SUPERSINGULAR $K3$ SURFACES IN ODD CHARACTERISTIC AND SEXTIC DOUBLE PLANES

ICHIRO SHIMADA

Abstract. We show that every supersingular $K3$ surface is birational to a double cover of a projective plane.

1. Introduction

A $K3$ surface is called *supersingular* (in the sense of Shioda) if the rank of the Picard lattice is equal to 22. Supersingular $K3$ surfaces exist only when the characteristic p of the base field is positive.

We call a pair (X, L) of a $K3$ surface X and a line bundle L on X a *sextic double plane* if L is effective of degree $L^2 = 2$, and $|L|$ has no fixed components. Let (X, L) be a sextic double plane, and let

$$X \xrightarrow{f} Y \xrightarrow{\pi} \mathbb{P}^2$$

be the Stein factorization of the morphism associated with $|L|$. Then f is birational, and π is a finite morphism of degree 2.

The purpose of this paper is to prove the following:

Main Theorem. *Every supersingular $K3$ surface X has a line bundle L of degree 2 such that (X, L) is a sextic double plane.*

In [10], we have proved that every supersingular $K3$ surface in characteristic 2 is birational to an *inseparable* double cover of a projective plane. Therefore we consider the case where p is an odd prime.

Let X be a supersingular $K3$ surface in characteristic p. We denote by S_X the Picard lattice of X, which is an even lattice of signature $(1, 21)$. Artin [1] proved that the discriminant of S_X is equal to $-p^{2\sigma_X}$, where σ_X is a positive integer ≤ 10. The integer σ_X is called the *Artin invariant* of X. In [1, 7, 11], it was established that, for every pair of a prime integer p and an integer σ with $1 \leq \sigma \leq 10$, there exists a supersingular $K3$ surface X in characteristic p with $\sigma_X = \sigma$. On the other hand, Rudakov and Šafarevič [8] showed that the Picard lattice of a supersingular $K3$ surface is determined, up to isomorphisms of lattices, by the characteristic p and the Artin invariant. Moreover, they constructed, for each p and σ, a lattice $\Lambda_{p,\sigma}$ that is isomorphic to the Picard lattice of a supersingular $K3$ surface X in characteristic p with $\sigma_X = \sigma$.

Let (X, L) be a sextic double plane in characteristic p. When $p > 2$, the double covering $\pi : Y \to \mathbb{P}^2$ induced from $|L|$ is *separable*, and it branches along a plane curve $B_{(X,L)}$ of degree 6 with only rational double points. Let us denote by $R_{(X,L)}$ the ADE-type of the singularities of $B_{(X,L)}$.

1991 *Mathematics Subject Classification.* Primary 14J28; Secondary 14Q10, 11H55.

In this paper, we give, for each odd prime p and the Artin invariant σ, a vector $h \in \Lambda_{p,\sigma}$ such that, under a certain isomorphism $\phi : \Lambda_{p,\sigma} \xrightarrow{\sim} S_X$ of lattices, the line bundle L corresponding to $\phi(h) \in S_X$ makes X a sextic double plane. We also calculate the ADE-type $R_{(X,L)}$ of some supersingular sextic double planes (X, L) obtained from the vector $h \in \Lambda_{p,\sigma}$.

The proof of Main Theorem depends on elementary but tedious calculations of linear algebra and quadratic polynomials. The reader is strongly recommended to use some computer algebra system while reading this paper. In particular, a program that calculates the projection of a given quadratic form to a coordinate axis (see §4 for the definition) will be very useful.

We will assume from now on that p is an *odd* prime.

The author would like to thank Professor I. R. Dolgachev for stimulating discussions.

2. Preliminaries

We use the following notation and terminologies. Let T be a lattice; that is, T is a free $\mathbb{Z}$-module of finite rank with a non-degenerate symmetric bilinear form $(x, y) \mapsto xy$ that takes values in $\mathbb{Z}$. We can express a lattice T by a symmetric matrix M_T of integer components with respect to a certain basis of T. The *opposite lattice* T^- of a lattice T is a lattice with the same underlying $\mathbb{Z}$-module as T such that $M_{T^-} = -M_T$. The non-degenerate bilinear form induces a natural injective homomorphism $T \hookrightarrow \mathrm{Hom}(T, \mathbb{Z})$. The *discriminant group* of T is the group $\mathrm{Hom}(T, \mathbb{Z})/T$, which is a finite abelian group of order $|\operatorname{disc} T| = |\det M_T|$. For a vector $h \in T$, we put

$$\begin{array}{rcl} h^\perp & := & \{\, u \in T \mid uh = 0 \,\}, \\ \mathcal{E}_0^\pm(h) & := & \{\, u \in T \mid uh = \pm 1, u^2 = 0 \,\}, \\ \mathcal{E}_\le^\pm(h) & := & \{\, u \in T \mid uh = \pm 1, u^2 \le 0 \,\}. \end{array}$$

A lattice T is said to be *even* if $v^2 \in 2\mathbb{Z}$ holds for every $v \in T$. Let T be a (positive or negative) definite even lattice. A vector $v \in T$ is called a *root* of T if v^2 is equal to 2 or -2. The roots in T form a root system ([4, 2]). We denote by $\Sigma(T)$ the ADE-type of this root system, which in a finite formal sum of the symbols $A_l (l \ge 1)$, $D_m (m \ge 4)$ and $E_n (n = 6, 7, 8)$. For simplicity, we put

$$D_3 = A_3, \quad D_2 = 2A_1, \quad \text{and} \quad D_1 = D_0 = 0.$$

See [3, Chapter 4, Section 7] for the reason of this convention.

Let X be a $K3$ surface in arbitrary characteristic, and let S_X be the Picard lattice of X.

Proposition 2.1 ([6, 12])**.** *Let L be a nef line bundle on X with degree 2.*

(1) *The pair (X, L) is a sextic double plane if and only if the set $\mathcal{E}_0^+([L])$ is empty, where $[L] \in S_X$ is the isomorphism class of L.*

(2) *If (X, L) is a sextic double plane, then $R_{(X,L)}$ is equal to $\Sigma([L]^\perp)$.* □

Proposition 2.2 ([8])**.** *Let $v \in S_X$ be a vector with $v^2 > 0$. Then there exists an isometry $\gamma : S_X \xrightarrow{\sim} S_X$ of S_X such that $\gamma(v)$ is the isomorphism class of a nef line bundle on X.* □

Let p be an odd prime, and σ a positive integer ≤ 10. We denote by $\Lambda_{p,\sigma}$ a lattice of rank 22 with the following properties:

(a) $\Lambda_{p,\sigma}$ is even,
(b) the signature of $\Lambda_{p,\sigma}$ is $(1, 21)$, and
(c) the discriminant group of $\Lambda_{p,\sigma}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2\sigma}$.

Proposition 2.3 ([8]). *These three conditions determine the lattice $\Lambda_{p,\sigma}$ uniquely up to isomorphisms.* □

Proposition 2.4 ([1, 8]). *The Picard lattice S_X of a supersingular $K3$ surface X in characteristic $p > 2$ with $\sigma_X = \sigma$ is isomorphic to $\Lambda_{p,\sigma}$.* □

Combining these propositions and changing the sign from $\Lambda_{p,\sigma}$ to $\Lambda^-_{p,\sigma}$, we obtain the following:

Proposition 2.5. *Let X be a supersingular $K3$ surface in characteristic $p > 2$ with $\sigma_X = \sigma$, and R an ADE-type. There exists a line bundle L on X such that (X, L) is a sextic double plane with $R_{(X,L)} = R$ if and only if there exists a vector $h \in \Lambda^-_{p,\sigma}$ such that $h^2 = -2$, $\Sigma(h^\perp) = R$, and $\mathcal{E}^-_0(h) = \emptyset$.* □

We say that *a sextic double plane (X, L) is obtained from $h \in \Lambda^-_{p,\sigma}$* if $[L] \in S_X$ is equal to $\phi^-(h)$, where $\phi^- : \Lambda^-_{p,\sigma} \xrightarrow{\sim} S_X$ is an *anti*-isometry of lattices. Note that $R_{(X,L)} = \Sigma(h^\perp)$ depends not on the choice of ϕ^- but only on $h \in \Lambda^-_{p,\sigma}$.

3. Constructing the Picard lattice

According to [8], we construct the opposite lattice $\Lambda^-_{p,\sigma}$ of $\Lambda_{p,\sigma}$ from the following lattices.

(I) We denote by U and $U^{(p)}$ the even indefinite lattices of rank 2 whose intersection matrices are given by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & p \\ p & 0 \end{bmatrix},$$

with respect a certain basis $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$, respectively.

(II) Let $H^{(p)}$ denote the maximal order in the quaternion algebra $A^{(p)}$ over $\mathbb{Q}$ ramified only at p and ∞. Then $H^{(p)}$ has a symmetric bilinear form

$$xy := \mathrm{Tr}(xy^*),$$

where $y \mapsto y^*$ is the usual involution of the quaternion algebra. With this bilinear form, $H^{(p)}$ is a positive definite lattice of rank 4. We can write the intersection matrix of $H^{(p)}$ by the following result due to Ibukiyama:

Proposition 3.1 ([5]). *Let $p_1, \dots, p_r$ be distinct primes. We put $\varepsilon := (-1)^r$. Let q be a prime integer satisfying $\varepsilon q \equiv 5 \bmod 8$ and*

$$\left(\frac{\varepsilon q}{p_i}\right) = -1 \quad \text{for all} \quad p_i \neq 2.$$

We put $\alpha := \varepsilon p_1 \cdots p_r$, $\beta := \varepsilon q$, and define a quaternion algebra $A^{(p_1,\dots,p_r)}$ to be

$$\mathbb{Q} + \mathbb{Q}a + \mathbb{Q}b + \mathbb{Q}ab, \quad \text{with} \quad a^2 = \alpha,\ b^2 = \beta,\ ab + ba = 0.$$

Then $A^{(p_1,\dots,p_r)}$ is ramified only at $p_1, \dots, p_r$ if r is even, and only at $p_1, \dots, p_r, \infty$ if r is odd. Let γ be an integer satisfying $\gamma^2 \equiv \alpha \bmod q$. Then

$$H^{(p_1,\dots,p_r)} := \mathbb{Z} + \mathbb{Z}\frac{1+b}{2} + \mathbb{Z}\frac{a(1+b)}{2} + \mathbb{Z}\frac{(\gamma + a)b}{q}$$

is the maximal order of $A^{(p_1,\dots,p_r)}$. □

(p,r,s)	$(p,8,0)$	$(7,2,1)$	$(5,4,1)$	$(3,4,2)$	$(3,6,1)$
$\Sigma(V^{(p)}_{r,s})$	E_8	A_1	A_4	$2A_2$	E_6

TABLE 3.1. The exceptional cases of $\Sigma(V^{(p)}_{r,s})$

With respect to the basis

$$\boldsymbol{a}_1 := 1, \quad \boldsymbol{a}_2 := (1+b)/2, \quad \boldsymbol{a}_3 := a(1+b)/2, \quad \boldsymbol{a}_4 := (\gamma+a)b/q,$$

the intersection matrix of $H^{(p)}$ is written as follows:

$$M_{H^{(p)}} := \begin{bmatrix} 2 & 1 & 0 & 0 \\ 1 & (q+1)/2 & 0 & \gamma \\ 0 & 0 & p(q+1)/2 & p \\ 0 & \gamma & p & 2(p+\gamma^2)/q \end{bmatrix},$$

where q is a prime such that

$$q \equiv 3 \bmod 8 \quad \text{and} \quad (\frac{-q}{p}) = -1,$$

and γ is an integer satisfying

$$\gamma^2 + p \equiv 0 \bmod q.$$

(Note that such a prime q and an integer γ always exist.) Hence the lattice $H^{(p)}$ is even and the discriminant of $H^{(p)}$ is p^2. Moreover, since all the entries of $pM^{-1}_{H^{(p)}}$ are integers, the discriminant group of $H^{(p)}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$.

(III) For integers r and s satisfying $0 \le s \le r$ and $0 < r$, we denote by $W^{(p)}_{r,s}$ the lattice of rank r generated by $\boldsymbol{w}_1, \dots, \boldsymbol{w}_r$ such that

$$\boldsymbol{w}_i \boldsymbol{w}_j = \begin{cases} p & \text{if } i = j \le s, \\ 1 & \text{if } i = j > s, \\ 0 & \text{if } i \ne j. \end{cases}$$

We can construct an even lattice $V^{(p)}_{r,s}$ from $W^{(p)}_{r,s}$ by the following method of Venkov [13]. Let V_0 be the submodule of $W^{(p)}_{r,s}$ generated by the vectors $\sum_{i=1}^r x_i \boldsymbol{w}_i$ with $\sum x_i \equiv 0 \bmod 2$, and let a be the vector $(1/2)\sum_{i=1}^r \boldsymbol{w}_i \in W^{(p)}_{r,s} \otimes (1/2)\mathbb{Z}$. We put

$$V^{(p)}_{r,s} := V_0 \cup (a + V_0) \quad \subset \quad W^{(p)}_{r,s} \otimes (1/2)\mathbb{Z}.$$

Then $V^{(p)}_{r,s}$ is a positive definite even lattice with discriminant group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus s}$ if and only if the following holds:

$$ps + (r-s) \equiv 0 \bmod 8.$$

Proposition 3.2. *Suppose that* $ps + (r-s) \equiv 0 \bmod 8$ *holds. Then the ADE-type* $\Sigma(V^{(p)}_{r,s})$ *of the roots in* $V^{(p)}_{r,s}$ *is equal to* D_{r-s} *except for the cases in Table 3.1.*

Proof. We have an orthogonal decomposition

$$W^{(p)}_{r,s} = W^{[p]} \oplus W^{[1]},$$

where $W^{[p]}$ (resp. $W^{[1]}$) is spanned by $\boldsymbol{w}_1, \dots, \boldsymbol{w}_s$ (resp. $\boldsymbol{w}_{s+1}, \dots, \boldsymbol{w}_r$). Suppose that $v \in V_0 \subset W^{(p)}_{r,s}$ is a root, and let

$$v = v^{[p]} + v^{[1]} \quad (v^{[p]} \in W^{[p]},\ v^{[1]} \in W^{[1]})$$

be the decomposition of v. Since the norm of $v^{[p]}$ is a multiple of $p > 2$, $v^{[p]}$ must be 0, and hence $v \in W^{[1]} \cap V_0$. Since $W^{[1]} \cap V_0$ is the so-called "checkerboard lattice" of rank $r-s$, the ADE-type of its roots is equal to D_{r-s} ([3, Chapter 4, Section 7]). Suppose that $v \in a + V_0$ is a root. Then v is written as $\sum b_i \boldsymbol{w}_i/2$, where $b_1, \dots, b_r$ are odd integers satisfying

$$p(b_1^2 + \cdots + b_s^2) + (b_{s+1}^2 + \cdots + b_r^2) = 8.$$

The left-hand side of this equality is $\geq ps + (r-s)$. Therefore $ps + (r-s) = 8$ holds. The triples (p, r, s) satisfying this equality are just the ones in Table 3.1. Thus, except for these cases, we have proved $\Sigma(V^{(p)}_{r,s}) = D_{r-s}$. The lattice $V^{(p)}_{8,0}$ is a positive-definite even unimodular lattice of rank 8, and hence is the root lattice of type E_8. The ADE-types for the other triples in Table 3.1 can be calculated directly, for example by the method described in Section 4. □

Let us fix the following vectors in $V^{(p)}_{r,s}$:

$$\begin{aligned}
\boldsymbol{v}_1 &:= \boldsymbol{w}_1 + \boldsymbol{w}_2,\\
\boldsymbol{v}_2 &:= (\boldsymbol{w}_1 + \cdots + \boldsymbol{w}_r)/2,\\
\boldsymbol{v}_j &:= \boldsymbol{w}_{j-1} + \boldsymbol{w}_j \quad (j = 3, \dots, r-1),\\
\boldsymbol{v}_r &:= 2\boldsymbol{w}_r.
\end{aligned}$$

When $V^{(p)}_{r,s}$ is an even lattice, the rank r is even and the vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_r$ form a basis of $V^{(p)}_{r,s}$. The intersection matrix of $V^{(p)}_{r,s}$ with respect to this basis is easily calculated.

Using the characterization of the lattice $\Lambda_{p,\sigma}$ (Proposition 2.3), we see that the following lattices are isomorphic to $\Lambda^-_{p,\sigma}$:

$U^{(p)} \oplus H^{(p)} \oplus V^{(p)}_{16,2\sigma-4}$	if ($p \equiv 1 \bmod 4$ and $\sigma > 1$) or ($p \equiv 3 \bmod 4$ and $\sigma \equiv 0 \bmod 2$);
$U \oplus H^{(p)} \oplus V^{(p)}_{16,2\sigma-2}$	if ($p \equiv 1 \bmod 4$ and $\sigma < 10$) or ($p \equiv 3 \bmod 4$ and $\sigma \equiv 1 \bmod 2$);
$U^{(p)} \oplus V^{(p)}_{20,2\sigma-2}$	if $p \equiv 3 \bmod 4$ and $\sigma \equiv 0 \bmod 2$;
$U \oplus V^{(p)}_{20,2\sigma}$	if $p \equiv 3 \bmod 4$ and $\sigma \equiv 1 \bmod 2$.

4. Computational tools

Let S_0 be a finite set of variables, and let $Q(X_i | X_i \in S_0)$ be an inhomogeneous quadratic form of variables $X_i \in S_0$ such that the homogeneous part Q_2 of degree 2 is positive definite. We denote by $\mathbb{R}^{(S_0)}$ the real affine space with the set of coordinates being S_0. We denote by B_Q the compact subset

$$\{\ (x_i | X_i \in S_0) \in \mathbb{R}^{(S_0)} \ \mid\ Q(x_i | X_i \in S_0) \leq 0\ \}$$

of $\mathbb{R}^{(S_0)}$, and call it the *quadratic body* associated with the quadratic form Q. For a non-empty subset S of S_0, we denote by

$$\mathrm{pr}_S : \mathbb{R}^{(S_0)} \to \mathbb{R}^{(S)}$$

the natural projection to the real affine space $\mathbb{R}^{(S)}$ with the set of coordinates being S. The image $\mathrm{pr}_S(B_Q)$ of B_Q by pr_S is the quadratic body associated with a new quadratic form $Q^{(S)}(X_j|X_j \in S)$ of variables $X_j \in S$ constructed by the following procedures. We solve the system of linear equations

$$\frac{\partial Q}{\partial X_i} = 0 \quad (X_i \notin S).$$

Since Q_2 is positive definite, this system of equations has a solution of the form

$$X_i = \xi_i(X_j \mid X_j \in S) \quad (X_i \notin S),$$

where ξ_i is an affine-linear form of variables $X_j \in S$. Then $Q^{(S)}(X_j|X_j \in S)$ is the quadratic form obtained from Q by substituting each $X_i \notin S$ with ξ_i.

We denote the new quadratic form $Q^{(S)}(X_j|X_j \in S)$ by

$$\pi(Q(X_i|X_i \in S_0), S),$$

and call it the *projection of Q to $\mathbb{R}^{(S)}$*. When the set S consists of a single element X_ν, $Q^{\{X_\nu\}}(X_\nu) = \pi(Q(X_i|X_i \in S_0), \{X_\nu\})$ is a quadratic polynomial of one variable. We put

$$J\pi(Q(X_i|X_i \in S_0), \{X_\nu\}) := \{\ x \in \mathbb{R} \ \mid \ Q^{\{X_\nu\}}(x) \le 0\ \},$$

which is just the image of the projection of B_Q to the X_ν-axis.

Suppose that $S_0 = \{X_1, \dots, X_n\}$, and consider an inhomogeneous positive definite quadratic form $Q(X_1, \dots, X_n)$. Let $A := \mathbb{Z}\alpha \subset \mathbb{R}$ be the $\mathbb{Z}$-module of rank 1 generated by a non-zero real number α. We can list up all points $(a_1, \dots, a_n) \in A^n$ satisfying $Q(a_1, \dots, a_n) \le 0$ as follows. We put

$$S_k := \{X_1, \dots, X_k\}, \quad \text{and} \quad Q^{(S_k)}(X_1, \dots, X_k) := \pi(Q(X_1, \dots, X_n), S_k).$$

If we have a point $(a_1, \dots, a_k) \in A^k$ such that $Q^{(S_k)}(a_1, \dots, a_k) \le 0$, then it is easy to calculate the set

$$\{\ a \in A \ \mid \ Q^{(S_{k+1})}(a_1, \dots, a_k, a) \le 0\ \} = J\pi(Q(a_1, \dots, a_k, X_{k+1}, \dots, X_n), \{X_{k+1}\}) \cap A,$$

where $Q(a_1, \dots, a_k, X_{k+1}, \dots, X_n)$ is considered as a quadratic form of variables $X_{k+1}, \dots, X_n$. Starting from $Q^{(S_1)}(X_1)$, we can make inductively the list of all points in $B_Q \cap A^n$.

Let T be a positive definite even lattice of rank n, and let $Q_T(X_1, \dots, X_n)$ be a homogeneous quadratic form associated with T. We can calculate the set of roots of T by applying the above algorithm to $Q_T(X_1, \dots, X_n) - 2$.

5. Proof of Main Theorem

The strategy of the proof is as follows. It is enough to find a vector $h \in \Lambda^-_{p,\sigma}$ such that $h^2 = -2$ and $\mathcal{E}^-_0(h) = \emptyset$. We decompose $\Lambda^-_{p,\sigma}$ into an orthogonal direct sum $M \oplus V$, where M is of rank r with signature $(r-1, 1)$, and show that there exists a vector $h_0 \in M$ satisfying $h_0^2 = -2$ and $\mathcal{E}^-_{\le}(h_0) = \emptyset$. Since V is positive definite, such a vector $h_0 \in M$ yields the hoped-for vector $h \in \Lambda^-_{p,\sigma}$ by the natural inclusion $M \hookrightarrow \Lambda^-_{p,\sigma}$.

In each of the cases below, we explicitly give a vector $h_0 \in M$ satisfying $h_0^2 = -2$, and a basis $e_1, \dots, e_{r-1} \in M$ of $h_0^\perp$. We put

$$v_0 := h_0/2 \ \in \ M \otimes (1/2)\mathbb{Z},$$

and define an inhomogeneous quadratic form Q with variables $X_1, \dots, X_{r-1}$ by

$$Q(X_1, \dots, X_{r-1}) := (v_0 + X_1 e_1 + \dots + X_{r-1} e_{r-1})^2.$$

By the $\mathbb{Z}$-*condition*, we mean a necessary and sufficient condition on $x_1, \dots, x_{r-1} \in (1/2)\mathbb{Z}$ for a vector $v_0 + x_1 e_1 + \dots + x_{r-1} e_{r-1} \in M \otimes (1/2)\mathbb{Z}$ to be in M. Since $v_0 h_0 = -1$, every vector $x \in M$ satisfying $x h_0 = -1$ is uniquely written as

$$x = v_0 + x_1 e_1 + \dots + x_{r-1} e_{r-1},$$

where $x_1, \dots, x_{r-1} \in (1/2)\mathbb{Z}$ satisfy the $\mathbb{Z}$-condition.

In order to prove that $\mathcal{E}^-_{\le}(h_0)$ is empty, it is therefore enough to show that there are no $x_1, \dots, x_{r-1} \in (1/2)\mathbb{Z}$ satisfying the $\mathbb{Z}$-condition and the inequality $Q(x_1, \dots, x_{r-1}) \le 0$.

We also investigate the ADE-type $R_{(X,L)}$ of the sextic double plane (X, L) obtained from the vector $h \in \Lambda^-_{p,\sigma}$ corresponding to the given $h_0 \in M$ via $M \hookrightarrow \Lambda^-_{p,\sigma}$. Since

$$R_{(X,L)} = \Sigma(h^\perp) = \Sigma(h_0^\perp) + \Sigma(V),$$

it is enough to calculate $\Sigma(V)$ and the set of the roots in the positive definite even lattice $h_0^\perp$. In order to calculate this set, we define the quadratic form G with variables $X_1, \dots, X_{r-1}$ by

$$G(X_1, \dots, X_{r-1}) := -2 + (X_1 e_1 + \dots + X_{r-1} e_{r-1})^2,$$

and find all the points $(b_1, \dots, b_{r-1}) \in \mathbb{Z}^{\oplus(r-1)}$ satisfying $G(b_1, \dots, b_{r-1}) = 0$.

We divide the entire situation into the following overlapping cases:

Case I. $p \equiv 1 \bmod 4$ and $\sigma < 10$.

Case II. $p \equiv 1 \bmod 4$ and $\sigma > 1$.

Case III. $p \equiv 3 \bmod 4$ and $\sigma \equiv 0 \bmod 2$.

Case IV. $p \equiv 3 \bmod 4$ and $\sigma \equiv 1 \bmod 2$.

5.1. **Case I.** $p \equiv 1 \bmod 4$ and $\sigma < 10$. In this case, we have

$$\Lambda^-_{p,\sigma} \ \cong\ U \oplus H^{(p)} \oplus V^{(p)}_{16,2\sigma-2}.$$

We choose $U \oplus H^{(p)}$ as the lattice M. We express vectors of $U \oplus H^{(p)}$ as row vectors with respect to the basis $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{a}_1, \dots, \boldsymbol{a}_4$. Replacing γ in the construction of $H^{(p)}$ by $\gamma + q$ if necessary, we can assume that γ is odd. Then $p + \gamma^2 \equiv 2 \bmod 4$, because $p \equiv 1 \bmod 4$. Therefore

$$t := -\frac{1}{4}\Big(\frac{p+\gamma^2}{q} + 2\Big)$$

is an integer. We put

$$\begin{array}{llcccccl}
h_0 & := [& 2, & 2\,t, & 1, & 0, & 0, & 1 \ ], \\
e_1 & := [& 1, & 0, & -t, & 0, & 0, & 0 \ ], \\
e_2 & := [& 0, & 1, & -1, & 0, & 0, & 0 \ ], \\
e_3 & := [& 0, & 0, & -(\gamma+1)/2, & 1, & 0, & 0 \ ], \\
e_4 & := [& 0, & 0, & -(p+\gamma^2)/q, & 0, & 0, & 1 \ ], \\
e_5 & := [& 0, & 0, & -p, & 0, & 2, & 0 \ ].
\end{array}$$

It is easy to see that $h_0^2 = -2$, and that $e_1, \dots, e_5$ form a basis of $h_0^\perp$, because p and 2 are prime to each other. The $\mathbb{Z}$-condition in this case is as follows:

$$x_1, x_2, x_3 \in \mathbb{Z}, \quad x_4, x_5 \in \mathbb{Z} + 1/2, \tag{5.1}$$

p	(q,γ)	$R_{(X,L)}$
41	$(3,1)$ $(11,5)$	$A_1+A_2+D_{18-2\sigma}$ $2A_1+D_{18-2\sigma}$
53	$(3,1)$ $(67,9)$	$A_1+A_2+D_{18-2\sigma}$ $A_3+D_{18-2\sigma}$
61	$(11,7)$ $(43,5)$	$2A_1+D_{18-2\sigma}$ $A_3+D_{18-2\sigma}$
101	$(3,1)$ $(11,3)$ $(163,15)$	$A_1+A_2+D_{18-2\sigma}$ $2A_1+D_{18-2\sigma}$ $A_3+D_{18-2\sigma}$

TABLE 5.1. Examples of $R_{(X,L)}$ in Case I

because $-(p+\gamma^2)/q$ is an even integer. We assume that there exist $a_1,\dots,a_5\in(1/2)\mathbb{Z}$ satisfying (5.1) and $Q(a_1,\dots,a_5)\le 0$, and derive a contradiction. Since

$$J\pi(Q(X_1,X_2,X_3,X_4,X_5),\{X_1\})=[-1,1],$$

we have $a_1=0$ or $a_1=\pm1$. From

$$\begin{aligned} J\pi(Q(\pm1,X_2,X_3,X_4,X_5),\{X_5\}) &= [0,0],\\ J\pi(Q(\ 0\ ,X_2,X_3,X_4,X_5),\{X_5\}) &= [-\sqrt{p}/2p,\sqrt{p}/2p], \end{aligned}$$

and $a_5\in\mathbb{Z}+1/2$, we get a contradiction. Thus $\mathcal{E}^-_{\le}(h_0)=\emptyset$ is proved. □

Let us investigate the ADE-type

$$R_{(X,L)}=\Sigma(h_0^\perp)+\Sigma(V^{(p)}_{16,2\sigma-2})=\Sigma(h_0^\perp)+D_{18-2\sigma}$$

of the sextic double plane (X,L) constructed from h_0. There are at least two roots

$$[0,1,-1,0,0,0],\quad\text{and}\quad[2,\,-(p+\gamma^2)/2q\,,1,0,0,1]$$

in $h_0^\perp$, which are perpendicular to each other. Numerical experiments show that the ADE-type $\Sigma(h_0^\perp)$ depends on the choice of q and γ in the construction of $H^{(p)}$. See Table 5.1.

Remark 5.1. When $p=5$ and $(q,\gamma)=(3,1)$, there exist two other roots

$$[0,-1,0,1,0,0],\quad\text{and}\quad[-1,0,0,-1,0,0]$$

in $h_0^\perp$, and $\Sigma(h_0^\perp)=A_4$ holds. Using the isomorphisms of $\Lambda^-_{5,\sigma}$ with the lattices in Table 5.2, we obtain examples of sextic curves $B_{(X,L)}$ with only rational double points such that the total Milnor number is 20. Note that, in characteristic 0, the maximum of the total Milnor number of sextic curves with only rational double points is 19. See Yang [14].

On the other hand, there exists a supersingular sextic double plane (X,L) in characteristic 5 with $\sigma_X=1$ such that the branch curve $B_{(X,L)}$ is smooth. Indeed, let $B\subset\mathbb{P}^2$ the Fermat curve

$$x_0^6+x_1^6+x_2^6=0$$

of degree 6, and let X_B be the double cover of $\mathbb{P}^2$ that branches along B. If $P\in B$ is an $\mathbb{F}_{25}$-rational point of B, then the tangent line ℓ_P to B at P intersects B only

σ	$\Lambda^-_{5,\sigma}$	$R_{(X,L)}$
1	$U \oplus H^{(5)} \oplus V^{(5)}_{16,0}$	$A_4 + D_{16}$
1	$U \oplus H^{(5)} \oplus E_8 \oplus E_8$	$A_4 + 2E_8$
2	$U \oplus H^{(5)} \oplus A_4 \oplus A_4 \oplus E_8$	$3A_4 + E_8$
3	$U \oplus H^{(5)} \oplus A_4 \oplus A_4 \oplus A_4 \oplus A_4$	$5A_4$

TABLE 5.2. Examples of $B_{(X,L)}$ with the total Milnor number 20 in characteristic 5

at P with multiplicity 6, and hence the pull-back of ℓ_P to X_B splits into two (-2)-curves ℓ_P^+ and ℓ_P^- intersecting only at one point with multiplicity 3. The number of $\mathbb{F}_{25}$-rational points of B is 126, and hence we obtain 252 smooth rational curves $\ell_P^\pm$ on X_B. It is easy to make the matrix of intersection numbers between these curves. Choosing suitable 22 curves from them, we obtain a matrix of determinant -25. Hence X_B is supersingular, and the Artin invariant of X_B is 1.

5.2. **Case II.** $p \equiv 1 \bmod 4$ and $\sigma > 1$. In this case, we have

$$\Lambda^-_{p,\sigma} \;\cong\; U^{(p)} \oplus H^{(p)} \oplus V^{(p)}_{16,2\sigma-4}.$$

We show that there exists a vector $h_0 \in M := U^{(p)} \oplus H^{(p)}$ such that $h_0^2 = -2$ and $\mathcal{E}^-_{\le}(h_0) = \emptyset$. Vectors of $U^{(p)} \oplus H^{(p)}$ are expressed as row vectors with respect to the basis $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{a}_1, \dots, \boldsymbol{a}_4$. Since $p \equiv 1 \bmod 4$, there exists an integer α such that $\alpha^2 \equiv -1 \bmod p$. Replacing α with $\alpha + p$ if necessary, we can assume that α is even. We put

$$b := -\frac{\alpha^2+1}{p},$$

and set

$$\begin{array}{llrrrrrrl} h_0 & := [& 1, & b, & \alpha, & 0, & 0, & 0 &], \\ e_1 & := [& 0, & 0, & 0, & 0, & 0, & 1 &], \\ e_2 & := [& 0, & 0, & 0, & 0, & 1, & 0 &], \\ e_3 & := [& 1, & -b, & 0, & 0, & 0, & 0 &], \\ e_4 & := [& 0, & 0, & 1, & -2, & 0, & 0 &], \\ e_5 & := [& 0, & -\alpha, & 0, & p, & 0, & 0 &]. \end{array}$$

Then h_0^2 is equal to -2, and $e_1, \dots, e_5$ form a basis of $h_0^\perp$. The $\mathbb{Z}$-condition in this case is as follows:

$$x_1, x_2, x_4, x_5 \in \mathbb{Z} \quad \text{and} \quad x_3 \in \mathbb{Z} + 1/2, \tag{5.2}$$

because α is even. We assume that there exist $a_1, \dots, a_5 \in (1/2)\mathbb{Z}$ satisfying (5.2) and $Q(a_1, \dots, a_5) \le 0$, and derive a contradiction. Since

$$\begin{aligned} J\pi(Q(X_1, X_2, X_3, X_4, X_5), \{X_2\}) &= [-1/\sqrt{p}, 1/\sqrt{p}], \\ J\pi(Q(X_1, X_2, X_3, X_4, X_5), \{X_3\}) &= [-1/2, 1/2], \end{aligned}$$

we have $a_2 = 0$ and $a_3 = \pm 1/2$. Since

$$\pi(Q(X_1, 0, \pm 1/2, X_4, X_5), \{X_5\}) = (pX_5 \mp \alpha)^2/2,$$

we have $a_5 = \pm\alpha/p$, which contradicts $a_5 \in \mathbb{Z}$. Thus $\mathcal{E}^-_{\le}(h_0) = \emptyset$ is proved. □

We show that $\Sigma(h_0^{\perp}) = 0$ in this case, so that the ADE-type $R_{(X,L)}$ of the sextic double plane (X, L) constructed from h_0 above is equal to

$$R_{(X,L)} = \Sigma(h_0^{\perp}) + \Sigma(V^{(p)}_{16,2\sigma-4}) = D_{20-2\sigma}.$$

Recall that

$$G(X_1, X_2, X_3, X_4, X_5) = -2 + (X_1e_1 + X_2e_2 + X_3e_3 + X_4e_4 + X_5e_5)^2.$$

We assume that there exist integers $b_1, \dots, b_5$ such that $G(b_1, \dots, b_5) = 0$, and derive a contradiction. From

$$\begin{aligned} J\pi(G(X_1, X_2, X_3, X_4, X_5), \{X_2\}) &= [-2/\sqrt{p}, 2/\sqrt{p}], \\ J\pi(G(X_1, X_2, X_3, X_4, X_5), \{X_3\}) &= [-1, 1], \end{aligned}$$

we obtain $b_2 = 0$ because $p > 4$, and $b_3 = 0$ or ± 1. Suppose that $b_3 = 0$. Since

$$J\pi(G(X_1, 0, 0, X_4, X_5), \{X_5\}) = [-2/p, 2/p],$$

we have b_5=0. Then

$$G(X_1, 0, 0, X_4, 0) = \frac{2}{q}((qX_4 - \gamma X_1)^2 + pX_1^2 - q).$$

Therefore we must have $(qb_4 - \gamma b_1)^2 \equiv q \bmod p$, which is impossible because q is in a non-quadratic residue modulo p in the case $p \equiv 1 \bmod 4$. Suppose that $b_3 = \pm 1$. Since

$$\pi(G(X_1, 0, \pm 1, X_4, X_5), \{X_5\}) = (pX_5 \mp 2\alpha)^2/2,$$

we obtain a contradiction to $b_5 \in \mathbb{Z}$. Therefore the assertion $R_{(X,L)} = D_{20-2\sigma}$ is proved. □

5.3. **Case III.** $p \equiv 3 \bmod 4$ and $\sigma \equiv 0 \bmod 2$. In this case, we have

$$\Lambda^-_{p,\sigma} \;\cong\; U^{(p)} \oplus H^{(p)} \oplus V^{(p)}_{16,2\sigma-4}.$$

We choose $U^{(p)} \oplus H^{(p)}$ as M. By replacing γ in the construction of $H^{(p)}$ with $\gamma + q$ if necessary, we can assume that $\gamma \not\equiv 0 \bmod p$. Using Chevalley-Warning theorem ([9]) and the assumption $p \equiv 3 \bmod 4$, we see that there exists a solution of the equation

$$X^2 + \alpha Y^2 = -1$$

with $Y \neq 0$ in $\mathbb{F}_p$ for any $\alpha \in \mathbb{F}_p$. Therefore we have integers x and y such that

$$x^2 + xy + \frac{q+1}{4}y^2 = \Big(x + \frac{y}{2}\Big)^2 + \frac{q}{4}y^2 \equiv -1 \bmod p$$

and $y \not\equiv 0 \bmod p$. Replacing x and y with $x + p$ and $y + p$ if necessary, we can assume that both of x and y are even. We then put

$$b := -\frac{1}{p}(x^2 + xy + \frac{q+1}{4}y^2 + 1) \in \mathbb{Z}.$$

Note that b is odd. Since $\gamma y \not\equiv 0 \bmod p$, there exist integers E_{36} and E_{46} satisfying

$$\gamma y E_{36} + (2x + y) \equiv 0 \bmod p, \quad \gamma y E_{46} + x + \frac{1+q}{2}y \equiv 0 \bmod p.$$

We then put

$$E_{32} := -\frac{1}{p}(\gamma y E_{36} + 2x + y) \in \mathbb{Z}, \quad E_{42} := -\frac{1}{p}(\gamma y E_{46} + x + \frac{1+q}{2}y) \in \mathbb{Z},$$

and set

$$\begin{array}{lllllllll} h_0 & := [& 1, & b, & x, & y, & 0, & 0 &], \\ e_1 & := [& 0, & 0, & 0, & 0, & 1, & 0 &], \\ e_2 & := [& 1, & -b, & 0, & 0, & 0, & 0 &], \\ e_3 & := [& 0, & E_{32}, & 1, & 0, & 0, & E_{36} &], \\ e_4 & := [& 0, & E_{42}, & 0, & 1, & 0, & E_{46} &], \\ e_5 & := [& 0, & -\gamma y, & 0, & 0, & 0, & p &]. \end{array}$$

It is easy to see that $h_0^2 = -2$, and that $e_1, \dots, e_5$ form a basis of $h_0^\perp$, because p and $-\gamma y$ are prime to each other. The $\mathbb{Z}$-condition in this case is as follows:

(5.3) $$x_1, x_3, x_4, x_5 \in \mathbb{Z}, \quad x_2 \in \mathbb{Z} + 1/2,$$

because x and y are even, and b is odd. Suppose that there exist $a_1, \dots, a_5 \in (1/2)\mathbb{Z}$ satisfying (5.3) and $Q(a_1, \dots, a_5) \le 0$. Since

$$J\pi(Q(X_1, X_2, X_3, X_4, X_5), \{X_1\}) = [-1/\sqrt{p}, 1/\sqrt{p}],$$

we have $a_1 = 0$. Since

$$J\pi(Q(0, X_2, X_3, X_4, X_5), \{X_2\}) = [-1/2, 1/2],$$

we have $a_2 = \pm 1/2$. Because $\pi(Q(0, \pm 1/2, X_3, X_4, X_5), \{X_5\})$ is a multiple of $(xE_{36} + yE_{46} \pm 2pX_5)^2$ by a positive constant, we obtain

$$a_5 = \mp \frac{xE_{36} + yE_{46}}{2p}.$$

In $\mathbb{F}_p$, however, we have

$$-(xE_{36} + yE_{46}) = \frac{4x^2 + 4xy + (1+q)y^2}{2\gamma y} = \frac{-2}{\gamma y} \neq 0.$$

Therefore a_5 cannot be an integer, and we arrive at a contradiction. Thus $\mathcal{E}^-_{\le}(h_0) = \emptyset$ is proved. □

We prove that

$$R_{(X,L)} = \Sigma(V^{(p)}_{16,2\sigma-4}) = D_{20-2\sigma}$$

holds for a sextic double plane (X, L) obtained from the vector h_0 above. It is enough to show that $\Sigma(h_0^\perp) = 0$. Again we assume that there exists an integer point $(b_1, \dots, b_5) \in \mathbb{Z}^{\oplus 5}$ satisfying $G(b_1, \dots, b_5) = 0$, and derive a contradiction. Since

$$J\pi(G(X_1, X_2, X_3, X_4, X_5), \{X_1\}) = [-2/\sqrt{p}, 2/\sqrt{p}],$$

we see that $b_1 = 0$ if $p > 3$, and $b_1 = 0$ or ± 1 if $p = 3$. Since

$$J\pi(G(X_1, X_2, X_3, X_4, X_5), \{X_2\}) = [-1, 1],$$

we see that $b_2 = 0$ or ± 1. Suppose that $(b_1, b_2) = (0, 0)$. Then we have

$$2qy^2 G(0, 0, X_3, X_4, X_5) \equiv -4((2X_3 + X_4)^2 + y^2 q) \mod p.$$

Since $-q$ is in a non-quadratic residue modulo p and $y \not\equiv 0 \bmod p$, we get a contradiction. Suppose that $(b_1, b_2) = (0, \pm 1)$. The projections of $G(0, \pm 1, X_3, X_4, X_5)$ to the X_3-axis and the X_4-axis are multiples of $(X_3 \mp x)^2$ and $(X_4 \mp y)^2$ by positive constants, respectively. Therefore $(b_3, b_4) = \pm(x, y)$. Solving the equation $G(0, \pm 1, \pm x, \pm y, X_5) = 0$, we obtain

$$b_5 = \mp(xE_{36} + yE_{46})/p,$$

which contradicts $b_5 \in \mathbb{Z}$. Suppose that $p = 3$ and $b_1 = \pm 1$. Since

$$J\pi(G(\pm 1, X_2, X_3, X_4, X_5), \{X_2\}) = [-1/2, 1/2],$$

we obtain $b_2 = 0$. Let ν be the positive integer $(p+\gamma^2)/q$. Projecting the quadratic form $G(\pm 1, 0, X_3, X_4, X_5)$ to the X_3-axis and the X_4-axis, we see that

$$3(2b_3 \pm \gamma)^2 - \nu - 3 = 0 \quad \text{and} \quad 3(b_4 \mp \gamma)^2 - \nu = 0.$$

In particular, both of $\nu/3$ and $\nu/3 + 1$ are square integers. Thus we get a contradiction, and the proof of the assertion $R_{(X,L)} = D_{20-2\sigma}$ is completed. □

5.4. **Case IV.** $p \equiv 3 \bmod 4$ and $\sigma \equiv 1 \bmod 2$. We have

$$\Lambda^-_{p,\sigma} \;\cong\; U \oplus V^{(p)}_{20,2\sigma}.$$

In this case, M is the entire lattice $U \oplus V^{(p)}_{20,2\sigma}$. We express vectors of $U \oplus V^{(p)}_{20,2\sigma}$ as row vectors with respect to the basis $\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{v}_1, \dots, \boldsymbol{v}_{20}$, where $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{20}$ are the basis of $V^{(p)}_{20,2\sigma}$ fixed in §3 (III). We put

$$\begin{array}{lllllllllll}
h_0 & := [& 2, & -(p+1)/2, & 1, & 0, & 0, & 0, & \dots & \dots, & 0\,], \\
e_1 & := [& 0, & 0, & 0, & 0, & 0, & 0, & \dots & \dots, & 1\,], \\
 & & \dots & & \dots & & & & \dots & & \\
e_i & := [& 0, & 0, & 0, & 0, & 0, & 0, & \dots & 1, \dots, & 0\,], \\
 & & \multicolumn{8}{l}{(1 \text{ is at the } (23-i)\text{-th place for } i = 1, \dots, 17)} \\
 & & \dots & & \dots & & & & \dots & & \\
e_{18} & := [& 1, & (p+1)/4, & 0, & 0, & 0, & 0, & \dots & \dots, & 0\,], \\
e_{19} & := [& 0, & -p, & 1, & 0, & 0, & 0, & \dots & \dots, & 0\,], \\
e_{20} & := [& 0, & 0, & 0, & 1, & -1, & 0, & \dots & \dots, & 0\,], \\
e_{21} & := [& 0, & p, & 0, & 0, & -2, & 0, & \dots & \dots, & 0\,].
\end{array}$$

It is easy to see that $h_0^2 = -2$, and that $e_1, \dots, e_{21}$ form a basis of $h_0^\perp$. Since $-(p+1)/2$ is an even integer, the $\mathbb{Z}$-condition in this case is as follows:

$$\text{(5.4)} \qquad x_i \in \mathbb{Z} \;\; (i \neq 19, 21), \quad x_{19}, x_{21} \in \mathbb{Z} + 1/2.$$

We use the notation Q_σ instead of Q in order to distinguish the situations for different Artin invariants σ. Suppose that there exist $a_1, \dots, a_{21} \in (1/2)\mathbb{Z}$ satisfying (5.4) and the inequality $Q_\sigma(a_1, \dots, a_{21}) \le 0$. We put

$$J_{\sigma,1} := J\pi(Q_\sigma(X_1, \dots, X_{21}), \{X_1\}),$$

and for $\nu = 2, \dots, 17$, we put

$$J_{\sigma,\nu} := J\pi(Q_\sigma(0, \dots, 0, X_\nu \dots, X_{21}), \{X_\nu\}).$$

Each interval $J_{\sigma,\nu}$ is expressed as $[-\sqrt{\tau_{\sigma,\nu}}, \sqrt{\tau_{\sigma,\nu}}]$, where $\tau_{\sigma,\nu}$ are calculated as in Table 5.3. We have

$$\text{(5.5)} \quad J_{\sigma,1} \cap \mathbb{Z} \;=\; \begin{cases} \{-1, 0, 1\} & \text{if } \sigma < 7 \text{ or } (p,\sigma) = (3,7), (7,7) \text{ or } (3,9), \\ \{0\} & \text{otherwise;} \end{cases}$$

$$\text{(5.6)} \quad J_{\sigma,\nu} \cap \mathbb{Z} \;=\; \{0\} \quad \text{for} \quad \nu = 2, \dots, 17.$$

From (5.6), we see that, if $a_1 = 0$, then $a_2 = \dots = a_{17} = 0$ holds inductively.

Suppose that $a_1 = 0$, so that $a_2 = \dots = a_{17} = 0$. We put

$$Q'_\sigma(X_{18}, X_{19}, X_{20}, X_{21}) := Q_\sigma(0, \dots, 0, X_{18}, X_{19}, X_{20}, X_{21}).$$

$\nu \setminus \sigma$	1	3	5	7	9
1	$\frac{9p+1}{4p}$	$\frac{7p+3}{4p}$	$\frac{5p+5}{4p}$	$\frac{3p+7}{4p}$	$\frac{p+9}{4p}$
2	$\frac{8p+1}{9p+1}$	$\frac{6p+3}{7p+3}$	$\frac{4p+5}{5p+5}$	$\frac{2p+7}{3p+7}$	$\frac{9}{p+9}$
3	$\frac{23p+3}{32p+4}$	$\frac{17p+9}{24p+12}$	$\frac{11p+15}{16p+20}$	$\frac{5p+21}{8p+28}$	$\frac{9p+17}{36p}$
4	$\frac{14p+2}{23p+3}$	$\frac{10p+6}{17p+9}$	$\frac{6p+10}{11p+15}$	$\frac{2p+14}{5p+21}$	$\frac{8p+8}{9p^2+17p}$
5	$\frac{33p+5}{56p+8}$	$\frac{23p+15}{40p+24}$	$\frac{13p+25}{24p+40}$	$\frac{3p+35}{8p+56}$	$\frac{23p+15}{32p^2+32p}$
6	$\frac{18p+3}{33p+5}$	$\frac{12p+9}{23p+15}$	$\frac{6p+15}{13p+25}$	$\frac{21}{3p+35}$	$\frac{14p+7}{23p^2+15p}$
7	$\frac{39p+7}{72p+12}$	$\frac{25p+21}{48p+36}$	$\frac{11p+35}{24p+60}$	$\frac{7p+39}{84p}$	$\frac{33p+13}{56p^2+28p}$
8	$\frac{20p+4}{39p+7}$	$\frac{12p+12}{25p+21}$	$\frac{4p+20}{11p+35}$	$\frac{6p+18}{7p^2+39p}$	$\frac{18p+6}{33p^2+13p}$
9	$\frac{41p+9}{80p+16}$	$\frac{23p+27}{48p+48}$	$\frac{5p+45}{16p+80}$	$\frac{17p+33}{24p^2+72p}$	$\frac{39p+11}{72p^2+24p}$
10	$\frac{20p+5}{41p+9}$	$\frac{10p+15}{23p+27}$	$\frac{5}{p+9}$	$\frac{10p+15}{17p^2+33p}$	$\frac{20p+5}{39p^2+11p}$
11	$\frac{39p+11}{80p+20}$	$\frac{17p+33}{40p+60}$	$\frac{p+9}{20p}$	$\frac{23p+27}{40p^2+60p}$	$\frac{41p+9}{80p^2+20p}$
12	$\frac{18p+6}{39p+11}$	$\frac{6p+18}{17p+33}$	$\frac{4p+20}{5p^2+45p}$	$\frac{12p+12}{23p^2+27p}$	$\frac{20p+4}{41p^2+9p}$
13	$\frac{33p+13}{72p+24}$	$\frac{7p+39}{24p+72}$	$\frac{11p+35}{16p^2+80p}$	$\frac{25p+21}{48p^2+48p}$	$\frac{39p+7}{80p^2+16p}$
14	$\frac{14p+7}{33p+13}$	$\frac{21}{7p+39}$	$\frac{6p+15}{11p^2+35p}$	$\frac{12p+9}{25p^2+21p}$	$\frac{18p+3}{39p^2+7p}$
15	$\frac{23p+15}{56p+28}$	$\frac{3p+35}{84p}$	$\frac{13p+25}{24p^2+60p}$	$\frac{23p+15}{48p^2+36p}$	$\frac{33p+5}{72p^2+12p}$
16	$\frac{8p+8}{23p+15}$	$\frac{2p+14}{3p^2+35p}$	$\frac{6p+10}{13p^2+25p}$	$\frac{10p+6}{23p^2+15p}$	$\frac{14p+2}{33p^2+5p}$
17	$\frac{9p+17}{32p+32}$	$\frac{5p+21}{8p^2+56p}$	$\frac{11p+15}{24p^2+40p}$	$\frac{17p+9}{40p^2+24p}$	$\frac{23p+3}{56p^2+8p}$
20	$\frac{p+2}{9p+17}$	$\frac{3}{5p+21}$	$\frac{3}{11p+15}$	$\frac{3}{17p+9}$	$\frac{3}{23p+3}$
21	$\frac{1}{4p+8}$	$\frac{1}{12p}$	$\frac{1}{12p}$	$\frac{1}{12p}$	$\frac{1}{12p}$

TABLE 5.3. The table of $\tau_{\sigma,\nu}$

The projection of the 4-dimensional quadratic body associated with Q'_σ to the X_{20}-axis is the interval $[-\sqrt{\tau_{\sigma,20}}, \sqrt{\tau_{\sigma,20}}]$, where $\tau_{\sigma,20}$ are given in Table 5.3. Hence $a_{20} = 0$. The projection of the 3-dimensional quadratic body associated with $Q'_\sigma(X_{18}, X_{19}, 0, X_{21})$ to the X_{21}-axis is the interval $[-\sqrt{\tau_{\sigma,21}}, \sqrt{\tau_{\sigma,21}}]$, which is disjoint from $\mathbb{Z} + 1/2$. Thus we get a contradiction to $a_{21} \in \mathbb{Z} + 1/2$.

From (5.5), we have completed the proof except for the cases where $\sigma < 7$ or $(p, \sigma) = (3, 7), (7, 7), (3, 9)$. The cases where $p = 3$ or 7 can be treated by numerical calculations described in §4. Therefore we assume $p > 7$ from now on, and prove the remaining cases $\sigma < 7$.

We have $a_1 = \pm 1$. Suppose that $a_1 = 1$. For $\nu \geq 2$, we put

$$[\rho^{(\sigma)}_{\nu,-}, \rho^{(\sigma)}_{\nu,+}] := J\pi(Q_\sigma(1, 2, 0, 2, 0, \ldots, 1 + (-1)^{\nu-1}, X_\nu, \ldots, X_{21}), \{X_\nu\}).$$

Case IV-1. $\sigma = 1$. The values $\rho^{(1)}_{\nu,\pm}$ are calculated as in Table 5.4. Inductively, we obtain

$$a_\nu = 1 + (-1)^\nu \qquad \text{for } \nu = 2, \ldots, 10.$$

Since $[\rho^{(1)}_{11,-}, \rho^{(1)}_{11,+}] \cap \mathbb{Z} = \emptyset$, there are no possible values for a_{11}.

Case IV-3. $\sigma = 3$. Again we obtain $a_\nu = 1 + (-1)^\nu$ for $\nu = 2, \ldots, 6$ from Table 5.4. Since $[\rho^{(3)}_{7,-}, \rho^{(3)}_{7,+}] \cap \mathbb{Z} = \emptyset$ for $p > 7$, there are no possible values for a_7.

Case IV-5. $\sigma = 5$. Since

$$[\rho^{(5)}_{2,-}, \rho^{(5)}_{2,+}] = \left[\frac{8p + 10 - \sqrt{4p^2 + 25p + 25}}{5p + 5}, \frac{8p + 10 + \sqrt{4p^2 + 25p + 25}}{5p + 5}\right],$$

we have $a_2 = 2$. Since

$$[\rho^{(5)}_{3,-}, \rho^{(5)}_{3,+}] = \left[\frac{2p - \sqrt{55p + 75}}{8p + 10}, \frac{2p + \sqrt{55p + 75}}{8p + 10}\right],$$

there are no possible values for a_3 except for the cases $p \leq 11$. The case $p = 11$ can be treated by numerical calculations.

The case where $a_1 = -1$ can be dealt with in the same way. □

Numerical experiments show that, if $3 < p < 10000$, then we have

$$R_{(X,L)} = \Sigma(h_0^\perp) = A_1 + D_{20-2\sigma}.$$

When $p = 3$, we have

$$R_{(X,L)} = \Sigma(h_0^\perp) = A_2 + D_{20-2\sigma}.$$

In the case $\sigma = 1$, the branch curve $B_{(X,L)}$ yields another example of a sextic curve with only rational double points such that the total Milnor number is 20.

References

1. M. Artin, *Supersingular K3 surfaces*, Ann. Sci. École Norm. Sup. (4) **7** (1974), 543–567 (1975).
2. N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV-Chapitre VI*, Hermann, Paris, 1968.
3. J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Springer-Verlag, New York, 1999.
4. W. Ebeling, *Lattices and codes*, Friedr. Vieweg & Sohn.
5. T. Ibukiyama, *A basis for the algebra of quaternions over the field of rational numbers and its maximal orders*, in Japanese, Sûgaku **24** (1972), 316–318.
6. V. V. Nikulin, *Weil linear systems on singular K3 surfaces*, Algebraic geometry and analytic geometry (Tokyo, 1990), Springer, Tokyo, 1991, pp. 138–164.

ν	$\rho^{(1)}_{\nu,\pm}$	$\rho^{(3)}_{\nu,\pm}$
2	$\dfrac{16\,p+2\ \pm\ \sqrt{40\,p^2+13\,p+1}}{9\,p+1}$	$\dfrac{12\,p+6\ \pm\ 3\sqrt{2\,p^2+3\,p+1}}{7\,p+3}$
3	$\dfrac{2\,p\ \pm\ \sqrt{92\,p^2+35\,p+3}}{16\,p+2}$	$\dfrac{2\,p\ \pm\ \sqrt{34\,p^2+69\,p+27}}{12\,p+6}$
4	$\dfrac{42\,p+6\ \pm\ \sqrt{154\,p^2+64\,p+6}}{23\,p+3}$	$\dfrac{30\,p+18\ \pm\ \sqrt{50\,p^2+120\,p+54}}{17\,p+9}$
5	$\dfrac{4\,p\ \pm\ \sqrt{198\,p^2+96\,p+10}}{28\,p+4}$	$\dfrac{4\,p\ \pm\ \sqrt{46\,p^2+168\,p+90}}{20\,p+12}$
6	$\dfrac{60\,p+10\ \pm\ \sqrt{234\,p^2+129\,p+15}}{33\,p+5}$	$\dfrac{40\,p+30\ \pm\ 3\sqrt{4\,p^2+23\,p+15}}{23\,p+15}$
7	$\dfrac{6\,p\ \pm\ \sqrt{234\,p^2+159\,p+21}}{36\,p+6}$	$\dfrac{2\,p\ \pm\ \sqrt{25\,p+21}}{8\,p+6}$
8	$\dfrac{70\,p+14\ \pm\ 2\sqrt{55\,p^2+46\,p+7}}{39\,p+7}$	
9	$\dfrac{4\,p\ \pm\ \sqrt{41\,p^2+50\,p+9}}{20\,p+4}$	
10	$\dfrac{72\,p+18\ \pm\ \sqrt{100\,p^2+205\,p+45}}{41\,p+9}$	
11	$\dfrac{10\,p\ \pm\ \sqrt{195\,p+55}}{40\,p+10}$	

TABLE 5.4. The table of $\rho^{(1)}_{\nu,\pm}$ and $\rho^{(3)}_{\nu,\pm}$

7. A. N. Rudakov and I. R. Šafarevič, *Supersingular $K3$ surfaces over fields of characteristic* 2, Izv. Akad. Nauk SSSR Ser. Mat. **42** (1978), no. 4, 848–869: Igor R. Shafarevich, Collected mathematical papers, Springer-Verlag, Berlin, 1989, pp. 614–632.
8. A. N. Rudakov and I. R. Šafarevič, *Surfaces of type $K3$ over fields of finite characteristic*, Current problems in mathematics, Vol. 18, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1981, pp. 115–207: Igor R. Shafarevich, Collected mathematical papers, Springer-Verlag, Berlin, 1989, pp. 657–714.
9. J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York, 1973.
10. I. Shimada, *Rational double points on supersingular $K3$ surfaces*, to appear in Math. Comp.
11. T. Shioda, *Supersingular $K3$ surfaces*, Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), Lecture Notes in Math., Vol. 732, Springer, Berlin, 1979, pp. 564–591.
12. T. Urabe, *Dynkin graphs and combinations of singularities on plane sextic curves*, Singularities (Iowa City, IA, 1986), Amer. Math. Soc., Providence, RI, 1989, pp. 295–316.
13. B. B. Venkov, *On the classification of integral even unimodular 24-dimensional quadratic forms* Trudy Mat. Inst. Steklov. **148** (1978), 65–76.
14. Jin-Gen Yang, *Sextic curves with simple singularities*, Tohoku Math. J. (2) **48** (1996), no. 2, 203–227.

Division of Mathematics, Graduate School of Science, Hokkaido University, Sapporo 060-0810, JAPAN
E-mail address: shimada@math.sci.hokudai.ac.jp