DYNKIN DIAGRAMS OF RANK 20 ON SUPERSINGULAR $K3$ SURFACES

ICHIRO SHIMADA AND DE-QI ZHANG

Abstract. We classify normal supersingular $K3$ surfaces Y with total Milnor number 20 in characteristic p, where p is an odd prime that does not divide the discriminant of the Dynkin type of the rational double points on Y.

1. Introduction

A *Dynkin type* is, by definition, a finite formal sum of the symbols $A_l (l \geq 1)$, $D_m (m \geq 4)$ and $E_n (n = 6, 7, 8)$ with non-negative integer coefficients. For a Dynkin type R, we denote by $L(R)$ the *negative-definite* lattice whose intersection matrix is (-1) times the Cartan matrix of type R. We denote by $\mathrm{rank}(R)$ the rank of $L(R)$, and by $\mathrm{disc}(R)$ the discriminant of $L(R)$.

A *normal* $K3$ *surface* is a normal surface whose minimal resolution is a $K3$ surface. It is well-known that a normal $K3$ surface has only rational double points as its singularities ([2, 3]). Hence we can associate a Dynkin type to the singular locus $\mathrm{Sing}(Y)$ of a normal $K3$ surface Y. The rank of the Dynkin type of $\mathrm{Sing}(Y)$ is equal to the total Milnor number of Y. In particular, it is at most 21.

If the total Milnor number of a normal $K3$ surface Y is ≥ 20, then the minimal resolution X of Y is a supersingular $K3$ surface (in the sense of Shioda [22]). In [9, Theorem 3.7], Goto proved that a normal $K3$ surface Y with total Milnor number 21 exists only when the characteristic of the base field divides the discriminant of the Dynkin type of $\mathrm{Sing}(Y)$. In [18], the first author made the complete list of the pairs (R, p) of a Dynkin type R of rank 21 and a prime integer p such that R is the Dynkin type of the singular locus of a normal $K3$ surface in characteristic p.

In this paper, we investigate normal $K3$ surfaces with total Milnor number 20.

Definition 1.1. Let R be a Dynkin type of rank 20. A prime integer p is called an *R-supersingular $K3$ prime* if it satisfies the following:

(i) p does not divide $2\,\mathrm{disc}(R)$, and
(ii) there exists a normal $K3$ surface Y defined over an algebraically closed field of characteristic p such that $\mathrm{Sing}(Y)$ is of type R.

We will prove that, if p is an R-supersingular $K3$ prime for a Dynkin type R with $\mathrm{rank}(R) = 20$, and if Y is a normal $K3$ surface in the condition (ii) above, then the Artin invariant of the minimal resolution of Y is 1. It is known that, for each p, the supersingular $K3$ surface with Artin invariant 1 is unique up to isomorphisms ([13, 7]). Therefore the condition (i) and (ii) above is equivalent to (i) and the following:

1991 *Mathematics Subject Classification.* 14J28.

(ii)$'$ the supersingular $K3$ surface X in characteristic p with Artin invariant 1 is birational to a normal $K3$ surface Y such that $\mathrm{Sing}(Y)$ is of type R.

In this paper, we present an algorithm to determine the set of R-supersingular $K3$ primes for a given Dynkin type R of rank 20. As a corollary, we prove the following.

Theorem 1.2. *Let R be a Dynkin type of rank 20, and let a_R be the product of the odd prime divisors of $\mathrm{disc}(R)$. We put $b_R := 8a_R$ if $\mathrm{disc}(R)$ is even, while $b_R := a_R$ if $\mathrm{disc}(R)$ is odd. Then there exists a subset Σ_R of $(\mathbb{Z}/b_R\mathbb{Z})^\times$ such that a prime integer p is an R-supersingular $K3$ prime if and only if $p \bmod b_R \in \Sigma_R$.*

In fact, we have a result finer than above. Let Y be a normal supersingular $K3$ surface in characteristic $p \neq 2$ such that $\mathrm{Sing}(Y)$ is of Dynkin type R with $\mathrm{rank}(R) = 20$, and let $X \to Y$ be the minimal resolution of Y. We denote by L_Y the sublattice of the Néron-Severi lattice $\mathrm{NS}(X)$ of X generated by the classes of the exceptional curves of $X \to Y$. Then L_Y is isomorphic to $L(R)$. Let T_Y denote the orthogonal complement of L_Y in $\mathrm{NS}(X)$. Then T_Y is an even indefinite lattice of rank 2. Our key observation is the following:

$$tt' \in p\mathbb{Z} \quad \text{for all} \quad t, t' \in T_Y, \tag{1.1}$$

where $tt' \in \mathbb{Z}$ is the intersection number of the classes t and t' in $\mathrm{NS}(X)$. Thus we can define an indefinite lattice T'_Y of rank 2 by introducing a new bilinear form

$$(t, t')_{T'_Y} := \frac{1}{p}(tt').$$

on the $\mathbb{Z}$-module underlying T_Y. It turns out that $\mathrm{disc}(T'_Y)$ divides $\mathrm{disc}(R)$. Note that, since p is odd, T'_Y is an even lattice. Let $\widetilde{L}_Y$ be the orthogonal complement of T_Y in $\mathrm{NS}(X)$. Then $\widetilde{L}_Y$ is an even overlattice of L_Y such that the set $\mathrm{roots}(\widetilde{L}_Y)$ of roots in $\widetilde{L}_Y$ coincides with the set $\mathrm{roots}(L_Y)$ of roots in L_Y. The following is a refinement of Theorem 1.2.

Theorem 1.3. *Let R be a Dynkin type of rank 20, let T' be an even indefinite lattice of rank 2 such that $\mathrm{disc}(T')$ divides $\mathrm{disc}(R)$, and let $\widetilde{L}$ be an even overlattice of $L(R)$ such that $\mathrm{roots}(\widetilde{L}) = \mathrm{roots}(L(R))$. Then there exist a subset S_l of $\{1, -1\}$ for each odd prime divisor l of $\mathrm{disc}(R)$, and a subset S_2 of $\{1, 3, 5, 7\}$, such that the following holds. There exists a normal $K3$ surface Y in characteristic $p > 2$ with $\mathrm{Sing}(Y)$ being of type R such that $T'_Y \cong T'$ and $\widetilde{L}_Y \cong \widetilde{L}$ if and only if*

(1.2) *$\left(\frac{p}{l}\right) \in S_l$ for each odd prime divisor l of $\mathrm{disc}(R)$, and*
$p \bmod 8 \in S_2$.

If $\mathrm{disc}(R)$ is odd, then we have $S_2 = \{1, 3, 5, 7\}$.

Using computer, we have made the complete list of R-supersingular $K3$ primes, which is too large to be included in this paper. It is available from the first author's home page:

`http://www.math.sci.hokudai.ac.jp/~shimada/preprints.html`

From this list, we derive the following fact:

Theorem 1.4. *For each Dynkin type R with $\mathrm{rank}(R) = 20$, the set of R-supersingular $K3$ primes is either empty or has a natural density $1/2$.*

As another corollary of the key observation (1.1), we obtain the following:

Corollary 1.5. *Let $Y \subset \mathbb{P}^N$ be a normal supersingular $K3$ surface of total Milnor number* 20 *such that* $\operatorname{Sing}(Y)$ *is of type R. If the characteristic p of the base field does not divide* $2\operatorname{disc}(R)$*, then the degree of Y is divisible by $2p$.*

Indeed the class of the pull-back of the hyperplane section of Y to X is contained in T_Y. Note that, if R is of rank 20, then every prime divisor of $\operatorname{disc}(R)$ is ≤ 19. Combining Corollary 1.5 with [9, Theorem 3.7], we obtain the following:

Corollary 1.6. *Let Y be a normal $K3$ surface of degree d in characteristic $p > 19$. If $d \bmod p \not\equiv 0$, then the total Milnor number of Y is ≤ 19.*

In particular, a sextic plane curve $C \subset \mathbb{P}^2$ or a quartic surface $S \subset \mathbb{P}^3$ in characteristic $p > 19$ with only rational double points as its singularities has total Milnor number ≤ 19. Yang [24, 25] classified all possible configurations of rational double points on sextic plane curves and quartic surfaces in characteristic 0. It would be interesting to investigate Yang's classification in characteristic $p > 19$.

In our previous paper [21], we have proved that normal $K3$ surfaces with ten ordinary cusps exist only in characteristic 3. This implies that the set of $10A_2$-supersingular $K3$ primes is empty. More generally, the proof of Dolgachev-Keum [6, Lemma 3.2] shows that, if $\operatorname{disc}(R)$ is a square integer, then there exist no R-supersingular $K3$ primes. (See Lemma 2.3.) There are 3058 Dynkin types of rank 20. Among them, there exist 2437 Dynkin types R such that $\operatorname{disc}(R)$ is not a square integer, and 483 Dynkin types with non-empty set of R-supersingular $K3$ primes.

This paper is organized as follows. In §2, we reduce the problem of determining R-supersingular $K3$ primes to the calculation of overlattices of $L(R)$ and their quadratic forms. In §3, we investigate how the multiplications by odd prime integers affects the isomorphism classes of finite quadratic forms. In §4, we present an algorithm to calculate the set of R-supersingular $K3$ primes. In the last section, we explain the algorithm in detail by using an example.

Acknowledgment. This work was done during the first author's stay in National University of Singapore in September 2005 under the financial support from JSPS and NUS. He would like to express his gratitude to both of them.

2. Lattice theory

A free $\mathbb{Z}$-module Λ of finite rank with a non-degenerate symmetric bilinear form $\Lambda \times \Lambda \to \mathbb{Z}$ is called a *lattice*. Let Λ be a lattice. The *dual lattice* $\Lambda^\vee$ of Λ is the $\mathbb{Z}$-module $\operatorname{Hom}(\Lambda, \mathbb{Z})$. Then Λ is naturally embedded into $\Lambda^\vee$ as a submodule of finite index. There exists a natural $\mathbb{Q}$-valued symmetric bilinear form on $\Lambda^\vee$ that extends the $\mathbb{Z}$-valued symmetric bilinear form on Λ. An *overlattice* of Λ is a submodule N of $\Lambda^\vee$ containing Λ such that the bilinear form on $\Lambda^\vee$ takes values in $\mathbb{Z}$ on $N \times N$. If Λ is a sublattice of a lattice Λ' with finite index, then Λ' is embedded into $\Lambda^\vee$ in a natural way, and hence Λ' can be regarded as an overlattice of Λ.

We say that Λ is *even* if $u^2 \in 2\mathbb{Z}$ holds for every $u \in \Lambda$. Let Λ be an even negative-definite lattice. A vector $r \in \Lambda$ is called a *root* if $r^2 = -2$. We denote by $\operatorname{roots}(\Lambda)$ the set of roots in Λ. For a Dynkin type R, we put

$$\mathcal{OL}(R) := \{\, \widetilde{L} \mid \widetilde{L} \text{ is an even overlattice of } L(R) \text{ with } \operatorname{roots}(\widetilde{L}) = \operatorname{roots}(L(R)) \,\}.$$

Let D be a finite abelian group. A *quadratic form* q on D is, by definition, a map $q : D \to \mathbb{Q}/2\mathbb{Z}$ that satisfies the following:

(i) $q(nx) = n^2 q(x)$ for any $x \in D$ and any $n \in \mathbb{Z}$, and

(ii) the map $b[q] : D \times D \to \mathbb{Q}/\mathbb{Z}$ defined by
$$b[q](x, y) := (q(x + y) - q(x) - q(y))/2$$
is a symmetric bilinear form on D.

Let q be a quadratic form on a finite abelian group D, and let H be a subgroup of D. We put
$$H^\perp := \{ \, x \in D \mid b[q](x, y) = 0 \text{ for any } y \in H \, \}.$$
We say that q is *non-degenerate* if $D^\perp = \{0\}$.

Let Λ be an even lattice. The finite abelian group $\Lambda^\vee/\Lambda$ is called the *discriminant group* of Λ, and is denoted by D_Λ. We define a quadratic form q_Λ on D_Λ by
$$q_\Lambda(\bar{x}) = x^2 \mod 2\mathbb{Z} \qquad (\text{where } \bar{x} := x \bmod \Lambda \in D_\Lambda \text{ for } x \in \Lambda^\vee),$$
and call q_Λ the *discriminant form* of Λ. It is easy to see that q_Λ is non-degenerate, and that
$$|D_\Lambda| = |\operatorname{disc}(\Lambda)|$$
holds. Let N be an even overlattice of Λ. Then we have a natural sequence of inclusions
$$\Lambda \hookrightarrow N \hookrightarrow N^\vee \hookrightarrow \Lambda^\vee.$$
Therefore $\operatorname{disc}(N)$ divides $\operatorname{disc}(\Lambda)$, and the exponent of D_N divides the exponent of D_Λ. For a prime p, we denote by $(D_\Lambda)_p$ and $(D_\Lambda)_{p'}$ the p-part and the prime-to-p part of D_Λ, and by $(q_\Lambda)_p$ and $(q_\Lambda)_{p'}$ the restrictions of q to $(D_\Lambda)_p$ and to $(D_\Lambda)_{p'}$, respectively. We have the following orthogonal decomposition:
$$(D_\Lambda, q_\Lambda) = ((D_\Lambda)_p, (q_\Lambda)_p) \oplus ((D_\Lambda)_{p'}, (q_\Lambda)_{p'}).$$

We now state the main theorem of this section.

Theorem 2.1. *Let R be a Dynkin type with* $\operatorname{rank}(R) = 20$*, and let p be a prime such that $p \nmid 2\operatorname{disc}(R)$. Then the following three conditions are equivalent:*

1. *p is an R-supersingular $K3$ prime.*
2. *The unique supersingular $K3$ surface X of Artin invariant $\sigma(X) = 1$ in characteristic p is birational to a normal $K3$ surface Y such that* $\operatorname{Sing}(Y)$ *is of Dynkin type R.*
3. *There exist an overlattice $\widetilde{L} \in \mathcal{OL}(R)$ and a lattice T' of rank 2 with signature $(1, 1)$ such that $(D_{T'}, pq_{T'})$ is isomorphic to $(D_{\widetilde{L}}, -q_{\widetilde{L}})$, where $pq_{T'}$ is the discriminant form of T' multiplied by p.*

Remark 2.2. (1) Since $-\operatorname{disc}(T') = \operatorname{disc}(\widetilde{L}) = \operatorname{disc}(R)/|\widetilde{L} : L(R)|^2$, neither $\operatorname{disc}(R)$ nor $-\operatorname{disc}(T')$ is a square by Lemma 2.3 below.

(2) Let $\Lambda = \operatorname{NS}(X)$. Then Λ is the unique even p-elementary lattice of signature $(1, 21)$ and discriminant $-p^2$; for the uniqueness of such Λ, see Rudakov-Shafarevich [15], Conway-Sloane [4], Chapter 15. With the T constructed in Lemma 2.4, there is an embedding $\widetilde{L} \oplus T \subset \Lambda$ of finite index such that both $\widetilde{L}$ and T are primitive in Λ so that $\widetilde{L} = T^\perp$ and $T = \widetilde{L}^\perp$ in Λ; see the proof of the theorem.

The following result follows from the proof of Dolgachev-Keum [6, Lemma 3.2]. We reprove it here for the convenience of the readers.

Lemma 2.3. *Suppose that* (p, R) *satisfies the condition in Theorem 2.1 (1). Then* $\mathrm{disc}(R)$ *is not a perfect square.*

Proof. By the assumption on (p, R), there exist a K3 surface X and 20 curves on X whose cohomology classes span a sublattice $L(R) \subset \mathrm{NS}(X)$ of Dynkin type R and which are contractible to rational double points on a normal K3 surface Y. Since $\rho(X) \geq 1 + 20$, we have $\rho(X) = 22$ and X is supersingular (Artin [1]). Let $T = L(R)^{\perp}$ in $\mathrm{NS}(X)$. Then $L(R) \oplus T$ is a sublattice of $\mathrm{NS}(X)$ of index a say. So we have:

$$(*) \quad \mathrm{disc}(R)\ \mathrm{disc}(T) = -a^2 p^{2\sigma(X)},$$

where $\mathrm{disc}(\mathrm{NS}(X)) = -p^{2\sigma(X)}$ with $\sigma(X) \in \{1, 2, \dots, 10\}$ the Artin invariant (being 1 now, indeed).

Suppose the contrary that $\mathrm{disc}(R)$ is a square. Then (*) implies that $-\mathrm{disc}(T)$ is a square too. By Conway-Sloane [4], Chapter 15, §3, T represents zero: there is a non-zero vector t in T with $t^2 = 0$. We may assume that t is primitive in T. By the Riemann-Roch theorem, we may assume that t is represented by an effective divisor. Applying Rudakov-Shafarevich [15], Chapter 3, Proposition 3, there is a composition of reflections $\sigma : \mathrm{NS}(X) \to \mathrm{NS}(X)$ such that $\sigma(t)$ is represented by a general fibre F of an elliptic or quasi-elliptic fibration $\varphi : X \to \mathbb{P}^1$. There is a natural inclusion below where the lattice $F^{\perp}$ is the orthogonal in $\mathrm{NS}(X)$ of $\mathbb{Z}[F]$:

$$\sigma(L(R)) \to F^{\perp}/\mathbb{Z}[F].$$

Since $\mathrm{rank}(L(R)) = 20$, we can write $F^{\perp}/\mathbb{Z}[F] \cong K_1 \oplus \cdots \oplus K_r$ which includes $\sigma(L(R))$ as a sublattice of finite index b say; whence

$$(**) \quad \mathrm{disc}(R) = b^2 \prod_{\ell=1}^{r} \mathrm{disc}(K_\ell);$$

moreover, each K_ℓ is of Dynkin type $A_{n(\ell)}$, $D_{n(\ell)}$, or $E_{n(\ell)}$ so that φ has reducible fibres of type $\widetilde{K_\ell}$ in the notation of Cossec-Dolgachev [5]; see the reasoning below and the proof of Lemma 2.2 in Kondo [10]. Let $j : J \to \mathbb{P}^1$ be the Jacobian fibration of φ so that j and φ have the same type of singular fibres. We note that $\rho(J) = 2 + 20$, J is supersingular, and J has a torsion Mordell-Weil group $MW(j)$. By Shioda [23], Theorem 1.3, we have

$$(***) \quad \prod_{\ell=1}^{r} \mathrm{disc}(K_\ell) = -p^{2\sigma(J)} |MW(j)|^2,$$

where $\mathrm{disc}(\mathrm{NS}(J)) = -p^{2\sigma(J)}$ with $\sigma(J) \in \{1, 2, \dots, 10\}$. Now (***) and (**) imply that p divides $\mathrm{disc}(R)$, a contradiction. So the lemma is true. □

The following easy result will be used in the proof of Theorem 2.1.

Lemma 2.4. *Let* $T' = \mathbb{Z}[t'_1, t'_2]$ *be a rank two lattice with the intersection matrix* $(t'_i.t'_j) = (t'_{ij})$. *Let* p *be a prime which does not divide* $\mathrm{disc}(T')$. *Define a lattice* $T = \mathbb{Z}[t_1, t_2]$ *so that the intersection matrix* $(t_i.t_j) = (t_{ij})$ *with* $t_{ij} = pt'_{ij}$. *Then the following are true.*

1. $((D_T)_{p'}, (q_T)_{p'}) \cong (D_{T'}, pq_{T'})$.
2. *We have* $\mathrm{disc}(T) = p^2\,\mathrm{disc}(T')$ *and*

$$T^{\vee}/T \cong \mathbb{Z}/(p\ell_1) \oplus \mathbb{Z}/(p\ell_2), \quad (T')^{\vee}/T' \cong \mathbb{Z}/(\ell_1) \oplus \mathbb{Z}/(\ell_2).$$

Proof. Since $\operatorname{rank}(T') = 2$, we can write $(T')^\vee/T' \cong \mathbb{Z}/(\ell_1) \oplus \mathbb{Z}/(\ell_2)$ so that $\ell_i > 0$, $\ell_1|\ell_2$ and $\operatorname{disc}(T') = \det(t'_{ij}) = \ell$ with $|\ell| = \ell_1\ell_2$. We can calculate the dual bases of T' and T as follows, where $s_{11} = t'_{22}$, $s_{22} = t'_{11}$ and $s_{12} = s_{21} = -t'_{12} = -t'_{21}$:

$$((t'_1)^*, (t'_2)^*) = (t'_1, t'_2)(t'_{ij})^{-1} = \frac{1}{\ell}(t'_1, t'_2)(s_{ij}),$$

$$(t^*_1, t^*_2) = (t_1, t_2)(t_{ij})^{-1} = \frac{1}{p^2\ell}(t_1, t_2)(ps_{ij}).$$

Note that $(T^\vee/T)_{p'}$ is generated by (cosets of) the two coordinates of the vector:

$$(pt^*_1, pt^*_2) = \frac{p}{\ell}(t_1, t_2)(s_{ij}).$$

Set $b_{T'} = b[q_{T'}]$, etc. Then

$$(b_{T'}((t'_i)^*, (t'_j)^*)) = (t'_{ij})^{-1} = \frac{1}{\ell}(s_{ij}),$$

$$(b_T(t^*_i, t^*_j)) = (t_{ij})^{-1} = \frac{1}{p^2\ell}(ps_{ij}).$$

One can check that the following is an isomorphism of abelian groups:

$$(T')^\vee/T' \to (T^\vee/T)_{p'}$$

$$(t'_i)^* + T' \mapsto pt^*_i + T.$$

Under the identification via this map, we have $pq_{T'} = (q_T)_{p'}$. This proves (1). Clearly, $\operatorname{disc}(T) = \det(t_{ij}) = p^2 \operatorname{disc}(T')$. Also the expression of the dual basis shows that $(T^\vee/T)_p$ is p-elementary. Thus (2) follows. This proves the lemma. □

The following is the key to the proof of Theorem 2.1.

Proposition 2.5. *Let R be a Dynkin type with* $\operatorname{rank}(R) = 20$*, and let $L \in \mathcal{OL}(R)$ (but we do not assume that* $\operatorname{roots}(L) = \operatorname{roots}(R)$*). Suppose that $p \not| 2\operatorname{disc}(L)$ (this is true if $p \not| 2\operatorname{disc}(R)$).*

1. *Suppose that $L \to \Lambda$ is a primitive embedding into an even p-elementary lattice of signature $(1, 21)$ with non-cyclic $\Lambda^\vee/\Lambda$. Let $T = L^\perp$ be the orthogonal (of signature $(1, 1)$) of L in Λ. Then* (1a) $\sim$ (1e) *below are true.*
   - (1a) *T is an even lattice of index $(1, 1)$ such that $\operatorname{disc}(T) = -p^2 \operatorname{disc}(L)$ and $T^\vee/T \cong \mathbb{Z}/(p\ell_1) \oplus \mathbb{Z}/(p\ell_2)$.*
   - (1b) *There are a canonical isomorphism $\varphi : L^\vee/L \to (T^\vee/T)_{p'}$ and the relation $(q_T)_{p'} = -q_L$ (after the identification via φ).*
   - (1c) *Write $T = \mathbb{Z}[t_1, t_2]$. Then $(t_i.t_j) = p(t'_{ij})$ for some $t'_{ij} \in \mathbb{Z}$.*
   - (1d) *Let $T' = \mathbb{Z}[t'_1, t'_2]$ be the lattice with signature $(1, 1)$ and intersection form $(t'_i.t'_j) = (t'_{ij})$. Then $(D_{T'}, pq_{T'}) \cong ((D_T)_{p'}, (q_T)_{p'}) \cong (D_L, -q_L)$.*
   - (1e) *Λ is the unique even p-elementary lattice of signature $(1, 21)$ and discriminant $-p^2$.*
2. *Conversely, suppose that T is a lattice of signature $(1, 1)$ satisfying (1a) and (1b). Then there is a primitive embedding $L \to \Lambda$ into the unique p-elementary even lattice Λ of signature $(1, 21)$ and determinant $-p^2$ such that T (as a lattice) is isomorphic to $L^\perp$ in Λ.*

Proof. We first prove Proposition 2.5 (1). Consider the inclusions:

$$(*)\quad L \oplus T \subset \Lambda \subset \Lambda^\vee \subset L^\vee \oplus T^\vee.$$

Since $L \to \Lambda$ is a primitive embedding, its dual is a surjection $\Lambda^\vee \to L^\vee$ which factors as $\Lambda^\vee \to L^\vee \oplus T^\vee \to L^\vee$ where the first is the inclusion in (*) while the second is the projection. This surjection induces surjections $\Lambda^\vee/(L \oplus T) \to L^\vee/L$ and $\varphi_1 : (\Lambda^\vee/(L \oplus T))_{p'} \to (L^\vee/L)_{p'} = L^\vee/L$ where the latter equality is because $\gcd(p, \operatorname{disc}(L)) = 1$. Since Λ is p-elementary we have $(\Lambda^\vee/\Lambda)_{p'} = 0$ and hence $(\Lambda^\vee/(L \oplus T))_{p'} = (\Lambda/(L \oplus T))_{p'}$. Similarly, we have surjection $\varphi_2 : (\Lambda^\vee/(L \oplus T))_{p'} \to (T^\vee/T)_{p'}$. On the other hand, the inclusion (*) and the assumption that Λ is p-elementary imply $|L^\vee/L|\,|(T^\vee/T)_{p'}| = |(\Lambda/(L \oplus T))_{p'}|^2 \geq |L^\vee/L|\,|(T^\vee/T)_{p'}|$ where the latter inequality is due to the surjectivity of both φ_i. Thus both φ_i are isomorphisms. Set $\varphi = \varphi_2\,\varphi_1^{-1} : L^\vee/L \to (T^\vee/T)_{p'}$. For every $\overline{r'} \in L^\vee/L$, we write $\varphi(\overline{r'}) = \overline{t'}$, and see that the coset of $r' + t'$ belongs to $(\Lambda/(L \oplus T))_{p'}$. So $0 = q_\Lambda(\overline{r' + t'}) = q_R(\overline{r'}) + (q_T)_{p'}(\overline{t'})$. This proves (1b).

Let e be the exponent of the abelian group $L^\vee/L$ so that the latter is e-torsion. This e is coprime to p by the assumption. Then $\Lambda/(L \oplus T)$ $(\cong (L^\vee \oplus T^\vee)/\Lambda^\vee)$ is e-torsion. Indeed, for $r' + t' \in \Lambda \subset L^\vee \oplus T^\vee$, we have, mod $L \oplus T$, that $e(r' + t') = et' \in \Lambda \cap L^\perp = T$. So $\Lambda/(L \oplus T)$ equals $(\Lambda/(L \oplus T))_{p'}$ and is isomorphic to both $L^\vee/L$ and $(T^\vee/T)_{p'}$ via φ_i's; denote by r the order of these three isomorphic groups, which is coprime to p.

We assert that $T^\vee/T$ is pe-torsion. Indeed, for $t' \in T^\vee$, we have $et' \in \Lambda^\vee$ and hence $pet' \in \Lambda \cap L^\perp = T$, because Λ is p-elementary. Since T is of rank 2, we have $T^\vee/T \cong \mathbb{Z}/(p^{\varepsilon_1}\ell_1) \oplus \mathbb{Z}/(p^{\varepsilon_2}\ell_2)$ where $\ell_i > 1$, each $\varepsilon_i \in \{0, 1\}$ and $\gcd(p, \ell_i) = 1$. Note that $\Lambda^\vee/\Lambda \cong (\mathbb{Z}/(p))^{\oplus\lambda}$ for some $\lambda \geq 2$. The inclusion (*) above implies that $-p^{\varepsilon_1+\varepsilon_2}\ell_1\ell_2 \operatorname{disc}(L) = \operatorname{disc}(T)\operatorname{disc}(L) = r^2 \operatorname{disc}(\Lambda) = -p^\lambda r^2$. So $|\Lambda| = -p^2$ and both $\varepsilon_i = 1$. Note also that $\ell_1\ell_2 = |(T^\vee/T)_{p'}| = r = \operatorname{disc}(L)$. This proves (1a) and (1e). The assertion (1c) is the observation in (1a) that $(T^\vee/T)_p$ is p-elementary, $\operatorname{rank}(T) = 2$ and $\operatorname{disc}(T) = p^2\times$ (some integer coprime to p) and that the calculation of $T^\vee/T$ is essentially the calculation of the matrix $(t_i.t_j)^{-1}$; see Lemma 2.4. The assertion (1d) follows from (1b) and Lemma 2.4 by noting that p does not divide $\operatorname{disc}(T') = -\operatorname{disc}(L)$.

Next we prove Proposition 2.5 (2). We define an overlattice Γ of $L \oplus T$ by adding elements $r' + t' \in L^\vee \oplus T^\vee$ such that $\varphi(\overline{r'}) = \overline{t'}$. Note that $q_{L\oplus T}(\overline{r' + t'}) = q_L(\overline{r'}) + (q_T)_{p'}(\overline{t'}) = 0$, so Γ is an even overlattice of $L \oplus T$ such that the projections induce isomorphisms: $L^\vee/L \cong \Gamma/(L \oplus T) \cong (T^\vee/T)_{p'}$. Now $|\Gamma| = |L \oplus T|/\operatorname{disc}(L)^2 = \operatorname{disc}(T)/\operatorname{disc}(L) = -p^2$ by (1a). Consider the inclusion (*) above but with Λ replaced by Γ, we see that $\Gamma^\vee/\Gamma = (\Gamma^\vee/\Gamma)_p$ is p-torsion because so is $((L^\vee \oplus T^\vee)/(L \oplus T))_p = (T^\vee/T)_p$ by (1a). So Γ is p-elementary. It is clear from the construction that both $L \to \Gamma$ and $T \to \Gamma$ are primitive embeddings, whence $T = L^\perp$ in Γ. This proves Proposition 2.5. $\square$

We now prove Theorem 2.1, the direction (1) $\Longrightarrow$ (2). So there is a normal $K3$ surface Y defined over an algebraically closed field k with $\operatorname{char}(k) = p$ such that $\operatorname{Sing}(Y)$ is of Dynkin type R. Let $f : X \to Y$ be the minimal resolution and $\operatorname{Ex}(f)$ the reduced exceptional divisor. Then $\operatorname{Ex}(f)$ is also of Dynkin type R. Since the Picard number $\rho(X) = \rho(Y) + \#\operatorname{Ex}(f) \geq 21$, we have $\rho(X) = 22$ (see Artin [1]) and hence X is supersingular in the sense of Shioda [22]. Let $\Lambda = \operatorname{NS}(X)$. Then Λ is p-elementary and $|\Lambda| = -p^{2\sigma}$ where $1 \leq \sigma \leq 10$ is the Artin invariant (Artin

[1], Rudakov-Shafarevich [14]). Let L denote the sublattice (of Dynkin type R) of Λ spanned by cohomology classes of irreducible components in $\mathrm{Ex}(f)$. Let $\widetilde{L}$ be the closure of the sublattice L in Λ. Applying Proposition 2.5 to the primitive embedding $\widetilde{L} \to \Lambda$, we see that $\sigma = 1$. So Theorem 2.1 (2) is true.

Next we prove Theorem 2.1, the direction (2) $\Longrightarrow$ (3). We use the notation above. We assert that $\mathrm{roots}(\widetilde{L}) = \mathrm{roots}(L)$. Indeed, suppose that $v \in \widetilde{L}$ is a (-2)-vector. By considering $-v$ and the Riemann-Roch theorem, we may assume that v is represented by an effective divisor V on X. Since this V is perpendicular to the pull back of an ample divisor on Y, our V is contractible to a point on Y, whence $v = [V]$ belongs to L. The assertion is proved. The rest of (3) follows from Proposition 2.5 applied to the primitive embedding $\widetilde{L} \to \Lambda$.

Finally, we prove Theorem 2.1, the direction (3) $\Longrightarrow$ (1). Define T as in Lemma 2.4. Then Propositions 2.5 (1a) and (1b) are satisfied by $\widetilde{L}$ and T. By Proposition 2.5 (both assertions there), there is a primitive embedding $\widetilde{L} \to \Lambda$ into the unique even p-elementary lattice of signature $(1, 21)$ and discriminant $-p^2$ such that $T = \widetilde{L}^{\perp}$ in Λ. Let $X = X_p$ be a supersingular $K3$ surface with $\mathrm{NS}(X) = \Lambda$ (see Rudakov-Shafarevich [14], Shioda [22]).

Take a primitive element v in $T^{\vee}$ such that $v^2 < -2$. Let h be a generator of $v^{\perp} \cap T^{\vee}$. So $h^2 > 0$. We claim that $\mathrm{roots}(h^{\perp} \cap \Lambda) = \mathrm{roots}(\widetilde{L})$. It is clear that LHS includes RHS. Let u be in LHS. Write $u = r' + t'$ with $r' \in \widetilde{L}^{\vee}$ and $t' \in T^{\vee}$. Then $0 = h.u = h.t'$, whence $t' \in T^{\vee} \cap h^{\perp} = \mathbb{Z}[v]$. So $t' = mv$ for some integer m. If $m \neq 0$, then $-2 = u^2 = (r')^2 + (t')^2 \leq m^2 v^2 < -2$, absurd. So $m = 0$ and $u = r' \in \widetilde{L}^{\vee} \cap \Lambda = \widetilde{L}$ and hence $u \in$ RHS. The claim is proved. By considering $-h$ and isometry of Λ, we may assume that a positive multiple of h is represented by a nef and big Cartier divisor H on X (see Rudakov-Shafarevich [14]). Note that $|2H|$ is base point free (see Nikulin [12], Proposition 0.1 and Saint-Donat [16], Corollary 3.2). Let $f : X \to Y$ be the birational morphism onto a normal surface, which is the Stein factorization of $\Phi_{|2H|} : X \to \mathbb{P}^N$ with $N = \dim |2H|$. Then f is nothing but the contraction of all the curves perpendicular to H. So by the genus formula and the Riemann-Roch theorem, $\mathrm{Ex}(f)$ contains and consists of all curves representing elements in $\mathrm{roots}(h^{\perp} \cap \Lambda) = \mathrm{roots}(\widetilde{L}) = \mathrm{roots}(L(R))$, whence $\mathrm{Ex}(f)$ is of Dynkin type R. Thus Y is a normal $K3$ surface with $\mathrm{Sing}(Y)$ of Dynkin type R. Hence the assertion (1) is true. This completes the proof of Theorem 2.1.

3. Finite quadratic forms

Let q and q' be quadratic forms on a finite abelian group D. We denote by d the order of D. In this subsection, we consider the set $K(q, q')$ of odd prime integers prime to d such that (D, pq) is isomorphic to (D, q').

For a prime l, we put

$$T_l := \begin{cases} (\mathbb{Z}/8\mathbb{Z})^{\times} & \text{if } l = 2, \\ \{1, -1\} & \text{if } l \neq 2, \end{cases}$$

and for a prime $p \neq l$, we define $\tau_l(p) \in T_l$ by

$$\tau_l(p) := \begin{cases} p \mod 8 & \text{if } l = 2, \\ \left(\frac{p}{l}\right) & \text{if } l \neq 2. \end{cases}$$

We then put

$$T_d := \prod_l T_l$$

where l runs through the prime divisors of d, and put

$$\tau_d(p) := (\tau_l(p)) \quad \in \quad T_d$$

for an odd prime integer p prime to d.

Proposition 3.1. *Let p_1 and p_2 be odd prime integers prime to d. If $\tau_d(p_1) = \tau_d(p_2)$, then $p_1 \in K(q, q')$ is equivalent to $p_2 \in K(q, q')$*

Proof. It is enough to prove that $(D, p_1 q)$ and $(D, p_2 q)$ are isomorphic. Let l be an odd prime divisor of d, and let ν be the largest integer such that $l^\nu | d$. It follows from $\tau_l(p_1) = \tau_l(p_2)$ that there exists an integer a_l such that $p_1 \equiv a_l^2 p_2 \bmod l^\nu$ holds. Note that a_l is prime to l. Suppose that d is even. It follows from $\tau_2(p_1) = \tau_2(p_2)$ that there exists an integer a_2 that satisfies $p_1 \equiv a_2^2 p_2 \bmod 2^{\mu+1}$, where μ is the largest integer such that $2^\mu | d$. Note that a_2 is odd. By the Chinese Remainder Theorem, we have an integer a that satisfies $a \equiv a_l \bmod l^\nu$ for each odd prime divisor l of d, and

$$a \equiv \begin{cases} a_2 \bmod 2^{\mu+1} & \text{if } d \text{ is even,} \\ 1 \bmod 2 & \text{if } d \text{ is odd.} \end{cases}$$

Then we have $p_1 \equiv a^2 p_2 \bmod 2d$. Note that a is prime to d. Since $b[q](x, x) = q(x) \bmod \mathbb{Z}$, $q(x)$ is contained in $(1/d)\mathbb{Z}/2\mathbb{Z} \subset \mathbb{Q}/2\mathbb{Z}$ for any $x \in D$. Therefore we have

$$p_1 q = a^2 p_2 q.$$

The multiplication by a induces an automorphism α of D. Since $\alpha^*(p_2 q) = p_1 q$, we see that $p_1 q$ and $p_2 q$ are isomorphic. □

Corollary 3.2. *There exists a subset $S(q, q')$ of T_d such that $K(q, q')$ is equal to the set of odd prime integers p prime to d such that $\tau_d(p) \in S(q, q')$.*

4. Algorithm

Let R be an Dynkin type of rank 20. We put

$$T(R) := \prod_l T_l,$$

where l runs through the set of prime divisors of $\operatorname{disc}(R)$, and for a prime p that does not divide $2\operatorname{disc}(R)$, we put

$$\tau(p) := (\tau_l(p))_l \in T(R).$$

In this section, we present an algorithm to obtain a subset $S(R) \subset T(R)$ with the following property: a prime p that does not divide $2\operatorname{disc}(R)$ is an R-supersingular $K3$ prime if and only if $\tau(p) \in S(R)$.

4.1. **Step 1.** We first calculate the set of even overlattices of $L(R)$ using the proposition due to Nikulin [11, Proposition 1.4.1]. For each even overlattice $\widetilde{L}$ of $L(R)$, we can calculate the set $\operatorname{roots}(\widetilde{L})$ of roots of $\widetilde{L}$ by the method described in [19] and [20]. Comparing $\operatorname{roots}(\widetilde{L})$ with $\operatorname{roots}(L(R))$ for each $\widetilde{L}$, we make the set $\mathcal{OL}(R)$.

4.2. **Step 2.** We calculate the discriminant group $D_{\widetilde{L}}$ for each $\widetilde{L} \in \mathcal{OL}(R)$, and make the set $\mathcal{OL}'(R)$ of all $\widetilde{L} \in \mathcal{OL}(R)$ such that the length of $D_{\widetilde{L}}$ is ≤ 2. For each $\widetilde{L} \in \mathcal{OL}'(R)$, we calculate the isomorphism class of the finite quadratic form $(D_{\widetilde{L}}, -q_{\widetilde{L}})$.

4.3. **Step 3.** For each $\widetilde{L} \in \mathcal{OL}'(R)$, we do the following calculation. We put $d := \operatorname{disc}(\widetilde{L})$, which is a positive integer. First we make the list $\mathcal{T}(d)$ of isomorphism classes of even indefinite lattices T' of rank 2 with discriminant $-d$ using the classical theory of binary forms due to Gauss [8]. (See also [4, Chapter 15, §3.3].) For each $T' \in \mathcal{T}(d)$ we calculate the discriminant group $D_{T'}$ of T'. If $D_{T'}$ is isomorphic to $D_{\widetilde{L}}$, then we calculate the set

$$S(\widetilde{L}, T') := \prod_{l \mid \operatorname{disc}(R)} S_l(\widetilde{L}, T') \quad \subset \quad T(R)$$

such that $(D_{T'}, pq_{T'})$ is isomorphic to $(D_{\widetilde{L}}, -q_{\widetilde{L}})$ if and only if $\tau_l(p) \in S_l(\widetilde{L}, T')$ for each prime divisor l of $\operatorname{disc}(R)$. In virtue of Proposition 3.1, we have to check only a finite number of prime integers. (Note that the set of prime divisors of $|D_{\widetilde{L}}|$ is a subset of the set of prime divisors of $\operatorname{disc}(R) = |D_{L(R)}|$. If a prime divisor l of $\operatorname{disc}(R)$ does not divide $\operatorname{disc}(\widetilde{L})$, then we put $S_l(\widetilde{L}, T') = T_l$.) If $D_{T'}$ is not isomorphic to $D_{\widetilde{L}}$, then we put $S(\widetilde{L}, T') = \emptyset$.

The set $S(R)$ is the union of all $S(\widetilde{L}, T')$, where $\widetilde{L}$ runs through the set $\mathcal{OL}'(R)$ and T' runs through the set $\mathcal{T}(\operatorname{disc}(\widetilde{L}))$.

5. Example

We will explain the case

$$R := D_7 + A_{11} + 2A_1$$

in detail. The discriminant form of the negative-definite root lattice $L(R)$ is expressed by the diagonal matrix

$$\operatorname{diag}[-7/4, -11/12, -1/2, -1/2]$$

with respect to the basis of the discriminant group

$$D_{L(R)} \;\cong\; \mathbb{Z}/4\mathbb{Z} \,\times\, \mathbb{Z}/12\mathbb{Z} \,\times\, \mathbb{Z}/2\mathbb{Z} \,\times\, \mathbb{Z}/2\mathbb{Z}$$

given in [19, Section 6]. There are eight isotropic vectors in $D_{L(R)}$:

$$0 := [0,0,0,0],\ \ v_1 := [0,6,1,1],\ \ v_2 := [1,3,0,0],\ \ v_3 := [1,9,0,0],\ \ v_4 := [2,0,1,1],$$
$$v_5 := [2,6,0,0] = 2v_2 = 2v_3,\ \ v_6 := [3,3,0,0] = -v_3,\ \ v_7 := [3,9,0,0] = -v_2.$$

Let $L_{(i)}$ be the even overlattice of $L(R)$ corresponding to the totally isotropic subgroup of $D_{L(R)}$ generated by v_i. The Dynkin type of $\operatorname{roots}(L_{(i)})$ is equal to R if $i \neq 4$, while it is $A_{11} + D_9$ if $i = 4$. Hence the even overlattice $L(H)$ of $L(R)$ corresponding to an totally isotropic subgroup H satisfies $\operatorname{roots}(L(H)) = \operatorname{roots}(L(R))$ if and only if $v_4 \notin H$. The totally isotropic subgroups that do not contain v_4 are listed as follows:

$$H_0 = \{0\},\ \ H_1 = \{0, v_1\},\ \ H_2 = \{0, v_5\},\ \ H_3 = \{0, v_2, v_5, v_7\},\ \ H_4 = \{0, v_3, v_5, v_6\}.$$

Let $\gamma \in \operatorname{Aut}(L(R))$ be the isometry of $L(R) = L(D_7) \oplus L(A_{11} + 2A_1)$ that is the multiplication by -1 on the factor $L(D_7)$ and the identity on $L(A_{11} + 2A_1)$. Then the action of γ on $D_{L(R)}$ interchanges H_3 and H_4. Therefore the even lattices $L(H_3)$ and $L(H_4)$ are isomorphic. The lengths of $D_{L(H_0)}$ and $D_{L(H_2)}$ are ≥ 3, while the lengths of $D_{L(H_1)}$ and $D_{L(H_3)} \cong D_{L(H_4)}$ are 2.

The discriminant form of $L(H_1)$ multiplied by (-1) is given by

$$\left(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \left[\begin{array}{cc} 7/4 & 0 \\ 0 & 3/4 \end{array}\right]\right) \times \left(\mathbb{Z}/3\mathbb{Z}, \left[\ 2/3\ \right]\right).$$

There are four isomorphism classes of even indefinite lattices of rank 2 with discriminant -48:

$$S_\pm := \left[\begin{array}{cc} \pm 2 & 6 \\ 6 & \mp 6 \end{array}\right], \qquad T_\pm := \left[\begin{array}{cc} \pm 4 & 4 \\ 4 & \mp 8 \end{array}\right].$$

The discriminant group of $S_\pm$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, and hence is not isomorphic to $D_{L(H_1)}$. The discriminant forms of $T_\pm$ are

$$\left(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \left[\begin{array}{cc} \pm 1/4 & 0 \\ 0 & \pm 5/4 \end{array}\right]\right) \times \left(\mathbb{Z}/3\mathbb{Z}, \left[\ \pm 2/3\ \right]\right).$$

Hence we have the following equivalence for prime integers $p \neq 2, 3$:

$$\begin{array}{lcll} p \in K(-q_{L(H_1)}, q_{T_+}) & \Longleftrightarrow & p \bmod 8 \equiv 3 \text{ or } 7 \quad \text{and} & \left(\frac{p}{3}\right) = 1, \\ p \in K(-q_{L(H_1)}, q_{T_-}) & \Longleftrightarrow & p \bmod 8 \equiv 1 \text{ or } 5 \quad \text{and} & \left(\frac{p}{3}\right) = -1. \end{array}$$

There are two isomorphism classes of even indefinite lattices of rank 2 with discriminant -12:

$$U_\pm := \left[\begin{array}{cc} \pm 2 & 2 \\ 2 & \mp 4 \end{array}\right].$$

By the same calculation as above, we have the following equivalence for prime integers $p \neq 2, 3$:

$$\begin{array}{lcll} p \in K(-q_{L(H_3)}, q_{U_+}) & \Longleftrightarrow & p \bmod 8 \equiv 1 \text{ or } 5 \quad \text{and} & \left(\frac{p}{3}\right) = -1, \\ p \in K(-q_{L(H_3)}, q_{U_-}) & \Longleftrightarrow & p \bmod 8 \equiv 3 \text{ or } 7 \quad \text{and} & \left(\frac{p}{3}\right) = 1. \end{array}$$

Thanks to the equalities

$$K(-q_{L(H_1)}, q_{T_+}) = K(-q_{L(H_3)}, q_{U_-}), \quad K(-q_{L(H_1)}, q_{T_-}) = K(-q_{L(H_3)}, q_{U_+}),$$

the natural density of R-supersingular $K3$ primes is 1/2.

References

[1] M. Artin, Supersingular $K3$ surfaces. Ann. Sci. École Norm. Sup. (4) **7** (1974), 543–567 (1975).

[2] M. Artin, Some numerical criteria for contractability of curves on algebraic surfaces, Am. J. Math. **84** (1962), 485–496.

[3] M. Artin, On isolated rational singularities of surfaces, Am. J. Math. **88** (1966), 129–136.

[4] J. H. Conway and N. J. Sloane, Sphere packings, lattices and groups. Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften, **290**. Springer-Verlag, New York, 1999.

[5] F. Cossec and I. Dolgachev, Enriques surfaces. I. Progress in Mathematics, 76. Birkhäuser Boston, Inc., Boston, MA, 1989.

[6] I. Dolgachev and J. Keum, Finite groups of symplectic automorphisms of K3 surfaces in positive characteristic, math.AG/0403478.

[7] I. Dolgachev and S. Kondo, A supersingular $K3$ surface in characteristic 2 and the Leech lattice, Int. Math. Res. Not. 2003, no. 1, 1–23.

[8] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986, Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[9] Y. Goto, *On the Néron-Severi groups of some $K3$ surfaces*, The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), CRM Proc. Lecture Notes, vol. 24, Amer. Math. Soc., Providence, RI, 2000, pp. 305–328.

[10] S. Kondo, Automorphisms of algebraic $K3$ surfaces which act trivially on Picard groups. J. Math. Soc. Japan 44 (1992), no. 1, 75–98.

[11] V. V. Nikulin, Integer symmetric bilinear forms and some of their applications. Math. USSR Izvestija **14** (1980), no. 1, 103–167.

[12] V. V. Nikulin, Weil linear systems on singular $K3$ surfaces. Algebraic geometry and analytic geometry (Tokyo, 1990), 138–164, ICM-90 Satell. Conf. Proc.

[13] A. Ogus, A crystalline Torelli theorem for supersingular $K3$ surfaces, Arithmetic and geometry, Vol II, pp. 361–349, Progr. Math. 36, Birkhäuser, Boston, 1983.

[14] A. N. Rudakov and I. R. Shafarevich, Supersingular $K3$ surfaces over fields of characteristic 2. Math. USSR-Izv. **42** (1978), no. 4, 147–165 (1979).

[15] A. N. Rudakov and I. R. Shafarevich, Surfaces of type $K3$ over fields of finite characteristic. (Russian) Current problems in mathematics, Vol. **18**, pp. 115–207, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1981.

[16] B. Saint-Donat, Projective models of $K-3$ surfaces. Amer. J. Math. **96** (1974), 602–639.

[17] J.-P. Serre, A course in arithmetic. Graduate Texts in Mathematics, **7**, Springer, New York, 1973.

[18] I. Shimada, Rational double points on supersingular $K3$ surfaces. Math. Comp. **73** (2004), no. 248, 1989–2017.

[19] I. Shimada, On elliptic $K3$ surfaces. Michigan Math. J. **47** (2000), no. 3, 423–446.

[20] I. Shimada, Supersingular $K3$ surfaces in odd characteristic and sextic double planes. Math. Ann. **328** (2004), no. 3, 451–468.

[21] I. Shimada and De-Qi Zhang, $K3$ surfaces with ten cusps, Contemporary Math.; Amer. Math. Soc. (Dolgachev's volume); to appear; also math.AG/0411425.

[22] T. Shioda, Supersingular $K3$ surfaces. Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), pp. 564–591, Lecture Notes in Math., **732**.

[23] T. Shioda, On the Mordell-Weil lattices. Comment. Math. Univ. St. Paul. 39 (1990), no. 2, 211–240.

[24] Jin-Gen Yang, Sextic curves with simple singularities. Tohoku Math. J. (2) **48** (1996), no. 2, 203–227.

[25] Jin-Gen Yang, Enumeration of combinations of rational double points on quartic surfaces. Singularities and complex geometry (Beijing, 1994), AMS/IP Stud. Adv. Math., vol. 5, Amer. Math. Soc., Providence, RI, 1997, pp. 275–312.

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

Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, SINGAPORE
E-mail address: `matzdq@nus.edu.sg`