Tôhoku Math. J.
46 (1994), 523–539

ON THE SOLUTIONS OF THUE EQUATIONS

MASAMI FUJIMORI

(Received July 5, 1993, revised January 20, 1994)

Abstract. Silverman's estimate for the number of integral points of the so-called Thue equation is improved in a certain special case. A sufficient condition for the non-existence of rational solutions is also given.

Introduction. Let $k/\boldsymbol{Q}$ be a finite extension, $p(X, Y) \in k[X, Y]$ a homogeneous polynomial of degree $n \geq 3$ with non-zero discriminant, and $a \in k^{\times} = k \setminus \{0\}$. Then the equation

$$p(X, Y) = aZ^n ,$$

which we call a Thue equation, defines a regular curve C^a in $\boldsymbol{P}_k^2$, which we call a Thue curve. Let J^a be the Jacobian variety of C^a.

First assume that a and the coefficients of $p(X, Y)$ are in the ring $\mathfrak{o}_k$ of integers in k.

Let $d = [k : \boldsymbol{Q}]$ and $R_a = \operatorname{rank} J^a(k)$. Silverman [9] proved the following among others:

THEOREM 0.1 (Silverman [9]). *There is a constant $G = G(k, p(X, Y))$ such that if $a \in \mathfrak{o}_k \setminus \{0\}$ satisfies $|N_{\boldsymbol{Q}}^k a| > G$ and $|1 + \rho_n(a)| \leq 9/4$, then*

$$\#\{(x, y) \in \mathfrak{o}_k^2 \,|\, p(x, y) = a\} < n^{2n^2}(12n^3 d)^{R_a} ,$$

where $\rho_n(a)$ is a number which measures the defect in a of the n-th power freeness and differs from $e(a)$ in Theorem 0.2 below by addition of the multiple of $1/\log|N_{\boldsymbol{Q}}^k \mathfrak{a}|$ by a constant depending only on k and n.

He mapped $C^a(k)$ to $J^a(k)$ and estimated the number of lattice points which lie in a ball of $J^a(k) \otimes_{\boldsymbol{Z}} \boldsymbol{R}$.

On the other hand, Mumford [7] had asserted that the heights of rational points on the Jacobian which come from a curve under a certain map grow exponentially if the genus is greater than 1.

We here try to count the integral points by the technique of Silverman and the method of Mumford and to improve the result of Silverman. Consider the prime ideal decomposition of $a\mathfrak{o}_k$. Collecting the factors appropriately, we get a unique factorization of the form $a\mathfrak{o}_k = \mathfrak{a}\mathfrak{b}^n$, where $\mathfrak{a}$ is an integral ideal not divisible by the n-th power of any

1991 *Mathematics Subject Classification.* Primary 11D41; Secondary 11G30.

prime ideal and $\mathfrak{b}$ is a fractional ideal.

THEOREM 0.2. *Let* $e(a)=n\log|N_{\boldsymbol{Q}}^k\mathfrak{b}|/\log|N_{\boldsymbol{Q}}^k\mathfrak{a}|$. *If* $n>3$, $p(X, Y)$ *has a linear factor in* $k[X, Y]$, $|1+e(a)|\leq 2$, *and* $|N_{\boldsymbol{Q}}^k a|$ *is sufficiently large, then we have*

$$\#\{(x, y)\in\mathfrak{o}_k^2\,|\,p(x, y)=a\}\leq 4\cdot 7^{R_a}\,.$$

In Theorem 5.4, we obtain the S-integer version of this theorem.

The following result is also relevant to what we consider in this paper:

THEOREM 0.3 (Bombieri and Schmidt [2]). *Assume that a and the coefficients of* $p(X, Y)$ *are in* $\boldsymbol{Z}$ *and that* $p(X, Y)$ *is irreducible in* $\boldsymbol{Z}[X, Y]$. *Then the number of primitive solutions (i.e., solutions in coprime integers in* $\boldsymbol{Z}$) *of the equation* $|p(x, y)|=a$ *does not exceed* $c_1\cdot n^{1+t}$, *where* c_1 *is an absolute constant and t is the number of prime factors of a. When n is greater than an absolute constant* c_2, *the number of primitive solutions (with* (x, y) *and* $(-x, -y)$ *regarded as the same) does not exceed* $215\cdot n^{1+t}$.

As for rational points, we find the following property:

From now on, a and the coefficients of $p(X, Y)$ are in k and may not be in $\mathfrak{o}_k$. Let μ_n be the set of n-th roots of unity in an algebraic closure of k. For $P=(x:y:1)\in C^a(k)$ and $\zeta\in\mu_n\cap k\setminus\{1\}$, we let $Q\in C^a(k)$ be the point $(x:y:\zeta)\in C^a(k)$. Then we have (cf. Proposition 6.4):

PROPOSITION 0.4. *Assume that* $n>3$ *and that* $p(X, Y)$ *has a linear factor in* $k[X, Y]$. *The angle that P and Q make in* $J^a(k)\otimes_{\boldsymbol{Z}}\boldsymbol{R}$ *under a certain map and by a certain metric is* $\cos^{-1}(-1/(n-1))$.

The proof depends on the calculation of the pull-back of an invertible sheaf and uses the global Néron pairing.

THEOREM 0.5. *Assume that* $n>3$ *and that* $p(X, Y)$ *has a linear factor in* $k[X, Y]$. *Then, except for a finite number of a* $\bmod (k^\times)^n$, *the assumption* $\operatorname{rank} J^a(k)<\min\{\#(\mu_n\cap k), n-1\}$ *implies*

$$\{(x, y)\in k^2\,|\,p(x, y)=a\}=\varnothing\,.$$

In fact this is an example to which [11, Theorem 1] is applicable. We show Theorem 0.5 directly. (The essence of the proof is the same as that in [11, Theorem 1].)

TERMINOLOGY AND NOTATION. Basically we use the terminology of [3].

Let $k/\boldsymbol{Q}$ be a finite extension, $d:=[k:\boldsymbol{Q}]$, $k^\times:=k\setminus\{0\}$, $N_{\boldsymbol{Q}}^k$ the norm function of numbers or ideals, $\bar{k}$ an algebraic closure of k, and μ_n the set of n-th roots of unity in $\bar{k}$.

Let $\boldsymbol{P}_k^\rho$ be the ρ-dimensional projective space over k. For a scheme X over k, $\bar{X}:=X\times_k\bar{k}$, $X(k):=\operatorname{Hom}(\operatorname{Spec} k, X)$, and $X(\bar{k}):=\operatorname{Hom}_k(\operatorname{Spec}\bar{k}, X)$. We do not distinguish an element of $X(k)$ and $\bar{X}(\bar{k})$ from the corresponding closed point of X and $\bar{X}$.

For a regular integral projective scheme V over k, we denote by $\operatorname{Div} V$ the group of Weil divisors on V and by $\operatorname{Pic} V$ the Picard group of V. For such a scheme V, the divisor class group and $\operatorname{Pic} V$ can be identified, so, sometimes we use the term *correspondence* to mean a certain type of invertible sheaf. For a non-zero function f on V, let $\operatorname{div}(f)$ be the divisor attached to f. For $D \in \operatorname{Div} V$, we denote by $\mathscr{L}(D)$ the invertible sheaf associated with D. When $\dim V = 1$, $\operatorname{Pic}^0 V$ denotes the subgroup of $\operatorname{Pic} V$ of degree 0. We often identify an invertible sheaf with its isomorphism class and use such an expression as $\mathscr{L}(D) \in \operatorname{Pic} V$. We use similar notation for regular integral projective schemes over $\bar{k}$. For a morphism f of schemes, let f^* be the pull-back functor of invertible sheaves.

Let $M_{\bar{k}}$ be the set of absolute values on $\bar{k}$ such that for an Archimedean $v \in M_{\bar{k}}$, the absolute value $|\cdot|_v$ is the usual one if restricted to $\boldsymbol{Q}$; for a non-Archimedean $v \in M_{\bar{k}}$, $|q|_v = 1/q$ for some prime $q \in \boldsymbol{Q}$. For a finite extension K of k, let $\sim_K$ be the equivalence relation on $M_{\bar{k}}$ so that $v \sim_K w$ if and only if $v|_K = w|_K$, and M_K the set of representatives of $M_{\bar{k}}/\sim_K$. Let K_v be the completion of K at $v \in M_{\bar{k}}$ and $\varepsilon_v^K := [K_v : \boldsymbol{Q}_v]/[K : \boldsymbol{Q}]$. The standard height h on $\boldsymbol{P}_k^\rho(\bar{k})$ is defined by

$$h((x_0 : \cdots : x_\rho)) = \sum_{v \in M_K} \varepsilon_v^K \log \max\{|x_0|_v, \ldots, |x_\rho|_v\}$$

for a finite extension K of k and $x_0, \ldots, x_\rho \in K$. We also denote by h the height on k defined by

$$h(x) = h((1 : x))$$

for $x \in k$. Let M_k^∞ be the subset of Archimedean absolute values of M_k. For a finite subset S of M_k containing M_k^∞, we denote by $\mathfrak{o}_S$ (resp. $\mathfrak{o}_S^\times$) the ring of S-integers (resp. the units of $\mathfrak{o}_S$).

1. Thue curves, twisting and the compatibility between heights. Let $k/\boldsymbol{Q}$ be a finite extension, $p(X, Y) \in k[X, Y]$ a homogeneous polynomial of degree $n > 3$ with non-zero discriminant and with a *linear factor* l in $k[X, Y]$, and $a \in k^\times$. Let C^a be the closed subscheme of $\boldsymbol{P}_k^2$ defined by

$$p(X, Y) = aZ^n .$$

Notice that the sheaf $\Omega_{C^a/k}$ of (holomorphic) differential forms of C^a over k is invertible, because $\overline{C^a}$ is a nonsingular curve (cf. [3, III. 10.2 and 10.0.2]). Let $Q^a \in C^a(k)$ be the point defined by $l(X, Y) = Z = 0$. Let D^a be the divisor $C^a \cap \{Z = 0\}$ on C^a.

LEMMA 1.1 (cf. [9, Lemma 4(a)]). *The divisor $(n-3)D^a$ is a canonical divisor on C^a.*

Let J^a be the Jacobian variety of C^a. We embed C^a in J^a. We refer the reader to [6] for details concerning relevant properties of the Jacobian varieties.

Let $\mathscr{M}^a \in \operatorname{Pic}(C^a \times_k J^a)$ be the universal divisorial correspondence between (C^a, Q^a)

and J^a. Let Δ^a be the diagonal divisor on $C^a \times_k C^a$ and

$$\mathscr{L}^a := \mathscr{L}(\Delta^a - \{Q^a\} \times_k C^a - C^a \times_k \{Q^a\}) \in \mathrm{Pic}(C^a \times_k C^a) .$$

Since $\mathscr{L}^a$ is a divisorial correspondence between (C^a, Q^a) and itself, there exists a unique morphism $f^a\colon C^a \to J^a$ such that $f^a(Q^a)=0$ and $\mathscr{L}^a \simeq (1_{C^a} \times f^a)^* \mathscr{M}^a$. We have a natural group isomorphism

$$J^a(\bar{k}) \simeq \mathrm{Pic}^0(\overline{C^a}) , \qquad \mathscr{L} \mapsto (1_{C^a} \times \mathscr{L})^* \mathscr{M}^a ,$$

through which we identify these two groups. Then we have

$$f^a(Q) = (1_{C^a} \times f^a(Q))^* \mathscr{M}^a = (1_{C^a} \times Q)^* \mathscr{L}^a = \mathscr{L}(Q - Q^a) \in \mathrm{Pic}^0(\overline{C^a})$$

for $Q \in C^a(\bar{k})$.

Let $\pi_a\colon \overline{C^a} \times \overline{J^a} \to C^a \times_k J^a$ be the projection map. We also note that $\pi_a^* \mathscr{M}^a$ is the universal divisorial correspondence between $(\overline{C^a}, Q^a)$ and $\overline{J^a}$, and that $\overline{J^a}$ is the Jacobian variety of $\overline{C^a}$.

Let g be the genus of C^a, which is equal to $(n-1)(n-2)/2$, and Θ^a the prime divisor on J^a obtained by the $(g-1)$-fold addition of C^a, i.e.,

$$\Theta^a(\bar{k}) = \{ f^a(Q_1) + \cdots + f^a(Q_{g-1}) \mid Q_1, \ldots, Q_{g-1} \in C^a(\bar{k}) \} .$$

Let $s_a, p_a, q_a\colon J^a \times_k J^a \to J^a$ be the sum, the projections onto the first and the second factors, respectively,

$$\mathscr{N}^a := s_a^* \mathscr{L}(\Theta^a) \otimes p_a^* \mathscr{L}(\Theta^a)^{-1} \otimes q_a^* \mathscr{L}(\Theta^a)^{-1} \in \mathrm{Pic}(J^a \times_k J^a) ,$$

and $B_a\colon J^a(\bar{k}) \times J^a(\bar{k}) \to \boldsymbol{R}$ the canonical height on $J^a \times_k J^a$ attached to $\mathscr{N}^a$. B_a is a symmetric bilinear form on $J^a(\bar{k}) \times J^a(\bar{k})$ and positive definite on $J^a(\bar{k})$ modulo torsion (cf. [7, Proposition 1]).

Let α be an element of $\bar{k}$ such that $\alpha^n = a$, and $\phi\colon \overline{C^a} \to \overline{C^1}$ the isomorphism given by $(x:y:z) \mapsto (x:y:\alpha z)$. We see that $\phi(Q^a) = Q^1$.

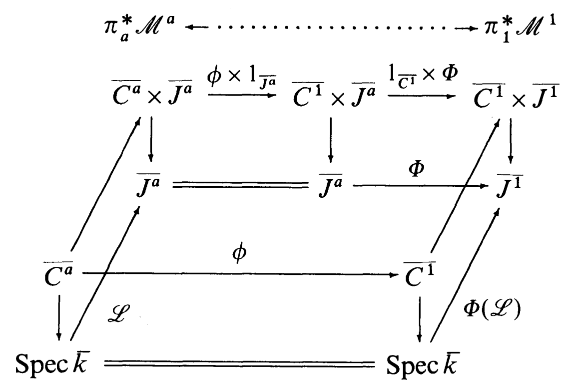
Since $(\phi^{-1} \times 1_{\overline{J^a}})^* \pi_a^* \mathscr{M}^a \in \mathrm{Pic}(\overline{C^1} \times \overline{J^a})$ is a divisorial correspondence between $(\overline{C^1}, Q^1)$ and $\overline{J^a}$, by the universality of $\pi_1^* \mathscr{M}^1$, there exists a unique isomorphism $\Phi\colon \overline{J^a} \to \overline{J^1}$ such that $\Phi(0)=0$ and

$$(\phi^{-1} \times 1_{\overline{J^a}})^* \pi_a^* \mathscr{M}^a \simeq (1_{\overline{C^1}} \times \Phi)^* \pi_1^* \mathscr{M}^1 .$$

Figure shows the relation among the maps. Because $\Phi(0)=0$, Φ is an isomorphism of abelian varieties (cf. [5, 2.2]), i.e., the diagram

$$\begin{array}{ccc} \overline{J^a} \times \overline{J^a} & \xrightarrow{s_a \times 1_{\bar{k}}} & \overline{J^a} \\ {\scriptstyle \Phi \times \Phi} \downarrow & & \downarrow {\scriptstyle \Phi} \\ \overline{J^1} \times \overline{J^1} & \xrightarrow{s_1 \times 1_{\bar{k}}} & \overline{J^1} \end{array}$$

is commutative. If we use the identification $J^a(\bar{k}) \simeq \mathrm{Pic}^0(\overline{C^a})$, we see by Figure that



FIGURE

$$\Phi(\mathscr{L})=(\phi^{-1})^*\mathscr{L}\in \mathrm{Pic}^0(\overline{C^1})$$

for $\mathscr{L}\in \mathrm{Pic}^0(\overline{C^a})$. In particular, we have

$$\Phi(f^a(Q))=(\phi^{-1})^*\mathscr{L}(Q-Q^a)=\mathscr{L}(\phi(Q)-Q^1)=f^1(\phi(Q))$$

for any closed point $Q\in C^a(\bar{k})$. Since $\overline{C^a}$ and $\overline{J^1}$ are varieties, the morphisms are completely determined by their effect on $C^a(\bar{k})$. So we have $\Phi\circ f^a=f^1\circ\phi$, i.e., the diagram

$$\begin{tikzcd}
\overline{C^a} \arrow[r, "f^a\times 1_{\bar{k}}"] \arrow[d, "\phi"'] & \overline{J^a} \arrow[d, "\Phi"] \\
\overline{C^1} \arrow[r, "f^1\times 1_{\bar{k}}"] & \overline{J^1}
\end{tikzcd}$$

is commutative.

Let $\varpi_a:\overline{J^a}\times\overline{J^a}\to J^a\times_k J^a$ be the projection map. From the above discussion, we see easily that

$$\varpi_a^*\mathscr{N}^a=(\Phi\times\Phi)^*\varpi_1^*\mathscr{N}^1 .$$

Therefore, by the functoriality of heights and the uniqueness of the canonical height, we have

$$B_a(\mathscr{L},\mathscr{M})=B_1(\Phi(\mathscr{L}),\Phi(\mathscr{M}))$$

for $\mathscr{L},\mathscr{M}\in J^a(\bar{k})$.

2. Relations among heights and a basic inequality. Choose a height h_a on C^a corresponding to $\mathscr{L}(Q^a)\in \mathrm{Pic}(C^a)$, where Q^a is the k-rational point on C^a defined by $l(X, Y)=Z=0$ (cf. §1). For $Q\in C^a(\bar{k})$, we denote by $h(Q)$ the height induced by the natural embedding $C^a\subset \boldsymbol{P}_k^2$. Since $D^a=C^a\cap\{Z=0\}$ is a hyperplane section, h corresponds to $\mathscr{L}(D^a)$.

LEMMA 2.1. *We have $h_a(Q)=n^{-1}h(Q)+O(1)$ for $Q\in C^a(\bar{k})$, where $n=\deg p(X, Y)$.*

PROOF. Since $\operatorname{div}(l(X, Y)/Z)=n\cdot Q^a-D^a\in \operatorname{Div}(C^a)$, we see that $\mathscr{L}(nQ^a)\simeq\mathscr{L}(D^a)$, which leads to the above relation between the heights h_a and h. q.e.d.

LEMMA 2.2. *We have $B_a(f^aQ, f^aQ)=(n-1)(n-2)n^{-1}h(Q)+O(1)$ for $Q\in C^a(\bar{k})$, where B_a is the height on $J^a\times_k J^a$ given in § 1 and $f^a: C^a\to J^a$ the map as in § 1.*

PROOF. Let $j: C^a\to C^a\times_k C^a$ be the diagonal map. Note that in general, for a non-singular curve C over k, the pull-back of the diagonal divisor on $C\times_k C$ by the diagonal map is the inverse of a canonical divisor. Since $\mathscr{L}((n-3)D^a)$ is the canonical sheaf (cf. Lemma 1.1), we see that $j^*\mathscr{L}(\Delta^a)\simeq\mathscr{L}(-(n-3)D^a)$. Hence we have

$$j^*\mathscr{L}^a=j^*\mathscr{L}(\Delta^a-\{Q^a\}\times_k C^a-C^a\times_k\{Q^a\})\simeq\mathscr{L}(-(n-3)D^a-2Q^a)\,.$$

On the other hand, we know that $\mathscr{M}^a\simeq((f^a\times 1_{J^a})^*\mathscr{N}^a)^{-1}$ (cf. [6, 6.11] or [7, § 2]) and $\mathscr{L}^a\simeq(1_{C^a}\times f^a)^*\mathscr{M}^a$ (cf. § 1). Therefore we have

$$\begin{aligned}j^*(f^a\times f^a)^*\mathscr{N}^a&=j^*(1_{C^a}\times f^a)^*(f^a\times 1_{J^a})^*\mathscr{N}^a\simeq j^*(1_{C^a}\times f^a)^*(\mathscr{M}^a)^{-1}\\&\simeq j^*(\mathscr{L}^a)^{-1}\simeq\mathscr{L}((n-3)D^a+2Q^a)\,.\end{aligned}$$

Since the height $B_a(f^aQ, f^aQ)$ for $Q\in C^a(\bar{k})$ corresponds to $j^*(f^a\times f^a)^*\mathscr{N}^a$ by the functoriality of heights while h corresponds to $\mathscr{L}(D^a)$, we obtain

$$B_a(f^aQ, f^aQ)=(n-3)h(Q)+2h_a(Q)+O(1)$$

for $Q\in C^a(\bar{k})$. By Lemma 2.1, we have the desired equation. q.e.d.

Let X^a be the $\boldsymbol{R}$-vector space $J^a(k)\otimes_{\boldsymbol{Z}}\boldsymbol{R}$ and $\langle\cdot,\cdot\rangle$ the bilinear form on $X^a\times X^a$ induced by B_a. Let $\|\cdot\|$ be the associated norm and $\psi^a: C^a(k)\to X^a$ the map defined by $Q\mapsto f^aQ\otimes 1$.

From Lemma 2.2, we obtain a relation between the norm $\|\cdot\|$ on X^a and the standard height h on $\boldsymbol{P}_k^2(\bar{k})$ for $Q\in C^a(k)$:

PROPOSITION 2.3. *There exist non-negative constants $m=m(C^1)$ and $M=M(C^1)$ such that*

$$-m\le\|\psi^aQ\|^2-\frac{(n-1)(n-2)}{n}h(\phi Q)\le M$$

for $Q\in C^a(k)$, where $n=\deg p(X, Y)$ and $\phi:\overline{C^a}\to\overline{C^1}$ is the twisting in § 1.

PROOF. By Lemma 2.2, there exist non-negative constants $m=m(C^1)$ and $M=M(C^1)$ such that

$$-m\le B_1(f^1P, f^1P)-\frac{(n-1)(n-2)}{n}h(P)\le M$$

for $P\in C^1(\bar{k})$. Take $P=\phi Q$ for $Q\in C^a(k)$. Using the commutativity $f^1\circ\phi=\Phi\circ f^a$ and the compatibility $B_1(\Phi\cdot,\Phi\cdot)=B_a(\cdot,\cdot)$ (cf. § 1), we have

$$-m\leq B_a(f^aQ, f^aQ)-\frac{(n-1)(n-2)}{n}h(\phi Q)\leq M,$$

which are equivalent to the above inequalities. q.e.d.

The next lemma is the inequality of Mumford in our case, and follows from Lemmas 2.1 and 2.2 as well as the results in [7, § 3].

LEMMA 2.4. *There exists a positive constant $L=L(C^1)$ such that*

$$B_1(f^1P, f^1Q)\leq\frac{1}{2g}\{B_1(f^1P, f^1P)+B_1(f^1Q, f^1Q)\}+L$$

for $P, Q\in C^1(\bar{k})$ with $P\neq Q$, where $g=(n-1)(n-2)/2$.

As a consequence, we obtain:

LEMMA 2.5. *For $P, Q\in C^a(k)$ with $P\neq Q$, we have*

$$\langle\psi^aP, \psi^aQ\rangle\leq\frac{1}{2g}(\|\psi^aP\|^2+\|\psi^aQ\|^2)+L,$$

where L is the constant in Lemma 2.4.

PROOF. By Lemma 2.4 applied to ϕP and ϕQ for $P, Q\in C^a(k)$ with $P\neq Q$, we have

$$B_1(f^1(\phi(P)), f^1(\phi(Q)))\leq\frac{1}{2g}\{B_1(f^1(\phi(P)), f^1(\phi(P)))+B_1(f^1(\phi(Q)), f^1(\phi(Q)))\}+L.$$

From the equalities $B_a(\cdot,\cdot)=B_1(\Phi\cdot,\Phi\cdot)$ and $\Phi\circ f^a=f^1\circ\phi$, we see that

$$\begin{aligned}B_a(f^aP, f^aQ)&=B_1(\Phi(f^a(P)), \Phi(f^a(Q)))\\&\leq\frac{1}{2g}\{B_1(\Phi(f^a(P)), \Phi(f^a(P)))+B_1(\Phi(f^a(Q)), \Phi(f^a(Q)))\}+L\\&=\frac{1}{2g}\{B_a(f^a(P), f^a(P))+B_a(f^a(Q), f^a(Q))\}+L.\end{aligned}$$

By the definitions of $\langle\cdot,\cdot\rangle$ and $\|\cdot\|$, we are done. q.e.d.

Lemma 2.5 implies the following, where we let $\cos(v, w)=\langle v, w\rangle/\|v\|\,\|w\|$ for $v, w\in X^a$:

PROPOSITION 2.6. *Let $P, Q\in C^a(k)$ be distinct points such that $\|\psi^aP\|\leq\|\psi^aQ\|$. If*

$$\|\psi^aP\|^2\geq 20(n-2)^{1/2}L$$

for the constant L in Lemma 2.4 *and*

$$\cos(\psi^a P, \psi^a Q) \geq \frac{21}{20(n-2)^{1/2}},$$

then we have

$$\|\psi^a Q\| \geq \frac{g}{(n-2)^{1/2}} \|\psi^a P\| .$$

In other words, if a rational point $P \in C^a(k)$ *with large norm appears in a cone* V *of* X^a *such that* $\cos(v, w) \geq 21/(20(n-2)^{1/2})$ *for* $v, w \in V$, *then another rational point* $Q \in C^a(k)$ *with the next smallest norm which appears in* V, *if any, has the norm at least* $g/(n-2)^{1/2}$*-times the norm of* P.

PROOF. By the above lemma, we see that

$$\frac{21}{20(n-2)^{1/2}} \leq \cos(\psi^a P, \psi^a Q) = \frac{\langle \psi^a P, \psi^a Q \rangle}{\|\psi^a P\| \, \|\psi^a Q\|} \leq \frac{1}{2g}\left(\frac{\|\psi^a P\|}{\|\psi^a Q\|} + \frac{\|\psi^a Q\|}{\|\psi^a P\|}\right) + \frac{L}{\|\psi^a P\| \, \|\psi^a Q\|} .$$

From the assumptions $\|\psi^a Q\|^2 \geq \|\psi^a P\|^2 \geq 20(n-2)^{1/2} L$, we have

$$\frac{21}{20(n-2)^{1/2}} \leq \frac{1}{g} \frac{\|\psi^a Q\|}{\|\psi^a P\|} + \frac{1}{20(n-2)^{1/2}} .$$

q.e.d.

3. Estimates for the heights of integral or rational points. Fix a number λ such that $2 < \lambda < n = \deg p(X, Y)$, where $p(X, Y)$ is the homogeneous polynomial defining C^a (cf. § 1). Recall that we have defined h as the standard height on a projective space or as the height function on k.

LEMMA 3.1 (cf. [9, Theorem 1]). *When the coefficients of* $p(X, Y)$ *are in* $\mathfrak{o}_S$, *there exists a constant* $c = c(k, S, p(X, Y), \lambda)$ *such that*

$$h((x : y : 1)) < \frac{1}{n-\lambda} h(p(x, y)) + c$$

for $x, y \in \mathfrak{o}_S$.

The next lemma is the S-integer version of [9, Proposition 2(b)]. The proof is similar to the original one.

LEMMA 3.2. *There exists a constant* c_k *depending only on* k *and satisfying the following property: for any* $a \in \mathfrak{o}_S \setminus \{0\}$, *there exists* $u \in \mathfrak{o}_S^\times$ *such that*

$$h(au^n) < \left| \frac{1}{d} \log | N_{\mathbf{Q}}^k a | + \sum_{v \in S \setminus M_k^\infty} \varepsilon_v^k \log | a |_v \right| + c_k \cdot n ,$$

where $d=[k:\boldsymbol{Q}]$ *and* $\varepsilon_v^k=[k_v:\boldsymbol{Q}_v]/[k:\boldsymbol{Q}]$.

We will use these two lemmas to bound the heights of integral points from above.

A version of [10, Theorem 2] which fits our aim is as follows, and can be proved similarly.

LEMMA 3.3. *For a closed point* $Q\in\boldsymbol{P}_k^\rho$, *let* $K=k(Q)$ *be the field of definition for* Q, *i.e., the residue field of the local ring at* Q, *and* D_k^K *the discriminant ideal. Then, if* $\delta=[K:k]>1$, *we have*

$$h(Q)\geq\frac{1}{2}\cdot\frac{1}{\delta-1}\left(\frac{1}{\delta d}\log|N_{\boldsymbol{Q}}^k D_k^K|-\log\delta\right),$$

where h *is the standard height on* $\boldsymbol{P}_k^\rho$ *and* $d=[k:\boldsymbol{Q}]$.

We use this lemma to estimate the heights of rational points from below.

4. Estimates from below. Recall that n is the degree of the homogeneous polynomial $p(X, Y)$ defining C^a (cf. §1). Let $a\mathfrak{o}_k=\prod_{\mathfrak{p}}\mathfrak{p}^b$ be the prime ideal decomposition of the fractional ideal $a\mathfrak{o}_k$. If $b=r+qn$ for $r, q\in\boldsymbol{Z}$ with $0\leq r<n$, then we can so arrange that $a\mathfrak{o}_k=\prod_{\mathfrak{p}}\mathfrak{p}^r(\prod_{\mathfrak{p}}\mathfrak{p}^q)^n$. Put $\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^r$ and $\mathfrak{b}=\prod_{\mathfrak{p}}\mathfrak{p}^q$. Then $a\mathfrak{o}_k=\mathfrak{a}\mathfrak{b}^n$ and $\mathfrak{a}$ is integral n-th power-free. We see easily that such a decomposition is unique.

There is a lower bound for the norms of k-rational points on C^a:

PROPOSITION 4.1. *For* $Q\in C^a(k)$ *such that the Z-coordinate is not zero, we have*

$$\|\psi^a Q\|^2\geq\frac{1}{2dn^2}\frac{n-2}{n-1}\log|N_{\boldsymbol{Q}}^k\mathfrak{a}|-\frac{\log 2}{2}\frac{(n-1)(n-2)}{n}-m,$$

where $\|\cdot\|$ *is the norm on* $X^a=J^a(k)\otimes_{\boldsymbol{Z}}\boldsymbol{R}$ *in* §2, $\psi^a: C^a(k)\to X^a$ *is the map given by* $Q\mapsto f^aQ\otimes 1$, $d=[k:\boldsymbol{Q}]$, *and* m *is the constant in Proposition* 2.3.

PROOF. We see from Proposition 2.3 that

$$\|\psi^a Q\|^2\geq\frac{(n-1)(n-2)}{n}h(\phi Q)-m.$$

Since the Z-coordinate of Q is not zero and $\phi:\overline{C^a}\to\overline{C^1}$ was defined as $(x:y:z)\mapsto(x:y:\alpha z)$ (cf. §1), we have $k(\phi Q)=k(\alpha)$, where $k(\phi Q)$ is the field of definition for ϕQ. Then, if $\delta=[k(\alpha):k]>1$, we find from Lemma 3.3 and the fact $2\leq\delta\leq n$ that

$$\begin{aligned}\|\psi^a Q\|^2&\geq\frac{(n-1)(n-2)}{2(\delta-1)\delta dn}\log|N_{\boldsymbol{Q}}^k D_k^{k(\alpha)}|-\frac{\log\delta}{2(\delta-1)}\frac{(n-1)(n-2)}{n}-m\\&\geq\frac{n-2}{2dn^2}\log|N_{\boldsymbol{Q}}^k D_k^{k(\alpha)}|-\frac{\log 2}{2}\frac{(n-1)(n-2)}{n}-m.\end{aligned}$$

The right hand side of the last inequality is negative if $k(\alpha)=k$, because we then have $|N_{\boldsymbol{Q}}^{k}D_{k}^{k(\alpha)}|=1$. Hence this inequality is valid also when $\delta=1$. If we look at the ramification in $k(\alpha)/k$, then we find $\mathfrak{a}\,|\,(D_{k}^{k(\alpha)})^{n-1}$. Thus $|N_{\boldsymbol{Q}}^{k}D_{k}^{k(\alpha)}|^{n-1}\geq|N_{\boldsymbol{Q}}^{k}\mathfrak{a}|$. q.e.d.

This means in particular that if $|N_{\boldsymbol{Q}}^{k}\mathfrak{a}|$ is sufficiently large, then $f^{a}Q$ is not a torsion point on $J^{a}(k)$ for $Q\in C^{a}(k)\setminus\{Z=0\}$.

5. Distribution of integral points. In this section, we assume that a and the coefficients of $p(X, Y)$ are in $\mathfrak{o}_{S}$.

Let $I_{S}^{a}:=\{(x, y)\in\mathfrak{o}_{S}^{2}\,|\,p(x, y)=a\}$, $a\mathfrak{o}_{k}=\mathfrak{a}\mathfrak{b}^{n}$ the ideal decomposition as in §4, and

$$e(a):=\frac{n\log|N_{\boldsymbol{Q}}^{k}\mathfrak{b}|+d\sum_{v\in S\setminus M_{k}^{\infty}}\varepsilon_{v}^{k}\log|a|_{v}}{\log|N_{\boldsymbol{Q}}^{k}\mathfrak{a}|},$$

where $n=\deg p(X, Y)$ and $d=[k:\boldsymbol{Q}]$. We regard I_{S}^{a} as a subset of $C^{a}(k)$.

Choose a number λ such that $2<\lambda<n$. We have defined a map $\psi^{a}\colon C^{a}(k)\to X^{a}=J^{a}(k)\otimes_{\boldsymbol{Z}}\boldsymbol{R}$ and a norm $\|\cdot\|$ on X^{a} in §2. We now bound the norms of S-integral points from above. This means in particular that I_{S}^{a} is a finite set, which can already be seen from Lemma 3.1.

LEMMA 5.1. *If $Q\in I_{S}^{a}\subset C^{a}(k)$, then the Z-coordinate of Q is not zero and*

$$\|\psi^{a}Q\|^{2}<\left(\frac{(n-1)(n-2)}{n^{2}}+\frac{(n-1)(n-2)}{(n-\lambda)n}\right)\frac{|1+e(a)|}{d}\log|N_{\boldsymbol{Q}}^{k}\mathfrak{a}|$$
$$+\left(\frac{(n-1)(n-2)}{n}+\frac{(n-1)(n-2)}{n-\lambda}\right)c_{k}+\frac{(n-1)(n-2)}{n}\cdot c+M\,,$$

where c_{k}, $c=c(k, S, p(X, Y), \lambda)$ and M are the constants in Lemmas 3.2 and 3.1 as well as Proposition 2.3, respectively.

PROOF. Note first that for $v\in M_{\bar{k}}$ and $x, y, z, \alpha\in\bar{k}$, we have

$$\max\{|x|_{v}, |y|_{v}, |\alpha z|_{v}\}\leq\max\{|1|_{v}, |\alpha^{n}|_{v}\}^{1/n}\cdot\max\{|x|_{v}, |y|_{v}, |z|_{v}\}\,.$$

If we use this for $Q=(x:y:z)$ and α in §1 and take the logarithms of both sides, then we see that

$$h(\phi Q)\leq\frac{1}{n}h(a)+h(Q)\,. \tag{1}$$

To the second inequality

$$\|\psi^{a}Q\|^{2}\leq\frac{(n-1)(n-2)}{n}h(\phi Q)+M$$

of Proposition 2.3 we apply the inequality (1) and Lemma 3.1, and we obtain

$$\|\psi^a Q\|^2 < \left(\frac{(n-1)(n-2)}{n^2} + \frac{(n-1)(n-2)}{(n-\lambda)n}\right) h(a) + \frac{(n-1)(n-2)}{n} \cdot c + M\,.$$

Now, for an arbitrary $u \in \mathfrak{o}_S^\times$, let $\chi: C^a \to C^{au^n}$ be given by $(x:y:z) \mapsto (x:y:u^{-1}z)$. Then we see that $\chi(I_S^a) = I_S^{au^n}$. In the same way as in the case of $\phi: C^a \to C^1$, we have

$$\|\psi^a P\|^2 = B_a(f^a P, f^a P) = B_{au^n}(f^{au^n}\chi P, f^{au^n}\chi P) = \|\psi^{au^n}\chi P\|^2$$

for $P \in C^a(k)$, hence

$$\|\psi^a Q\|^2 \le \left(\frac{(n-1)(n-2)}{n^2} + \frac{(n-1)(n-2)}{(n-\lambda)n}\right) \inf_{u \in \mathfrak{o}_S^\times} h(au^n) + \frac{(n-1)(n-2)}{n} \cdot c + M\,.$$

By Lemma 3.2, we see that

$$\|\psi^a Q\|^2 < \left(\frac{(n-1)(n-2)}{n^2} + \frac{(n-1)(n-2)}{(n-\lambda)n}\right) \left| \frac{1}{d} \log |N_{\mathbf{Q}}^k a| + \sum_{v \in S \setminus M_k^\infty} \varepsilon_v^k \log |a|_v \right|$$
$$+ \left(\frac{(n-1)(n-2)}{n} + \frac{(n-1)(n-2)}{n-\lambda}\right) c_k + \frac{(n-1)(n-2)}{n} \cdot c + M\,.$$

By the definition of e, we are done. q.e.d.

Let V be a cone of X^a such that $\cos(v, w) \ge 21/(20(n-2)^{1/2})$ for $v, w \in V$.

Lemma 5.2. *Let $t = \#(I_S^a \cap (\psi^a)^{-1} V) - 1$ and assume $t \ge 0$. If $|N_{\mathbf{Q}}^k \mathfrak{a}|$ is sufficiently large, then we have*

$$\left(\frac{(n-1)^2(n-2)}{4}\right)^t < 4(1 + |1 + e(a)|)\left(1 + \frac{n}{n-\lambda}\right)(n-1)^2\,.$$

Proof. Let $I_S^a \cap (\psi^a)^{-1} V = \{Q^{(0)}, Q^{(1)}, \ldots, Q^{(t)}\}$ and $\|\psi^a Q^{(0)}\| \le \|\psi^a Q^{(1)}\| \le \cdots \le \|\psi^a Q^{(t)}\|$. When

$$\log |N_{\mathbf{Q}}^k \mathfrak{a}| \ge 2dn^2 \frac{n-1}{n-2}\left(\frac{\log 2}{2} \frac{(n-1)(n-2)}{n} + m + 20(n-2)^{1/2} L\right),$$

we see by Proposition 4.1 that $\|\psi^a Q^{(i)}\|^2 \ge 20(n-2)^{1/2} L$ for any i. So, by Proposition 2.6, we have

$$\left(\frac{g^2}{n-2}\right)^t \cdot \|\psi^a Q^{(0)}\|^2 \le \left(\frac{g^2}{n-2}\right)^{t-1} \cdot \|\psi^a Q^{(1)}\|^2 \le \cdots \le \|\psi^a Q^{(t)}\|^2\,.$$

Applying Lemma 5.1 to the extreme right-hand side and again Proposition 4.1 to the extreme left-hand side, we find

$$\left(\frac{g^2}{n-2}\right)^t < \left[\left(\frac{(n-1)(n-2)}{n^2} + \frac{(n-1)(n-2)}{(n-\lambda)n}\right) \frac{|1 + e(a)|}{d} \log |N_{\mathbf{Q}}^k \mathfrak{a}|\right.$$

$$+\left(\frac{(n-1)(n-2)}{n}+\frac{(n-1)(n-2)}{n-\lambda}\right)c_k+\frac{(n-1)(n-2)}{n}c+M\Bigg]$$

$$\cdot\left[\frac{1}{2dn^2}\frac{n-2}{n-1}\log|N_{\boldsymbol{Q}}^k\mathfrak{a}|-\frac{\log 2}{2}\frac{(n-1)(n-2)}{n}-m\right]^{-1}.$$

Further if

$$\log|N_{\boldsymbol{Q}}^k\mathfrak{a}|\geq\max\left\{\left[\left(\frac{(n-1)(n-2)}{n}+\frac{(n-1)(n-2)}{n-\lambda}\right)c_k+\frac{(n-1)(n-2)}{n}c+M\right]\right.$$

$$\cdot\left[\left(\frac{(n-1)(n-2)}{n^2}+\frac{(n-1)(n-2)}{(n-\lambda)n}\right)\frac{1}{d}\right]^{-1},$$

$$\left.\left[\frac{\log 2}{2}\frac{(n-1)(n-2)}{n}+m\right]\left[\frac{1}{4dn^2}\frac{n-2}{n-1}\right]^{-1}\right\},$$

then, substituting $(n-1)(n-2)/2$ for g and estimating the right hand side of the above inequality, we obtain

$$\left(\frac{(n-1)^2(n-2)}{4}\right)^t<\left(\frac{(n-1)(n-2)}{n^2}+\frac{(n-1)(n-2)}{(n-\lambda)n}\right)\frac{|1+e(a)|+1}{d}\cdot 4dn^2\frac{n-1}{n-2}$$

$$=4\left((n-1)^2+\frac{(n-1)^2n}{n-\lambda}\right)(|1+e(a)|+1).$$

q.e.d.

Silverman [9] estimated the number of lattice points in a ball of $X^a=J^a(k)\otimes_{\boldsymbol{Z}}\boldsymbol{R}$ centered at the origin. Here, using Lemma 5.2, we bound the number of points in a cone of X^a which come from S-integral points.

LEMMA 5.3. *Let V be a cone as above. If $|1+e(a)|\leq 2$ and $|N_{\boldsymbol{Q}}^k\mathfrak{a}|$ is sufficiently large, then*

$$\#(I_S^a\cap(\psi^a)^{-1}V)\leq\begin{cases}1 & \text{for } n\geq 194\\ 2 & \text{for } n\geq 7\\ 3 & \text{for } n\geq 5\\ 4 & \text{for } n\geq 4.\end{cases}$$

PROOF. In Lemma 5.2, take $\lambda=2n/3$ when $n\geq 5$; $\lambda=5/2$, $n=4$. q.e.d.

Summing up, we have:

THEOREM 5.4. *If $|1+e(a)|\leq 2$ and $|N_{\boldsymbol{Q}}^k\mathfrak{a}|$ is sufficiently large, then*

$$\# I_S^a\leq 4\cdot 7^{R_a},$$

where $R_a = \operatorname{rank} J^a(k)$.

PROOF. Notice that $21/(20(n-2)^{1/2}) < 3/4$, because $n > 3$. We know that $\boldsymbol{R}^\rho$ can be covered by 7^ρ cones V such that $\cos(v, w) > 3/4$ for $v, w \in V$ (cf. [1, § 10]), hence, by Lemma 5.3, we obtain the result. q.e.d.

6. The angle made by two rational points in a special relation. Let $\mu_n = \{\zeta_1 = 1, \zeta_2, \ldots, \zeta_n\}$ be the set of n-th roots of unity in $\bar{k}$, where $n = \deg p(X, Y)$ (cf. § 1). For $P = (x:y:z) \in C^a(\bar{k})$ and $\zeta_i \in \mu_n$, we denote by P_i the point $(x:y:\zeta_i z) \in C^a(\bar{k})$. These points turn out to be *linearly dependent*:

PROPOSITION 6.1. *When $\mu_n \subset k$, we have for $P \in C^a(k)$*

$$\sum_{1 \le i \le n} \psi^a P_i = 0 \in X^a = J^a(k) \otimes_{\mathbf{Z}} \boldsymbol{R},$$

where $\psi^a \colon C^a(k) \to X^a$ is the map given by $Q \mapsto f^a Q \otimes 1$ (cf. § 2).

PROOF. For $P = (x:y:z) \in C^a(k)$ with $x, y, z \in k$, we have $\operatorname{div}((yX - xY)/l(X, Y)) = \sum P_i - nQ^a \in \operatorname{Div}(C^a)$. Hence, if we use the identification $J^a(k) \simeq \operatorname{Pic}^0(C^a)$, we see (cf. § 1) that

$$\sum_i f^a P_i = \bigotimes_i \mathscr{L}(P_i - Q^a) = \mathscr{L}(\sum_i P_i - nQ^a) = 0 \in J^a(k).$$

Passing to X^a, we obtain the above relation. q.e.d.

Note, however, that $n-1$ of them are independent. We see below the *angle* made by two of them (cf. Proposition 6.4). For the proof, we need a lemma.

For $\zeta_i \in \mu_n$, let $j_i \colon \overline{C^a} \to \overline{C^a} \times \overline{C^a}$ be the map defined by

$$(x:y:z) \mapsto ((x:y:\zeta_i z), (x:y:z))$$

and $\overline{\Delta^a}$ the diagonal divisor on $\overline{C^a} \times \overline{C^a}$.

LEMMA 6.2. *For $i \ne 1$, we have*

$$j_i^* \mathscr{L}(\overline{\Delta^a}) = \mathscr{L}(\overline{D^a}),$$

where $\overline{D^a} = \overline{C^a} \cap \{Z = 0\} \in \operatorname{Div}(\overline{C^a})$.

PROOF. Let X_1, Y_1, Z_1, X_2, Y_2, Z_2 be the natural homogeneous coordinates in $\overline{C^a} \times \overline{C^a}$. We first see that $Z_1/X_1 - Z_2/X_2$ is a generator of the prime ideal of the local ring of $\overline{C^a} \times \overline{C^a}$ at $(P, P) = ((1:y:0), (1:y:0)) \in \overline{\Delta^a} \cap \{Z_1 = Z_2 = 0, X_1 X_2 \ne 0\}$ corresponding to $\overline{\Delta^a}$. Indeed, the ring of sections of the structure sheaf over the affine open set $\{X_1 X_2 \ne 0\}$ is

$$\bar{k}[Y_1/X_1, Z_1/X_1]/(p(1, Y_1/X_1) - a\cdot(Z_1/X_1)^n) \otimes_{\bar{k}} \bar{k}[Y_2/X_2, Z_2/X_2]/(p(1, Y_2/X_2) - a\cdot(Z_2/X_2)^n),$$

and the prime ideal of this ring corresponding to $\overline{\Delta^a}$ is

$$(Y_1/X_1 - Y_2/X_2, Z_1/X_1 - Z_2/X_2).$$

There exists a polynomial $q(T_1, T_2) \in k[T_1, T_2]$ such that

$$p(1, T_1) - p(1, T_2) = (T_1 - T_2)q(T_1, T_2).$$

Differentiating both sides with respect to T_1 and evaluating at $T_1 = T_2 = y$, we have

$$0 \neq \frac{\partial p}{\partial Y}(1, y) = q(y, y),$$

since $p(X, Y)$ has non-zero discriminant (cf. § 1). This means that $q(Y_1/X_1, Y_2/X_2)$ is invertible in the local ring of $\overline{C^a} \times \overline{C^a}$ at (P, P). On the other hand, in the above ring, we have

$$\begin{aligned}(Y_1/X_1 - Y_2/X_2) \cdot q(Y_1/X_1, Y_2/X_2) &\equiv a(Z_1/X_1)^n - a(Z_2/X_2)^n \\ &\equiv a(Z_1/X_1 - Z_2/X_2)((Z_1/X_1)^{n-1} + \cdots + (Z_2/X_2)^{n-1}),\end{aligned}$$

hence $Z_1/X_1 - Z_2/X_2$ is a generator of the prime ideal of the local ring of $\overline{C^a} \times \overline{C^a}$ at (P, P) corresponding to $\overline{\Delta^a}$. Similarly, $Z_1/Y_1 - Z_2/Y_2$ is a generator of the prime ideal of the local ring of $\overline{C^a} \times \overline{C^a}$ at $((x:1:0), (x:1:0)) \in \overline{\Delta^a} \cap \{Z_1 = Z_2 = 0, Y_1 Y_2 \neq 0\}$ corresponding to $\overline{\Delta^a}$. Therefore the Cartier divisor corresponding to $\overline{\Delta^a}$ is defined by the rational functions

1	on	$\overline{C^a} \times \overline{C^a} \setminus \overline{\Delta^a}$
$Z_1/X_1 - Z_2/X_2$	near	the closed points $\in \overline{\Delta^a} \cap \{Z_1 = Z_2 = 0, X_1 X_2 \neq 0\}$
$Z_1/Y_1 - Z_2/Y_2$	near	the closed points $\in \overline{\Delta^a} \cap \{Z_1 = Z_2 = 0, Y_1 Y_2 \neq 0\}$
some functions	near	the other closed points $\in \overline{\Delta^a}$.

Thus, pulling them back, we see that the Cartier divisor corresponding to the pull-back of $\overline{\Delta^a}$ by j_i is defined by the rational functions

1	on	$\overline{C^a} \setminus \{Z = 0\}$
$\zeta_i Z/X - Z/X = (\zeta_i - 1)Z/X$	near	$\overline{C^a} \cap \{Z = 0, X \neq 0\}$
$\zeta_i Z/Y - Z/Y = (\zeta_i - 1)Z/Y$	near	$\overline{C^a} \cap \{Z = 0, Y \neq 0\}$.

Since Z/X or Z/Y is a generator of the maximal ideal of the local ring of $\overline{C^a}$ at a point in $\overline{C^a} \cap \{Z = 0\}$, we are done. q.e.d.

We denote by $N(\cdot, \cdot)$ the global Néron pairings on the curve C^a, on the product $C^a \times_k C^a$ as well as on the product of Jacobian varieties $J^a \times_k J^a$ (cf. [8]). Since B_a is the canonical height on $J^a(\bar{k}) \times J^a(\bar{k})$ attached to $\mathscr{N}^a \in \mathrm{Pic}(J^a \times_k J^a)$ (cf. § 1), we have

$$B_a(\mathscr{L}, \mathscr{M}) = -N(\mathscr{N}^a, (\mathscr{L}, \mathscr{M}) - (0, 0))$$

for $\mathscr{L}, \mathscr{M} \in J^a(\bar{k})$.

We note that

$$B_a(f^aP_i, f^aP_i) = B_a(f^aP, f^aP) \tag{2}$$

(cf. the proof of Lemma 5.1), where $f^a\colon C^a \to J^a$ is the map in §1.

LEMMA 6.3. *When $i \neq 1$, we have*

$$B_a(f^aP_i, f^aP) = -\frac{1}{n-1} B_a(f^aP, f^aP)$$

for $P \in C^a(\bar{k}) \setminus \{Z=0\}$.

PROOF. Let j_i be the map defined immediately before Lemma 6.2, $\overline{\Delta^a}$ the diagonal divisor on $\overline{C^a} \times \overline{C^a}$, and $\overline{D^a} = \overline{C^a} \cap \{Z=0\} \in \mathrm{Div}(\overline{C^a})$. As described above, we have

$$B_a(f^aP_i, f^aP) = -N(\mathcal{N}^a, (f^aP_i, f^aP) - (0, 0)).$$

Using the functoriality of the Néron pairing, we see that

$$\begin{aligned} B_a(f^aP_i, f^aP) &= -N((f^a \times f^a)^*\mathcal{N}^a, (P_i, P) - (Q^a, Q^a)) \\ &= -N(j_i^*(f^a \times f^a)^*\mathcal{N}^a, P - Q^a). \end{aligned}$$

Since $(f^a \times f^a)^*\mathcal{N}^a \simeq \mathcal{L}(\{Q^a\} \times_k C^a + C^a \times_k \{Q^a\} - \Delta^a)$ (cf. the proof of Lemma 2.2), we obtain by Lemma 6.2 and the proof of Lemma 2.1 that $j_i^*(f^a \times f^a)^*\mathcal{N}^a \simeq \mathcal{L}(2Q^a - \overline{D^a}) \simeq \mathcal{L}(-(n-2)Q^a)$. Hence we have

$$B_a(f^aP_i, f^aP) = (n-2) \cdot N(Q^a, P - Q^a).$$

On the other hand, we have

$$\begin{aligned} B_a(f^aP, f^aP) &= -N(\mathcal{N}^a, (f^aP, f^aP) - (0, 0)) \\ &= -N(j^*(f^a \times f^a)^*\mathcal{N}^a, P - Q^a) \end{aligned}$$

and $j^*(f^a \times f^a)^*\mathcal{N}^a \simeq \mathcal{L}(2Q^a + (n-3)D^a) \simeq \mathcal{L}((n-1)(n-2)Q^a)$ (cf. the proof of Lemma 2.2). Hence

$$B_a(f^aP, f^aP) = -(n-1)(n-2) \cdot N(Q^a, P - Q^a).$$

q.e.d.

In particular, we get the angle which P_i and P make:

PROPOSITION 6.4. *For $\zeta_i \in \mu_n \cap k \setminus \{1\}$ and $P \in C^a(k) \setminus \{Z=0\}$ such that $\|\psi^a P\| \neq 0$, we have*

$$\cos(\psi^a P_i, \psi^a P) = -\frac{1}{n-1},$$

where $\psi^a\colon C^a(k) \to X^a = J^a(k) \otimes_{\mathbf{Z}} \mathbf{R}$ is the map given by $Q \mapsto f^aQ \otimes 1$.

PROOF. Divide both sides of the equation in Lemma 6.3 by $\|\psi^a P_i\| \cdot \|\psi^a P\| = \|\psi^a P\|^2$. By the definition given before Proposition 2.3, we have the desired result. q.e.d.

As an application, we next consider the matrices of the quadratic form B_a defined by $f^a P_1, \dots, f^a P_n$ for $P \in C^a(\bar{k})$.

LEMMA 6.5. *If $B_1(f^1 P, f^1 P) > 0$ $(P \in C^1(\bar{k}))$, then we have*

$$\det(B_1(f^1 P_{i_s}, f^1 P_{i_t}))_{s,t=1,\dots,r} > 0$$

for $r < n$ and distinct $i_1, \dots, i_r \in \{1, \dots, n\}$.

PROOF. For $b \in \boldsymbol{R}$ such that $-1/(r-1) < b \leq 0$, we know that the $r \times r$ determinant

$$\det \begin{pmatrix} 1 & b & \cdots & b \\ b & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \cdots & b & 1 \end{pmatrix} > 0 .$$

Hence we are done by Lemma 6.3 and the equality (2). q.e.d.

COROLLARY 6.6. *Let $r < n$ and let $\zeta_{i_1}, \dots, \zeta_{i_r} \in \mu_n \cap k$ be distinct. For $P \in C^a(k)$ such that $\|\psi^a P\| \neq 0$, the points $\psi^a P_{i_1}, \dots, \psi^a P_{i_r}$ are linearly independent, where $\psi^a \colon C^a(k) \to X^a = J^a(k) \otimes_{\boldsymbol{Z}} \boldsymbol{R}$ is the map defined by $Q \mapsto f^a Q \otimes 1$.*

PROOF. Note first that $\phi(P_{i_s}) = (\phi P)_{i_s}$, where ϕ is the twisting in §1. By the definition given before Proposition 2.3, the determinant of the quadratic form $\langle \cdot, \cdot \rangle$ on X^a defined by $\psi^a P_{i_1}, \dots, \psi^a P_{i_r}$ is

$$\det(\langle \psi^a P_{i_s}, \psi^a P_{i_t} \rangle)_{s,t=1,\dots,r} = \det(B_a(f^a P_{i_s}, f^a P_{i_t}))_{s,t=1,\dots,r} \, .$$

From the compatibility $B_a(\cdot, \cdot) = B_1(\Phi \cdot, \Phi \cdot)$ between the heights, and the commutativity $\Phi \circ f^a = f^1 \circ \phi$ (cf. §1), this equals

$$\begin{aligned} \det(B_1(\Phi(f^a(P_{i_s})), \Phi(f^a(P_{i_t})))) &= \det(B_1(f^1(\phi(P_{i_s})), f^1(\phi(P_{i_t})))) \\ &= \det(B_1(f^1(\phi P)_{i_s}, f^1(\phi P)_{i_t})) \, , \end{aligned}$$

which is positive by Lemma 6.5. Hence $\psi^a P_{i_1}, \dots, \psi^a P_{i_r}$ are independent. q.e.d.

Recall that $R_a = \operatorname{rank} J^a(k)$ and that $a\mathfrak{o}_k = \mathfrak{a}\mathfrak{b}^n$ is the ideal decomposition with $\mathfrak{a}$ integral n-th power-free (cf. §4). Consequently, we have:

THEOREM 6.7. *If $R_a < \min\{\#(\mu_n \cap k), n-1\}$, then $\|\psi^a P\| = 0$ for $P \in C^a(k)$. If furthermore $|N^k_{\boldsymbol{Q}} \mathfrak{a}|$ is sufficiently large, then $p(x, y) = a$ has no k-rational solution.*

PROOF. The former assertion is immediate by Corollary 6.6. As for the later, take a so that

$$\log|N_{\mathbf{Q}}^{k}\mathfrak{a}|>2dn^{2}\frac{n-1}{n-2}\left[\frac{\log 2}{2}\frac{(n-1)(n-2)}{n}+m\right].$$

Then, by Proposition 4.1, we have $\|\psi^{a}P\|>0$ for $P\in C^{a}(k)\setminus\{Z=0\}$, a contradiction. q.e.d.

REMARK 6.8. For any given constant H, the number of $a \bmod (k^{\times})^{n}$ satisfying $|N_{\mathbf{Q}}^{k}\mathfrak{a}|<H$ is finite because of the finiteness of the ideal class group of k.

REFERENCES

[1] E. BOMBIERI, The Mordell conjecture revisited, Ann. Scuola Norm. Sup. Pisa 17 (1990), 615–640; Errata-corrige, ibid. 18 (1991), 473.

[2] E. BOMBIERI AND W. M. SCHMIDT, On Thue's equation, Invent. Math. 88 (1987), 69–81; Correction, ibid. 97 (1989), 445.

[3] R. HARTSHORNE, Algebraic Geometry, Graduate Texts in Math. 52, Springer-Verlag, New York-Heidelberg, 1977.

[4] S. LANG, Fundamentals of Diophantine Geometry, Springer-Verlag, New York-Berlin, 1983.

[5] J. S. MILNE, Abelian varieties, in Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Storrs Conn. 1984, Springer-Verlag, New York-Berlin, 1986, 103–150.

[6] J. S. MILNE, Jacobian varieties, in Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Storrs Conn. 1984, Springer-Verlag, New York-Berlin, 1986, 167–212.

[7] D. MUMFORD, A remark on Mordell's conjecture, Amer. J. Math. 87 (1965), 1007–1016.

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

[9] J. H. SILVERMAN, Representations of integers by binary forms and the rank of the Mordell-Weil group, Invent. Math. 74 (1983), 281–292.

[10] J. H. SILVERMAN, Lower bounds for height functions, Duke Math. J. 51 (1984), 395–403.

[11] J. H. SILVERMAN, Rational points on certain families of curves of genus at least 2, Proc. London Math. Soc. 55 (1987), 465–481.

MATHEMATICAL INSTITUTE
FACULTY OF SCIENCE
TOHOKU UNIVERSITY
SENDAI 980-77
JAPAN