyperelliptic Surfaces

Let S be a nonsingular projective algebraic surface defined over $\bar{\mathbf{Q}}$ without exceptional curves of the first kind. S is called *a hyperelliptic surface* if the Kodaira dimension $\kappa(S)$ of S is 0 and the second Betti number B_2 of S is 2 (cf. [2]).

Any hyperelliptic surface can be expressed as a quotient space of an abelian variety by a finite group of automorphisms. This fact is due to [3], and we quote the following more explicit result from [2].

Theorem 2.1 *For any hyperelliptic surface S, there exist elliptic curves E_1, E_2 and a finite subgroup G of $\mathrm{Aut}(E_1) \times \mathrm{Aut}(E_2)$ such that $S \cong (E_1 \times E_2)/G$. Further, these elliptic curves E_1, E_2 and the subgroup G of $\mathrm{Aut}(E_1) \times \mathrm{Aut}(E_2)$ satisfy one of the following conditions*:

(2a) E_1, E_2 *arbitrary*, $G = \langle g \rangle$,
$g : (P_1, P_2) \longmapsto (P_1 + T_1, -P_2)$, $T_1 \in E_1(\bar{\mathbf{Q}})$, order $T_1 = 2$;

(2b) E_1, E_2 *arbitrary*, $G = \langle g, g' \rangle$,
$g : (P_1, P_2) \longmapsto (P_1 + T_1, -P_2)$, $g' : (P_1, P_2) \longmapsto (P_1 + T_1', P_2 + T_2')$,
$T_1, T_1' \in E_1(\bar{\mathbf{Q}})$, order $T_1 =$ order $T_1' = 2$, $\langle T_1 \rangle \cap \langle T_1' \rangle = \{O\}$,
$T_2' \in E_2(\bar{\mathbf{Q}})$, order $T_2' = 2$;

(3a) E_1 *arbitrary*, $j(E_2) = 0$, $G = \langle g \rangle$,
$g : (P_1, P_2) \longmapsto (P_1 + T_1, \rho^2 P_2)$, $T_1 \in E_1(\bar{\mathbf{Q}})$, order $T_1 = 3$;

(3b) E_1 *arbitrary*, $j(E_2) = 0$, $G = \langle g, g' \rangle$,
$g : (P_1, P_2) \longmapsto (P_1 + T_1, \rho^2 P_2)$, $g' : (P_1, P_2) \longmapsto (P_1 + T_1', P_2 + T_2')$,
$T_1, T_1' \in E_1(\bar{\mathbf{Q}})$, order $T_1 =$ order $T_1' = 3$, $\langle T_1 \rangle \cap \langle T_1' \rangle = \{O\}$,
$T_2' \in E_2(\bar{\mathbf{Q}})$, order $T_2' = 3$, $\rho^2 T_2' = T_2'$;

(4a) E_1 *arbitrary*, $j(E_2) = 1728$, $G = \langle g \rangle$,
$g : (P_1, P_2) \longmapsto (P_1 + T_1, iP_2)$, $T_1 \in E_1(\bar{\mathbf{Q}})$, order $T_1 = 4$;

(4b) E_1 *arbitrary*, $j(E_2) = 1728$, $G = \langle g, g' \rangle$,
$g : (P_1, P_2) \longmapsto (P_1 + T_1, iP_2)$, $g' : (P_1, P_2) \longmapsto (P_1 + T_1', P_2 + T_2')$,
$T_1, T_1' \in E_1(\bar{\mathbf{Q}})$, order $T_1 = 4$, order $T_1' = 2$, $\langle T_1 \rangle \cap \langle T_1' \rangle = \{O\}$,
$T_2' \in E_2(\bar{\mathbf{Q}})$, order $T_2' = 2$, $iT_2' = T_2'$;

(6a) E_1 *arbitrary*, $j(E_2) = 0$, $G = \langle g \rangle$,
$g : (P_1, P_2) \longmapsto (P_1 + T_1, \rho P_2)$, $T_1 \in E_1(\bar{\mathbf{Q}})$, order $T_1 = 6$.

Here, $j(E_2)$ *denotes the* j*–invariant of the elliptic curve* E_2*, while* ρ *(resp.* i*) denotes an element of* $\mathrm{Aut}(E_2, O)$ *of order* 6 *(resp. of order* 4*).*

Let $A = E_1 \times E_2$ be the product variety, and let $\pi : A \to S$ be the natural morphism. Then A is a 2–dimensional abelian variety, π is an étale morphism, and π induces an isomorphism of A/G onto S.

Remark 2.2 (i) The natural projection $G \to \mathrm{Aut}(E_l)$ $(l = 1, 2)$ is a homomorphism of groups. We denote by G_l the image of this map.

(ii) Let $O = (O_1, O_2)$ be the unit element of the abelian variety A and let $\mathrm{pr}_1 : A \to E_1$ be the projection. Then the image of the G–orbit O^G under pr_1 coincides with the G_1–orbit $O_1^{G_1}$. We denote this orbit by Γ :

$$\Gamma = \mathrm{pr}_1(O^G) = O_1^{G_1}.$$

Then Γ is a finite subgroup of $E_1(\bar{\mathbf{Q}})$, which is generated by one element T_1, or two elements T_1 and T_1'.

(iii) The group G_1 acts on the elliptic curve E_1 as translations by elements of Γ. More precisely, for $P = (P_1, P_2) \in A(\bar{\mathbf{Q}})$ and $f = (f_1, f_2) \in G$, we have

$$\mathrm{pr}_1(f(P)) = f_1(P_1) = P_1 + f_1(O_1) = P_1 + \mathrm{pr}_1(f(O)),$$

and hence

$$\mathrm{pr}_1(P^G) = P_1^{G_1} = P_1 + \Gamma.$$

(iv) The map

$$G \longrightarrow \Gamma, \qquad f \longmapsto \mathrm{pr}_1(f(O))$$

is an isomorphism of groups.

Since Γ is a finite subgroup of $E_1(\bar{\mathbf{Q}})$, there exists an isogeny $\phi : E_1 \to E$ of elliptic curves such that $\mathrm{Ker}\ \phi = \Gamma$. These E and ϕ are determined by E_1 and Γ uniquely up to isomorphisms. Since E is isomorphic to the quotient variety E_1/G_1, we have the following commutative diagram:

$$(*) \qquad \begin{array}{ccc} A = E_1 \times E_2 & \xrightarrow{\mathrm{pr}_1} & E_1 \\ \pi\big\downarrow & & \phi\big\downarrow \\ S \cong A/G & \xrightarrow{p} & E \cong E_1/G_1 \end{array}$$

3 Rational Points on Hyperelliptic Surfaces

Let k be an algebraic number field of finite degree and let S be a hyperelliptic surface defined over k. Then, by Theorem 2.1, there exist two elliptic curves E_1, E_2 and a finite subgroup G of $\mathrm{Aut}(E_1) \times \mathrm{Aut}(E_2)$ such that $S \cong (E_1 \times E_2)/G$ over $\bar{\mathbf{Q}}$.

Throughout this section, we assume that this isomorphism is defined over k. More precisely, *we assume*:

(C1) E_1 and E_2 are defined over k;
(C2) $E_1(k) \neq \emptyset$ and $E_2(k) \neq \emptyset$;
(C3) all elements of G are defined over k;
(C4) the natural morphism $\pi : A \to S$ is defined over k.

As we will show later, any field k which satisfies these conditions (C1)–(C4) can be used as the field k' mentioned in Theorem A.

These conditions (C1)–(C4) imply:

(C5) $A = E_1 \times E_2$ is a 2-dimensional abelian variety defined over k;
(C6) $T_1, T_1' \in E_1(k)$ and $T_2' \in E_2(k)$;
(C7) in cases (3a), (3b) and (6a), $(1 + \sqrt{-3})/2 \in k$ and $\rho \in \mathrm{Aut}_k(E_2, O)$;
(C8) in cases (4a) and (4b), $\sqrt{-1} \in k$ and $i \in \mathrm{Aut}_k(E_2, O)$.

It follows from (C3) that, for every $f \in G$, $(f(P))^\sigma = f(P^\sigma)$ holds for any $P \in A(\bar{\mathbf{Q}})$ and $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/k)$. Further it follows from (C4) that $(\pi(P))^\sigma = \pi(P^\sigma)$ holds for any $P \in A(\bar{\mathbf{Q}})$ and $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/k)$. Therefore, for any $P \in A(\bar{\mathbf{Q}})$, $\pi(P)$ is a k–rational point on S if and only if the G–orbit of P is defined over k (i.e., the set P^G is invariant under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/k)$). In particular, $\pi(A(k)) \subset S(k)$.

In the rest of this section, we study the set $\pi^{-1}(S(k))$.

By (C6), Γ is a finite subgroup of $E_1(k)$. Hence we may assume that the elliptic curve E and the isogeny $\phi : E_1 \to E$ are defined over k. We note that the k–isomorphism classes

of E and ϕ are determined uniquely. Hence *all varieties and morphisms in the diagram* $(*)$ *are defined over* k.

Since ϕ is defined over k, $\phi(E_1(k)) \subset E(k)$. Since E_1 and E are k–isogenous, we obtain

$$\text{rank } E_1(k) = \text{rank } \phi(E_1(k)) = \text{rank } E(k) = \text{rank } \phi^{-1}(E(k)).$$

Consequently, both of the groups $\phi^{-1}(E(k))/E_1(k)$ and $E(k)/\phi(E_1(k))$ are finite, and ϕ induces an isomorphism between these two groups.

Lemma 3.1 *If* $P = (P_1, P_2) \in A(\bar{\mathbf{Q}})$ *satisfies* $\pi(P) \in S(k)$, *then* $P_1 \in \phi^{-1}(E(k))$.

Proof This lemma follows easily from the k–rationality and the commutativity of the diagram $(*)$. q.e.d.

In view of this lemma, we first study elements of the group $\phi^{-1}(E(k))$.

For any $P = (P_1, P_2) \in \pi^{-1}(S(k))$, let $k(P)$ (resp. $k(P_1)$) be the field generated over k by the coordinates of P (resp. P_1). We see later that $k(P)$ and $k(P_1)$ coincide. (In other words, we see later that $P_2 \in E_2(\bar{\mathbf{Q}})$ is defined over $k(P_1)$.) Hence we study $k(Q)$ $(Q \in \phi^{-1}(E(k)))$.

Lemma 3.2 (i) *For any* $Q \in \phi^{-1}(E(k))$, $k(Q)$ *is a finite Galois extension of* k, *and the map*

$$\text{Gal}(k(Q)/k) \longrightarrow \Gamma, \qquad \sigma \longmapsto Q^\sigma - Q$$

is an injective homomorphism. In particular, $k(Q)$ *is an abelian extension of* k.

(ii) *If* $Q, Q' \in \phi^{-1}(E(k))$ *satisfy* $Q \equiv Q'$ (mod. $E_1(k)$), *then* $k(Q) = k(Q')$ *holds.*

Proof (i) Let σ be any element of $\text{Gal}(\bar{\mathbf{Q}}/k)$. Since ϕ and $\phi(Q)$ are defined over k, $\phi(Q) = (\phi(Q))^\sigma = \phi(Q^\sigma)$. Hence $Q^\sigma - Q$ is contained in $\text{Ker } \phi = \Gamma$. It follows that

$$Q^\sigma \in Q + \Gamma \subset Q + E_1(k).$$

Hence Q^σ is defined over $k(Q)$. Thus $k(Q)$ is a Galois extension of k.

If σ and τ are contained in $\text{Gal}(k(Q)/k)$, then we have

$$Q^{\sigma\tau} - Q = (Q^\sigma - Q)^\tau + Q^\tau - Q = (Q^\sigma - Q) + (Q^\tau - Q),$$

because $Q^\sigma - Q \in \Gamma \subset E_1(k)$. Therefore the map $\sigma \mapsto Q^\sigma - Q$ is a homomorphism of groups. The injectivity of this map is obvious.

(ii) Clear. q.e.d.

Remark 3.3 Let v be a finite prime divisor of k such that v is prime to the exponent of Γ, and that the elliptic curve E_1 has a good reduction at v. Then v is unramified in $k(Q)/k$ (cf., e.g., [10, Chapter VII, Proposition 4.1, (a)]).

Now we study the second elliptic curve E_2.

We fix a point Q of $E_1(\bar{\mathbf{Q}})$. In view of Lemma 3.1, we may assume $Q \in \phi^{-1}(E(k))$, because we are interested in a case such that $\pi((Q,R)) \in S(k)$ for some $R \in E_2(\bar{\mathbf{Q}})$. We denote by $E_2\{Q\}$ the set consisting of all such points R :

$$E_2\{Q\} = \{R \in E_2(\bar{\mathbf{Q}}) \ ; \ (Q,R) \in \pi^{-1}(S(k))\}.$$

By composing the homomorphisms $\mathrm{Gal}(k(Q)/k) \to \Gamma \to G \to \mathrm{Aut}_k(E_2)$ mentioned in Remark 2.2 and Lemma 3.2, we obtain an injective homomorphism

$$\xi^Q : \mathrm{Gal}(k(Q)/k) \longrightarrow \mathrm{Aut}_k(E_2), \qquad \sigma \longmapsto \xi^Q_\sigma.$$

Lemma 3.4 (i) *For any $Q \in \phi^{-1}(E(k))$, we have*

$$E_2\{Q\} = \{R \in E_2(k(Q)) \ ; \ R^\sigma = \xi^Q_\sigma(R) \ \ \textit{for any} \ \ \sigma \in \mathrm{Gal}(k(Q)/k)\}.$$

(ii) *If $Q, Q' \in \phi^{-1}(E(k))$ satisfy $Q \equiv Q'$ (mod. $E_1(k)$), then $E_2\{Q\} = E_2\{Q'\}$ holds.*

Proof (i) Let R be any point of $E_2\{Q\}$. We show that R is defined over $k(Q)$. Let σ be any element of $\mathrm{Gal}(\bar{\mathbf{Q}}/k(Q))$. Since (Q,R) is a point of $\pi^{-1}(S(k))$, the point

$$(Q,R)^\sigma = (Q^\sigma, R^\sigma) = (Q, R^\sigma)$$

belongs to the G–orbit$(Q,R)^G$. Hence there exists an element $f \in G$ such that $(Q,R^\sigma) = f(Q,R)$. It follows from Remark 2.2, (iii) that $Q = Q + \mathrm{pr}_1(f(O))$. Since the map $G \ni f \mapsto \mathrm{pr}_1(f(O)) \in \Gamma$ is injective (cf. Remark 2.2, (iv)), we have $f = \mathrm{id}$. Consequently, we obtain

$$(Q,R)^\sigma = (Q,R) \quad \text{for any} \quad \sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/k(Q)),$$

and hence R is defined over $k(Q)$. Therefore $E_2\{Q\} \subset E_2(k(Q))$.

Let R be as above, and let σ be any element of $\mathrm{Gal}(k(Q)/k)$. Then there exists a unique element f of G such that $(Q,R)^\sigma = f(Q,R)$. This f is the element of G which corresponds to $Q^\sigma - Q \in \Gamma$ under the isomorphism $G \cong \Gamma$. Hence, by the definition of ξ^Q, we have $R^\sigma = \xi^Q_\sigma(R)$. Therefore

$$E_2\{Q\} \subset \{R \in E_2(k(Q)) \ ; \ R^\sigma = \xi^Q_\sigma(R) \ \ \text{for any} \ \ \sigma \in \mathrm{Gal}(k(Q)/k)\}.$$

By reversing the above argument, we obtain

$$E_2\{Q\} \supset \{R \in E_2(k(Q)) \ ; \ R^\sigma = \xi^Q_\sigma(R) \ \ \text{for any} \ \ \sigma \in \mathrm{Gal}(k(Q)/k)\}.$$

(ii) Suppose that $Q \equiv Q'$ (mod. $E_1(k)$). Then it follows from Lemma 3.2, (ii) that $k(Q) = k(Q')$. Hence

$$Q^\sigma - Q = (Q')^\sigma - Q' \quad \text{for any} \quad \sigma \in \mathrm{Gal}(k(Q)/k) = \mathrm{Gal}(k(Q')/k),$$

which implies that $\xi^Q = \xi^{Q'}$. Therefore, by (i), the equality $E_2\{Q\} = E_2\{Q'\}$ holds.

q.e.d.

By using Lemma 3.1 and Lemma 3.4, (i), we have

$$k(P) = k(P_1) \quad \text{for any} \quad P = (P_1, P_2) \in \pi^{-1}(S(k)).$$

The following corollary shows that we may assume that $P \in A(\bar{\mathbf{Q}})$ is defined over a fixed finite extension of k.

Corollary 3.5 *The number of the extensions* $\{k(P)\ ;\ P \in \pi^{-1}(S(k))\}$ *of* k *is finite.*

Proof Let $P = (P_1, P_2)$ be any point of $\pi^{-1}(S(k))$. It follows from Lemma 3.1 that $P_1 \in \phi^{-1}(E(k))$. We also have $k(P) = k(P_1)$. Therefore

$$\{k(P)\ ;\ P \in \pi^{-1}(S(k))\} \subset \{k(Q)\ ;\ Q \in \phi^{-1}(E(k))\}.$$

On the one hand, by Lemma 3.2, (ii), we have

$$\{k(Q)\ ;\ Q \in \phi^{-1}(E(k))\} = \{k(Q)\ ;\ Q \in \phi^{-1}(E(k))/E_1(k)\}.$$

Since $\phi^{-1}(E(k))/E_1(k)$ is a finite set, we obtain the corollary. q.e.d.

Remark 3.6 We note that this corollary can be proved also by using Lemma 3.2, (i) and Remark 3.3. We can prove it also by using Hermite's finiteness theorem and the Chevalley-Weil theorem (cf. [9, pp 49–50]).

Remark 3.7 Since the homomorphism ξ^Q is a 1-cocycle in $H^1(\mathrm{Gal}(k(Q)/k), \mathrm{Aut}(E_2))$, we can twist the elliptic curve E_2 by this cocycle ξ^Q. Hence there exists an algebraic curve C defined over k and an isomorphism $\theta : C \to E_2$ defined over $k(Q)$ such that

$$\xi^Q_\sigma = \theta^\sigma \circ \theta^{-1} \quad \text{for any} \quad \sigma \in \mathrm{Gal}(k(Q)/k).$$

One can easily check that for any $R \in E_2(\bar{\mathbf{Q}})$, $R \in E_2\{Q\}$ if and only if $\theta^{-1}(R) \in C(k)$.

$E_2\{Q\}$ may be empty. But, if $E_2\{Q\}$ has a point, it coincides with a coset of a subgroup of $E_2(k(Q))$. Namely, we have the following:

Lemma 3.8 *Let Q be a point of $\phi^{-1}(E(k))$. We assume $E_2\{Q\}$ to be nonempty. Then there exists a unique subgroup $C\{Q\}$ of $E_2(k(Q))$ such that*

$$E_2\{Q\} = R + C\{Q\} \quad \textit{for any} \quad R \in E_2\{Q\}.$$

In particular, if $O \in E_2\{Q\}$, then $E_2\{Q\}$ is a subgroup of $E_2(k(Q))$.

Proof Let C and θ be as in the above remark, and we fix a point R of $E_2\{Q\}$. Then $\theta^{-1}(R)$ is a k–rational point on C. Since E_2 is isomorphic to C over $k(Q)$, the genus of C is 1. Hence the curve C has a structure of 1–dimensional abelian variety defined over k with $\theta^{-1}(R)$ as its unit element. Hence the map

$$E_2 \longrightarrow C, \qquad R' \longmapsto \theta^{-1}(R' + R)$$

is an isomorphism of abelian varieties defined over $k(Q)$. We denote by $C\{Q\}$ the inverse image of $C(k)$ under this map. It follows that $C\{Q\}$ is a subgroup of $E_2(k(Q))$, and that $C\{Q\} = \theta(C(k)) - R = E_2\{Q\} - R$. Hence $E_2\{Q\} = R + C\{Q\}$. It is easy to check that $C\{Q\}$ is independent of the choice of R, and that such $C\{Q\}$ is uniquely determined by Q. q.e.d.

By using this lemma, we can obtain an explicit expression for the set $\pi^{-1}(S(k))$.

Theorem 3.9 *Let k be an algebraic number field of finite degree, S a hyperelliptic surface defined over k, and A, π, etc. as in §2. Suppose that the conditions* (C1)–(C4) *are satisfied. Let $E_2\{Q\}$ and $C\{Q\}$ ($Q \in \phi^{-1}(E(k))$) be as above. Then $\pi^{-1}(S(k))$ is expressed as a disjoint union of a finite number of cosets* (*cf. Lemma* 3.8):

$$\pi^{-1}(S(k)) = \coprod_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \Big((Q, R) + E_1(k) \times C\{Q\} \Big).$$

Here R denotes a point of $E_2\{Q\}$.

Proof Let $\{Q^{(1)}, Q^{(2)}, \cdots, Q^{(t)}\} \subset \phi^{-1}(E(k))$ be a complete set of representatives of $\phi^{-1}(E(k))/E_1(k)$. Suppose that $P = (P_1, P_2)$ is contained in $\pi^{-1}(S(k))$. Then it follows from Lemma 3.1 that a congruence $P_1 \equiv Q^{(l)}$ (mod. $E_1(k)$) holds for some l. Therefore, by Lemma 3.4, (ii), we have $P_2 \in E_2\{P_1\} = E_2\{Q^{(l)}\}$. Hence $P \in \Big(Q^{(l)} + E_1(k)\Big) \times E_2\{Q^{(l)}\}$. Therefore we obtain

$$\pi^{-1}(S(k)) \subset \bigcup_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \Big(Q + E_1(k)\Big) \times E_2\{Q\}.$$

Conversely, if $E_2\{Q^{(l)}\}$ is not empty, then it follows from the definition of $E_2\{Q^{(l)}\}$ and from Lemma 3.4, (ii) that

$$\Big(Q^{(l)} + E_1(k)\Big) \times E_2\{Q^{(l)}\} \subset \pi^{-1}(S(k)).$$

Therefore

$$\pi^{-1}(S(k)) = \bigcup_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \Big(Q + E_1(k)\Big) \times E_2\{Q\}.$$

Since the union

$$\bigcup_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \Big(Q + E_1(k)\Big)$$

is disjoint, the union

$$\bigcup_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \Big(Q + E_1(k)\Big) \times E_2\{Q\}$$

is also disjoint. Hence, using Lemma 3.8, we obtain the desired result. q.e.d.

Remark 3.10 Let $\{Q^{(1)}, Q^{(2)}, \cdots, Q^{(t)}\} \subset \phi^{-1}(E(k))$ be a complete set of representatives of $\{Q \in \phi^{-1}(E(k))/E_1(k)\ ;\ E_2\{Q\} \neq \emptyset\}$. Then, for each l, there exists an elliptic curve $C^{(l)}$ defined over k and an isomorphism $\theta^{(l)} : C^{(l)} \to E_2$ defined over $k(Q^{(l)})$ such that $E_2\{Q^{(l)}\} = \theta^{(l)}(C^{(l)}(k))$, as we have mentioned in Remark 3.7. Hence we can rewrite the above expression as

$$\pi^{-1}(S(k)) = \coprod_{l=1}^{t} \Big(Q^{(l)} + E_1(k)\Big) \times \theta^{(l)}(C^{(l)}(k)).$$

In particular, if we can calculate effectively the set $C(k)$ of k–rational points on any elliptic curve C defined over k, then we can also calculate effectively the set $S(k)$ of k–rational points on a hyperelliptic surface S.

Remark 3.11 Let E be an elliptic curve defined over k. Then the quotient variety of E by $\{\pm \mathrm{id}_E\}$ is isomorphic to $\mathbf{P}^1$. Since $\mathbf{P}^1$ has much more rational points than elliptic curves, by comparing the number of rational points on $\mathbf{P}^1$ and the number of rational points on a finite disjoint union of elliptic curves, we observe that in this case, *an infinite number* of twists E^σ of E over quadratic extensions of k are needed to express $\varpi^{-1}(\mathbf{P}^1(k)) = \coprod_\sigma E^\sigma(k)$, where $\varpi : E \to \mathbf{P}^1$ is the natural morphism.

On the other hand, we need only *a finite number* of twists $E_1 \times C^{(1)},\ E_1 \times C^{(2)}, \cdots,\ E_1 \times C^{(t)}$ of $A = E_1 \times E_2$ to express $\pi^{-1}(S(k))$ in our case.

4 Number of Rational Points of Bounded Heights

Now we state the main result of this paper, which is a more precise form of Theorem A in §1.

Theorem 4.1 (Main Theorem) *Let k be an algebraic number field of finite degree and let S be a hyperelliptic surface defined over k. We assume that the conditions* (C1)–(C4) *in* §3 *are satisfied. Then, for any ample invertible sheaf $\mathcal{L}$ on the k–variety S, we have*

$$N_{\mathcal{L}}(S(k); M) = cM^{r/2} + O(M^{(r-1)/2}) \quad as \quad M \to \infty,$$

where

$$r = \text{rank } E_1(k) + \max_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \text{rank } C\{Q\}$$

is a non-negative integer, and c is a positive constant which depends on the algebraic equivalence class of $\mathcal{L}$.

Remark 4.2 Using the notation of Remark 3.10, we can express the integer r as

$$r = \text{rank } E_1(k) + \max_{1 \leq l \leq t} \text{rank } C^{(l)}(k).$$

Hence the integer r is determined by the structure of the groups of k–rational points on elliptic curves E_1, $C^{(1)}$, $C^{(2)}, \cdots$, $C^{(t)}$. Therefore, if we assume the Birch and Swinnerton-Dyer conjecture on elliptic curves, then r can be described in terms of the behavior at $s = 1$ of the L–functions of these elliptic curves.

To obtain Theorem 4.1 from Theorem 3.9, we use the following results (Lemmas 4.3 and 4.4) on height functions.

Lemma 4.3 *If $f : V \to W$ is a morphism of nonsingular projective varieties, and if $\mathcal{L}$ is an invertible sheaf on W, then we have*

$$h_{f^*\mathcal{L}} = h_{\mathcal{L}} \circ f + O(1)$$

as functions on $V(\bar{\mathbf{Q}})$, where $h_{\mathcal{L}}$ (resp. $h_{f^*\mathcal{L}}$) denotes the height function on W (resp. V) associated to $\mathcal{L}$ (resp. $f^*\mathcal{L}$). (We note that all varieties, morphisms, sheaves are assumed to be defined over $\bar{\mathbf{Q}}$.)

Proof See [11, Theorem 3.3, (b)]. q.e.d.

Lemma 4.4 *Let K be an algebraic number field of finite degree and let A be an abelian variety defined over K. Let $\mathcal{L}$ be an invertible sheaf on A/K and let $h_{\mathcal{L}}$ be the height function associated to $\mathcal{L}$. Then we have*:

(i) *There exists a unique quadratic form $q_{\mathcal{L}} : A(\bar{\mathbf{Q}}) \to \mathbf{R}$ and a unique linear form $l_{\mathcal{L}} : A(\bar{\mathbf{Q}}) \to \mathbf{R}$ such that*

$$h_{\mathcal{L}} = q_{\mathcal{L}} + l_{\mathcal{L}} + O(1)$$

as functions on $A(\bar{\mathbf{Q}})$. (The function $q_{\mathcal{L}} + l_{\mathcal{L}} : A(\bar{\mathbf{Q}}) \to \mathbf{R}$ is called the Néron-Tate height *or the* canonical height *associated to $\mathcal{L}$.)*

(ii) *Suppose that $\mathcal{L}$ is ample. Then $q_{\mathcal{L}}$ vanishes on $A(\bar{\mathbf{Q}})_{\mathtt{tor}}$, and the extension of $q_{\mathcal{L}}$ to the $\mathbf{R}$–vector space $A(K)_{\mathbf{R}} = A(K) \otimes_{\mathbf{Z}} \mathbf{R}$ is a positive definite quadratic form. Further, if $\mathcal{M}$ is an invertible sheaf on A which is algebraically equivalent to $\mathcal{L}$, then $q_{\mathcal{M}}$ and $q_{\mathcal{L}}$ coincide.*

(iii) *Suppose that $\mathcal{L}$ is ample. Then, for any $Q \in A(K)$ and any infinite subgroup $\mathcal{B}$ of $A(K)$, we have the following asymptotic formula*:

$$\#\{P \in Q + \mathcal{B} \ ; \ h_{\mathcal{L}}(P) \le M\} = cM^{r/2} + O(M^{(r-1)/2}) \quad as \quad M \to \infty,$$

where

$$r = \text{rank } \mathcal{B} \quad and \quad c = \#\mathcal{B}_{\mathtt{tor}} \times \frac{\text{Vol}(\{x \in \mathcal{B}_{\mathbf{R}} \ ; \ q_{\mathcal{L}}(x) \le 1\})}{\text{Vol}(\mathcal{B}_{\mathbf{R}}/\mathcal{B}_{\mathtt{free}})}.$$

Proof (i) See [5, Chapter 4, Theorem 3.1].

(ii) Suppose that $\mathcal{L}$ is ample, Then we have

$$\#\{P \in A(K) \ ; \ h_{\mathcal{L}}(P) \le M\} < \infty$$

for any constant M (cf., e.g., [11, Corollary 3.4]). Since $q_{\mathcal{L}}$ is quadratic and since $l_{\mathcal{L}}$ is linear, we obtain

$$\#\{P \in A(K) \ ; \ q_{\mathcal{L}}(P) \le M\} < \infty$$

for any constant M. Since $q_{\mathcal{L}}$ is a quadratic form, it is easy and well-known that $q_{\mathcal{L}}$ vanishes on $A(\bar{\mathbf{Q}})_{\mathtt{tor}}$. Hence $q_{\mathcal{L}}$ is a positive definite quadratic form on $A(K)_{\mathbf{R}}$ (cf. [5, Chapter 5, §7]).

Suppose that $\mathcal{M}$ is algebraically equivalent to $\mathcal{L}$. Then we have

$$\frac{h_{\mathcal{M}}(P)}{h_{\mathcal{L}}(P)} \to 1 \quad \text{as} \quad h_{\mathcal{M}}(P) \to \infty \quad (P \in A(K))$$

(cf. [5, Chapter 4, Proposition 5.3]). Since non-degenerate quadratic forms grow faster than linear forms, it follows that

$$\frac{q_{\mathcal{M}}(P)}{q_{\mathcal{L}}(P)} \to 1 \quad \text{as} \quad q_{\mathcal{M}}(P) \to \infty \quad (P \in A(K)).$$

Since $q_{\mathcal{M}}$ and $q_{\mathcal{L}}$ are quadratic forms, the equality $q_{\mathcal{M}} = q_{\mathcal{L}}$ holds as functions on $A(K)$.

(iii) It follows from (ii) that $l_{\mathcal{L}} = O(q_{\mathcal{L}}^{1/2})$ holds as functions on $A(K)$. By using this estimate, one can obtain the asymptotic formula as in [5, Chapter 5, Theorem 7.5]. q.e.d.

Proof of Theorem 4.1 Since the natural morphism $\pi : A \to S$ is finite and surjective, the inverse image $\pi^*\mathcal{L}$ is an ample invertible sheaf on the abelian variety A. It follows from Lemma 4.3 that

$$h_{\pi^*\mathcal{L}} = h_{\mathcal{L}} \circ \pi + O(1)$$

holds as functions on $A(\bar{\mathbf{Q}})$. On the one hand, we have

$$N_{\mathcal{L}}(S(k); M) = \frac{\#\{P \in \pi^{-1}(S(k)) \ ; \ h_{\mathcal{L}}(\pi(P)) \leq M\}}{\#G},$$

where G is the subgroup of $\mathrm{Aut}(E_1) \times \mathrm{Aut}(E_2)$ defined in Theorem 2.1. Hence there exists a positive constant M_0 such that

$$\frac{N_{\pi^*\mathcal{L}}(\pi^{-1}(S(k)); M - M_0)}{\#G} \leq N_{\mathcal{L}}(S(k); M) \leq \frac{N_{\pi^*\mathcal{L}}(\pi^{-1}(S(k)); M + M_0)}{\#G},$$

where

$$N_{\pi^*\mathcal{L}}(\pi^{-1}(S(k)); M \pm M_0) = \#\{P \in \pi^{-1}(S(k)) \ ; \ h_{\pi^*\mathcal{L}}(P) \leq M \pm M_0\}.$$

By Theorem 3.9, $\pi^{-1}(S(k))$ can be expressed as

$$\pi^{-1}(S(k)) = \coprod_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \Big((Q, R) + E_1(k) \times C\{Q\} \Big).$$

Hence we have

$$\begin{aligned} &N_{\pi^*\mathcal{L}}(\pi^{-1}(S(k)); M \pm M_0) \\ &\quad = \sum_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \#\{P \in (Q, R) + E_1(k) \times C\{Q\} \ ; \ h_{\pi^*\mathcal{L}}(P) \leq M \pm M_0\}. \end{aligned}$$

Now, if $E_2\{Q\}$ is not empty, then it follows from Lemma 4.4, (iii) that

$$\begin{aligned} &\#\{P \in (Q, R) + E_1(k) \times C\{Q\} \ ; \ h_{\pi^*\mathcal{L}}(P) \leq M \pm M_0\} \\ &\quad = c(Q)(M \pm M_0)^{r(Q)/2} + O((M \pm M_0)^{(r(Q)-1)/2}) \\ &\quad = c(Q)M^{r(Q)/2} + O(M^{(r(Q)-1)/2}) \end{aligned}$$

as $M \to \infty$, where

$$r(Q) = \mathrm{rank}\ (E_1(k) \times C\{Q\}) = \mathrm{rank}\ E_1(k) + \mathrm{rank}\ C\{Q\}$$

and

$$c(Q) = \#(E_1(k) \times C\{Q\})_{\mathtt{tor}} \times \frac{\mathrm{Vol}(\{x \in (E_1(k) \times C\{Q\})_{\mathbf{R}} \ ; \ q_{\pi^*\mathcal{L}}(x) \leq 1\})}{\mathrm{Vol}((E_1(k) \times C\{Q\})_{\mathbf{R}}/(E_1(k) \times C\{Q\})_{\mathtt{free}})}$$

(if $r(Q) = 0$, we put $c(Q) = \#(E_1(k) \times C\{Q\})$). We denote by c' the sum of the $c(Q)$ $(Q \in \phi^{-1}(E(k))/E_1(k),\ E_2\{Q\} \neq \emptyset)$ which satisfy

$$\text{rank } C\{Q\} = \max_{\substack{Q' \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q'\} \neq \emptyset}} \text{rank } C\{Q'\}.$$

Then c' is a positive number, and we have

$$\begin{aligned} N_{\pi^*\mathcal{L}}(\pi^{-1}(S(k)); M \pm M_0) &= \sum_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \left(c(Q) M^{r(Q)/2} + O(M^{(r(Q)-1)/2}) \right) \\ &= c' M^{r/2} + O(M^{(r-1)/2}) \end{aligned}$$

as $M \to \infty$, where

$$r = \max_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} r(Q) = \text{rank } E_1(k) + \max_{\substack{Q \in \phi^{-1}(E(k))/E_1(k) \\ E_2\{Q\} \neq \emptyset}} \text{rank } C\{Q\}.$$

By putting $c = c'/\#G$, we obtain the desired asymptotic formula. q.e.d.

Though k does not satisfy the conditions (C1)–(C4) in §3 in general, there exists a finite extension k' of k which satisfies these conditions. Then we have

$$\{P \in S(k) \ ; \ h_{\mathcal{L}}(P) \leq M\} \subset \{P \in S(k') \ ; \ h_{\mathcal{L}}(P) \leq M\}.$$

Since the integer r in Theorem 4.1 is independent of the choice of $\mathcal{L}$, we obtain the following result.

Corollary 4.5 *Let k be an algebraic number field of finite degree and let S be a hyperelliptic surface defined over k. Then there exists a non-negative integer r such that*

$$N_{\mathcal{L}}(S(k); M) = O(M^{r/2}) \quad \textit{as} \quad M \to \infty$$

for any ample invertible sheaf $\mathcal{L}$ on the k–variety S.

Let k be an algebraic number field of finite degree, V a nonsingular projective variety defined over k, and $\mathcal{L}$ an ample invertible sheaf on V/k. Let $H_{\mathcal{L}} = \exp \circ h_{\mathcal{L}}$ be the (absolute) exponential height function. Then the Dirichlet series

$$Z_{\mathcal{L}}(V(k); s) = \sum_{P \in V(k)} H_{\mathcal{L}}(P)^{-s} \qquad (s \in \mathbf{C})$$

was studied in [1] and [4]. By using Corollary 4.5, we obtain the following:

Corollary 4.6 *Let S be a hyperelliptic surface defined over an algebraic number field k of finite degree, and let $\mathcal{L}$ be an ample invertible sheaf on S/k. Then, for any $\delta > 0$, the Dirichlet series*

$$Z_{\mathcal{L}}(S(k); s) = \sum_{P \in S(k)} H_{\mathcal{L}}(P)^{-s} \qquad (s \in \mathbf{C})$$

converges absolutely and uniformly for $\mathrm{Re}(s) \geq \delta$.

Remark 4.7 Since the canonical bundle of S is torsion, the algebraic invariant $\alpha(\mathcal{L})$ of Batyrev-Manin [1] is zero. Since this corollary implies that the arithmetic invariant $\beta_S(\mathcal{L})$ is zero, Conjecture A of [1] holds in this case.

References

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

[2] E. Bombieri and D. Mumford, Enriques' classification of surfaces in char. p, Ⅱ, in Complex Analysis and Algebraic Geometry (W. L. Baily, Jr. and T. Shioda eds.), Iwanami Shoten, Publishers, Tokyo, and Cambridge Univ. Press, Cambridge, 1977.

[3] F. Enriques et F. Severi, Mémoire sur les surfaces hyperelliptiques, Acta Math. **32** (1909), 283–392; **33** (1910), 321–403.

[4] J. Franke, Yu. I. Manin and Yu. Tschinkel, Rational points of bounded height on Fano varieties, Invent. Math. **95** (1989), 421–435.

[5] S. Lang, Fundamentals of Diophantine geometry, Springer-Verlag, New York, 1983.

[6] Y. Morita, On rational points on algebraic surfaces, in Proc. of the 35-th Symposium on Algebra at Hokkaido Univ., 1989 (in Japanese).

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

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

[9] J. P. Serre, Lectures on the Mordell-Weil Theorem, Vieweg, Braunschweig, 1989.

[10] J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York, 1985.

[11] J. H. Silverman, The theory of height functions, in Arithmetic Geometry (G. Cornell and J. H. Silverman eds.), Springer-Verlag, New York, 1985.

Mathematical Institute
Faculty of Science
Tohoku University
Aoba, Sendai 980
Japan