ON ELLIPTIC $K3$ SURFACES

ICHIRO SHIMADA

Abstract. We make a complete list of all possible ADE-types of singular fibers of complex elliptic $K3$ surfaces and the torsion parts of their Mordell-Weil groups.

1. Introduction

By virtue of Torelli theorem for the period map on the moduli of complex $K3$ surfaces ([4], [13], [18]), we can study many aspects of $K3$ surfaces from the lattice-theoretic point of view. In this paper, we determine all possible ADE-types of singular fibers of elliptic $K3$ surfaces using Nikulin's theory of discriminant forms of even integral lattices. We also determine, for each ADE-type of singular fibers, all possible torsion parts of the Mordell-Weil groups. Throughout this paper, we use the term "an elliptic $K3$ surface" for "a complex elliptic $K3$ surface with a distinguished zero section" and the term "an elliptic fibration" for "a complex Jacobian elliptic fibration".

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 is called an ADE-type. For an ADE-type

$$\Sigma := \sum a_l A_l + \sum d_m D_m + \sum e_n E_n,$$

we denote by $L(\Sigma)^-$ the negative-definite root lattice generated by a root system of type Σ, and by $\operatorname{rank}\Sigma$ the rank of $L(\Sigma)^-$. By definition, we have $\operatorname{rank}\Sigma = \sum a_l l + \sum d_m m + \sum e_n n$.

Let $f : X \to \mathbb{P}^1$ be an elliptic $K3$ surface, and $O : \mathbb{P}^1 \to X$ the zero section of f. Let MW_f be the Mordell-Weil group of f. The torsion part of MW_f is a finite abelian group, which we shall denote by G_f. We put

$$R_f := \{\, p \in \mathbb{P}^1 \;:\; f^{-1}(p) \text{ is reducible} \,\},$$

and, for each $p \in R_f$, we denote by $f^{-1}(p)^\sharp$ the union of irreducible components of $f^{-1}(p)$ that are disjoint from the zero section. It is known that the cohomology classes of irreducible components of $f^{-1}(p)^\sharp$ span a negative-definite root lattice generated by an indecomposable root system of type A_l, D_m or E_n. Let $\tau_{f,p}$ be the type. The type of singular fiber $f^{-1}(p)$ in the list of Kodaira's classification [7] is related to $\tau_{f,p}$ in an almost one-to-one way (cf. Table 2.8). We define the ADE-type Σ_f of $f : X \to \mathbb{P}^1$ by

$$\Sigma_f := \sum_{p \in R_f} \tau_{f,p}.$$

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

The Néron-Severi lattice NS_X of X contains the sublattice S_f generated by the cohomology classes of the irreducible components of $\cup_{p \in R_f} f^{-1}(p)^\sharp$, which is isomorphic to $L(\Sigma_f)^-$.

Through computer-aided calculation, we have made the complete list of pairs (Σ, G) of an ADE-type Σ and a finite abelian group G that can be realized as the data (Σ_f, G_f) of an elliptic $K3$ surface $f : X \to \mathbb{P}^1$. This list $\mathcal{P}$ consists of 3693 pairs. In this paper, we present the list $\mathcal{P}$, deduce some geometric facts from it, and explain the algorithm for obtaining it.

The list $\mathcal{P}$ is too large to be included here in a naive way. Therefore we describe $\mathcal{P}$ by giving a subset $\mathcal{S}$ of $\mathcal{P}$ and a set of transformation rules of ADE-types that generate $\mathcal{P}$ from $\mathcal{S}$ (cf. § 2). The reader can obtain $\mathcal{P}$ easily using this description. [1]

An elliptic $K3$ surface $f : X \to \mathbb{P}^1$ is said to be extremal if the sublattice S_f attains the maximal rank 18. After the work of Miranda and Persson [10], supplemented by Artal-Bartolo, Tokunaga and Zhang [1] and Ye [23], the ADE-types of singular fibers of extremal elliptic $K3$ surfaces and their Mordell-Weil groups were completely determined in [16]. The list consists of 336 pairs.

One of the remarkable facts that can be read off from the list $\mathcal{P}$ is that an ADE-type Σ is an ADE-type of an elliptic $K3$ surface with trivial Mordell-Weil torsion if and only if Σ is obtained from an ADE-type of an extremal elliptic $K3$ surface with trivial Mordell-Weil torsion by *elementary transformation*; that is, by deleting vertices from the corresponding Dynkin graph (cf. Theorem 2.3). In order to describe the list of ADE-types of elliptic $K3$ surfaces with non-trivial Mordell-Weil torsion, however, we have to forbid to use some types of elementary transformation (cf. Theorems 2.4-2.7).

By Nishiyama [12] and by Besser [2], the technique of discriminant forms was used to find out all possible elliptic fibrations on special $K3$ surfaces. In [19, 20], Urabe investigated possible configurations of singular points on $K3$ surfaces and suggested an existence of a set of simple rules that generates all possible configurations. In [21, 22], Yang made the complete list of all possible configurations of singularities of ADE-type on plane sextic curves and quartic surfaces using the technique of discriminant forms and a computer.

This paper is organized as follows. In § 2, we describe $\mathcal{P}$ and state some facts about elliptic $K3$ surfaces that can be derived from the list $\mathcal{P}$. In § 3, we recall the definition and properties of local invariants of lattices over $\mathbb{Z}$ according to Conway and Sloane [6, Chapter 15]. In § 4 and 5, we review Nikulin's theory [11] of discriminant forms of even lattices over $\mathbb{Z}$. A criterion whether there exists an even integral lattice of a given signature and a discriminant form is described in detail in § 5. This criterion is slightly different from [11, Theorem 1.10.1], and is more suited to machine calculation. In § 6, we recall the properties of root lattices. In § 7, we show that it is possible to determine by a purely lattice-theoretic calculation whether a given pair (Σ, G) can be realized as (Σ_f, G_f) of an elliptic $K3$ surface $f : X \to \mathbb{P}^1$. Here we use Kondo-Nishiyama's lemma on the Néron-Severi lattice of an elliptic $K3$ surface. In § 8, we explain our algorithm.

[1] The list can also be retrieved from the author's homepage.
`http://www.math.sci.hokudai.ac.jp/~shimada/K3.html`

Table 2.1. Cardinalities of $\mathcal{P}^G$

G	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[2, 2]	[4, 2]	[6, 2]	[3, 3]	[4, 4]	total
$\lvert\mathcal{P}^G\rvert$	2746	732	85	41	6	10	1	1	61	5	1	3	1	3693

The program for making $\mathcal{P}$ was written by Maple V. The author would like to thank Waterloo Maple Incorporation for developing the nice software. The author also would like to thank the referee for suggesting some improvements on the first version of the paper.

2. Main results

All results in this section are obtained simply by looking at the list $\mathcal{P}$.

2.1. **Torsion parts of Mordell-Weil groups.**

Theorem 2.1. *The torsion part of the Mordell-Weil group of an elliptic $K3$ surface is isomorphic to one of the following*:

$$\begin{gathered}(0),\ \mathbb{Z}/(2),\ \mathbb{Z}/(3),\ \mathbb{Z}/(4),\ \mathbb{Z}/(5),\ \mathbb{Z}/(6),\ \mathbb{Z}/(7),\ \mathbb{Z}/(8),\\ \mathbb{Z}/(2)\times\mathbb{Z}/(2),\ \mathbb{Z}/(4)\times\mathbb{Z}/(2),\ \mathbb{Z}/(6)\times\mathbb{Z}/(2),\\ \mathbb{Z}/(3)\times\mathbb{Z}/(3),\ \mathbb{Z}/(4)\times\mathbb{Z}/(4).\end{gathered} \tag{2.1}$$

For a group G in (2.1), we denote by $\mathcal{P}^G$ the set of all ADE-types Σ such that there exists an elliptic $K3$ surface $f : X \to \mathbb{P}^1$ with $\Sigma_f = \Sigma$ and $G_f \cong G$. The cardinalities of $\mathcal{P}^G$ are given in Table 2.1. Here, $[a]$ denotes the cyclic group $\mathbb{Z}/(a)$, and $[a, b]$ denotes $\mathbb{Z}/(a) \times \mathbb{Z}/(b)$. In particular, [1] denotes the trivial group.

For a positive integer r, let $\mathcal{P}^G_r$ be the subset of $\mathcal{P}^G$ that consists of $\Sigma \in \mathcal{P}^G$ with $\operatorname{rank}\Sigma = r$. Let $f : X \to \mathbb{P}^1$ be an elliptic $K3$ surface. Since the Néron-Severi lattice NS_X of X is the orthogonal direct sum of $S_f \cong L(\Sigma_f)^-$ and the lattice of rank 2 generated by the cohomology classes of the zero section and a general fiber, and since the Néron-Severi rank of X is at most 20, we always have

$$\operatorname{rank}(\Sigma_f) \le 18.$$

Hence $\mathcal{P}^G_r$ is empty for $r > 18$.

2.2. ADE**-types of singular fibers.**

Next we describe the list $\mathcal{P}^G$ for each abelian group G in (2.1). We carry out this task by three different methods according to the size of $\mathcal{P}^G$.

Case 1. $G \in \{[1], [2], [3], [4], [2, 2]\}$. We describe $\mathcal{P}^G$ by giving a subset $\mathcal{S}^G \subset \mathcal{P}^G$ and a set of transformation rules on ADE-types that generate the whole $\mathcal{P}^G$ from the subset $\mathcal{S}^G$.

Let $\Gamma(\Sigma)$ be the Dynkin graph of the ADE-type Σ. If we remove a vertex P of $\Gamma(\Sigma)$ and the edges emitting from P, we obtain the Dynkin graph $\Gamma(\Sigma')$ of another ADE-type Σ' with $\operatorname{rank}\Sigma' = \operatorname{rank}\Sigma - 1$. In this case, we say that Σ' is obtained from Σ by deleting a vertex. In other words, an ADE-type Σ' is obtained from Σ by deleting a vertex if and only if Σ' is obtained by applying to Σ one of the substitutions listed in Table 2.2. In this Table, we understand that $A_0 := 0$.

Table 2.2. Substitutions.

$$
\begin{array}{lll}
A_l & \mapsto & A_{l'} + A_{l-1-l'} \quad (0 \le l' \le l/2), \\
D_m & \mapsto & \begin{cases} A_{m-1}, \quad 2A_1 + A_{m-3}, \quad A_3 + A_{m-4}, \\ D_{m'} + A_{m-1-m'} \quad (4 \le m' \le m-1), \end{cases} \\
E_n & \mapsto & \begin{cases} A_{n-1}, \quad D_{n-1}, \quad A_1 + A_{n-2}, \quad A_1 + A_2 + A_{n-4}, \quad A_4 + A_{n-5}, \\ D_5 + A_{n-6}, \quad E_{n'} + A_{n-1-n'} \quad (6 \le n' \le n-1). \end{cases}
\end{array}
$$

Definition 2.2. When we can obtain an ADE-type Σ' from an ADE-type Σ by applying substitutions in Table 2.2 several times, we say that Σ' is obtained from Σ by *elementary transformation.*

Theorem 2.3. (1) *The list* $\mathcal{P}^{[1]}_{18}$ *consists of* 199 *elements listed below.*
$2E_8 + A_2$, $2E_8 + 2A_1$, $E_8 + E_7 + A_3$, $E_8 + E_7 + A_2 + A_1$, $E_8 + E_6 + D_4$, $E_8 + E_6 + A_4$, $E_8 + E_6 + A_3 + A_1$, $E_8 + D_{10}$, $E_8 + D_9 + A_1$, $E_8 + D_7 + A_2 + A_1$, $E_8 + D_6 + A_4$, $E_8 + D_6 + 2A_2$, $E_8 + 2D_5$, $E_8 + D_5 + A_5$, $E_8 + D_5 + A_4 + A_1$, $E_8 + A_{10}$, $E_8 + A_9 + A_1$, $E_8 + A_8 + A_2$, $E_8 + A_8 + 2A_1$, $E_8 + A_7 + A_2 + A_1$, $E_8 + A_6 + A_4$, $E_8 + A_6 + A_3 + A_1$, $E_8 + A_6 + 2A_2$, $E_8 + A_6 + A_2 + 2A_1$, $E_8 + 2A_5$, $E_8 + A_5 + A_4 + A_1$, $E_8 + A_5 + A_3 + A_2$, $E_8 + 2A_4 + 2A_1$, $E_8 + A_4 + A_3 + A_2 + A_1$, $E_8 + 2A_3 + 2A_2$, $2E_7 + A_4$, $2E_7 + 2A_2$, $E_7 + E_6 + D_5$, $E_7 + E_6 + A_5$, $E_7 + E_6 + A_4 + A_1$, $E_7 + E_6 + A_3 + A_2$, $E_7 + D_{11}$, $E_7 + D_9 + A_2$, $E_7 + D_7 + A_4$, $E_7 + D_5 + A_6$, $E_7 + D_5 + A_4 + A_2$, $E_7 + A_{11}$, $E_7 + A_{10} + A_1$, $E_7 + A_9 + A_2$, $E_7 + A_8 + A_3$, $E_7 + A_8 + A_2 + A_1$, $E_7 + A_7 + A_4$, $E_7 + A_7 + 2A_2$, $E_7 + A_6 + A_5$, $E_7 + A_6 + A_4 + A_1$, $E_7 + A_6 + A_3 + A_2$, $E_7 + A_6 + 2A_2 + A_1$, $E_7 + A_5 + A_4 + A_2$, $E_7 + A_4 + A_3 + 2A_2$, $2E_6 + D_6$, $2E_6 + A_6$, $2E_6 + 2A_3$, $E_6 + D_{12}$, $E_6 + D_{11} + A_1$, $E_6 + D_9 + A_3$, $E_6 + D_9 + A_2 + A_1$, $E_6 + D_8 + A_4$, $E_6 + D_7 + D_5$, $E_6 + D_7 + A_4 + A_1$, $E_6 + D_6 + A_6$, $E_6 + D_6 + A_4 + A_2$, $E_6 + D_5 + A_7$, $E_6 + D_5 + A_6 + A_1$, $E_6 + D_5 + A_4 + A_3$, $E_6 + A_{12}$, $E_6 + A_{11} + A_1$, $E_6 + A_{10} + A_2$, $E_6 + A_{10} + 2A_1$, $E_6 + A_9 + A_3$, $E_6 + A_9 + A_2 + A_1$, $E_6 + A_8 + A_4$, $E_6 + A_8 + A_3 + A_1$, $E_6 + A_7 + A_5$, $E_6 + A_7 + A_4 + A_1$, $E_6 + A_6 + A_5 + A_1$, $E_6 + A_6 + A_4 + A_2$, $E_6 + A_6 + A_4 + 2A_1$, $E_6 + A_6 + A_3 + A_2 + A_1$, $E_6 + A_5 + A_4 + A_3$, $E_6 + 2A_4 + A_3 + A_1$, D_{18}, $D_{17} + A_1$, $D_{15} + A_2 + A_1$, $D_{14} + A_4$, $D_{14} + 2A_2$, $D_{13} + D_5$, $D_{13} + A_5$, $D_{13} + A_4 + A_1$, $D_{11} + A_6 + A_1$, $D_{11} + A_5 + A_2$, $D_{11} + A_4 + A_2 + A_1$, $D_{11} + A_3 + 2A_2$, $D_{10} + A_8$, $D_{10} + A_6 + A_2$, $D_{10} + 2A_4$, $2D_9$, $D_9 + D_5 + A_4$, $D_9 + A_9$, $D_9 + A_8 + A_1$, $D_9 + A_6 + A_2 + A_1$, $D_9 + A_5 + A_4$, $D_9 + A_4 + 2A_2 + A_1$, $D_8 + A_6 + 2A_2$, $2D_7 + 2A_2$, $D_7 + A_{10} + A_1$, $D_7 + A_9 + A_2$, $D_7 + A_6 + A_5$, $D_7 + A_6 + A_4 + A_1$, $D_7 + A_6 + A_3 + A_2$, $D_7 + 2A_4 + A_2 + A_1$, $D_6 + A_{12}$, $D_6 + A_{10} + A_2$, $D_6 + A_8 + A_4$, $D_6 + 2A_6$, $D_6 + A_6 + A_4 + A_2$, $D_6 + 2A_4 + 2A_2$, $2D_5 + A_8$, $2D_5 + 2A_4$, $D_5 + A_{13}$, $D_5 + A_{12} + A_1$, $D_5 + A_{10} + A_2 + A_1$, $D_5 + A_9 + A_4$, $D_5 + A_9 + 2A_2$, $D_5 + A_8 + A_5$, $D_5 + A_8 + A_4 + A_1$, $D_5 + 2A_6 + A_1$, $D_5 + A_6 + A_5 + A_2$, $D_5 + A_6 + A_4 + A_2 + A_1$, $D_5 + A_6 + A_3 + 2A_2$, $D_5 + A_5 + 2A_4$, A_{18}, $A_{17} + A_1$, $A_{16} + A_2$, $A_{16} + 2A_1$, $A_{15} + A_2 + A_1$, $A_{14} + A_4$, $A_{14} + A_3 + A_1$, $A_{14} + A_2 + 2A_1$, $A_{13} + A_5$, $A_{13} + A_4 + A_1$, $A_{13} + A_3 + A_2$, $A_{13} + 2A_2 + A_1$, $A_{12} + A_6$, $A_{12} + A_5 + A_1$, $A_{12} + A_4 + A_2$, $A_{12} + A_4 + 2A_1$, $A_{12} + A_3 + A_2 + A_1$, $A_{12} + 2A_2 + 2A_1$, $A_{11} + A_6 + A_1$, $A_{11} + A_4 + A_2 + A_1$, $A_{10} + A_8$, $A_{10} + A_7 + A_1$, $A_{10} + A_6 + A_2$, $A_{10} + A_6 + 2A_1$, $A_{10} + A_5 + A_3$, $A_{10} + A_5 + A_2 + A_1$, $A_{10} + 2A_4$, $A_{10} + A_4 + A_3 + A_1$, $A_{10} + A_4 + 2A_2$, $A_{10} + A_4 + A_2 + 2A_1$, $A_{10} + 2A_3 + A_2$, $A_{10} + A_3 + 2A_2 + A_1$, $2A_9$, $A_9 + A_8 + A_1$, $A_9 + A_7 + A_2$, $A_9 + A_6 + A_3$, $A_9 + A_6 + A_2 + A_1$, $A_9 + A_5 + A_4$, $2A_8 + 2A_1$, $A_8 + A_7 + A_2 + A_1$, $A_8 + A_6 + A_4$, $A_8 + A_6 + A_3 + A_1$, $A_8 + A_6 + A_2 + 2A_1$, $A_8 + A_5 + A_4 + A_1$, $A_8 + 2A_4 + 2A_1$, $A_8 + A_4 + A_3 + A_2 + A_1$, $2A_7 + 2A_2$, $A_7 + A_6 + A_5$, $A_7 + A_6 + A_4 + A_1$, $A_7 + A_6 + A_3 + A_2$, $A_7 + A_6 + 2A_2 + A_1$, $A_7 + A_5 + A_4 + A_2$, $A_7 + A_4 + A_3 + 2A_2$, $2A_6 + A_4 + A_2$, $2A_6 + 2A_3$, $2A_6 + 2A_2 + 2A_1$, $A_6 + A_5 + A_4 + A_3$, $A_6 + A_5 + A_4 + A_2 + A_1$, $A_6 + 2A_4 + A_3 + A_1$, $A_6 + 2A_4 + A_2 + 2A_1$, $A_6 + A_4 + 2A_3 + A_2$, $A_6 + A_4 + A_3 + 2A_2 + A_1$, $2A_5 + 2A_4$, $2A_4 + 2A_3 + 2A_2$.

(2) *An* ADE*-type* Σ *with* $r := \operatorname{rank}\Sigma < 18$ *is a member of* $\mathcal{P}^{[1]}_r$ *if and only if* Σ *is obtained from a member of* $\mathcal{P}^{[1]}_{18}$ *by elementary transformation.*

Theorem 2.4. (1) *The list* $\mathcal{P}^{[2]}_{18}$ *consists of* 84 *elements listed below.*

TABLE 2.3. Forbidden substitutions for [2].

A_l	$\mapsto$	$A_{l'} + A_{l-1-l'}$ with l odd and l' even $(0 \le l' < l/2)$,
D_m	$\mapsto$	A_{m-1},
D_m	$\mapsto$	$A_3 + A_{m-4}$ with m even,
D_m	$\mapsto$	$D_{m'} + A_{m-1-m'}$ with m even and m' odd $(5 \le m' \le m-1)$,
E_7	$\mapsto$	$A_6,\ A_4 + A_2,\ E_6$.

TABLE 2.4. Forbidden substitutions for [3].

A_l	$\mapsto$	$A_{l_1} + A_{l_2}$ $(l_1 + l_2 = l - 1,\ 0 \le l_1 \le l_2)$
		with $l \bmod 3 = 2$, $l_1 \bmod 3 \ne 2$, $l_2' \bmod 3 \ne 2$,
E_6	$\mapsto$	$A_4 + A_1,\ D_5$.

TABLE 2.5. Forbidden substitutions for [4].

A_1	$\mapsto$	0
A_l	$\mapsto$	$A_{l_1} + A_{l_2}$ $(l_1 + l_2 = l - 1,\ 0 \le l_1 \le l_2)$
		with $l \bmod 4 = 3$, $l_1 \bmod 4 \ne 3$, $l_2' \bmod 4 \ne 3$,
D_m	$\mapsto$	$A_{m-1},\ D_{m-1},\ 2A_1 + A_{m-3}$ with m odd,
D_m	$\mapsto$	$D_{m-3} + A_2$ with m odd and > 6.

TABLE 2.6. Forbidden substitutions for [2, 2].

A_l	$\mapsto$	$A_{l'} + A_{l-1-l'}$ with l odd and l' even $(0 \le l' < l/2)$,
D_m	$\mapsto$	$A_{m-1},\ A_3 + A_{m-4}$ with m even,
D_m	$\mapsto$	$D_{m'} + A_{m-1-m'}$ with m even and m' odd $(5 \le m' \le m-1)$.

$2E_7 + D_4$, $2E_7 + A_3 + A_1$, $E_7 + D_{10} + A_1$, $E_7 + D_8 + A_2 + A_1$, $E_7 + D_7 + A_3 + A_1$, $E_7 + D_6 + D_5$, $E_7 + D_6 + A_5$, $E_7 + D_6 + A_3 + A_2$, $E_7 + D_5 + A_5 + A_1$, $E_7 + A_9 + A_2$, $E_7 + A_9 + 2A_1$, $E_7 + A_7 + A_3 + A_1$, $E_7 + A_7 + A_2 + 2A_1$, $E_7 + A_5 + A_4 + 2A_1$, $E_7 + A_5 + 2A_3$, $E_7 + A_5 + A_3 + A_2 + A_1$, $E_7 + A_4 + 2A_3 + A_1$, $D_{16} + A_2$, $D_{16} + 2A_1$, $D_{14} + A_3 + A_1$, $D_{14} + A_2 + 2A_1$, $D_{12} + D_6$, $D_{12} + D_5 + A_1$, $D_{12} + A_4 + 2A_1$, $D_{12} + A_3 + A_2 + A_1$, $D_{12} + 2A_2 + 2A_1$, $D_{10} + D_7 + A_1$, $D_{10} + D_6 + A_2$, $D_{10} + D_5 + A_2 + A_1$, $D_{10} + A_5 + A_3$, $D_{10} + A_4 + A_3 + A_1$, $D_9 + A_7 + 2A_1$, $D_9 + A_5 + A_3 + A_1$, $D_8 + 2D_5$, $D_8 + A_9 + A_1$, $D_8 + A_7 + A_2 + A_1$, $D_8 + 2A_5$, $D_8 + A_5 + A_4 + A_1$, $D_8 + 2A_3 + 2A_2$, $D_7 + D_6 + A_5$, $D_7 + D_5 + A_5 + A_1$, $D_7 + A_9 + 2A_1$, $D_7 + A_7 + A_2 + 2A_1$, $D_6 + D_5 + A_7$, $D_6 + D_5 + A_5 + A_2$, $D_6 + A_{11} + A_1$, $D_6 + A_9 + A_3$, $D_6 + A_9 + A_2 + A_1$, $D_6 + A_7 + A_4 + A_1$, $D_6 + A_7 + A_3 + A_2$, $D_6 + A_7 + 2A_2 + A_1$, $D_6 + A_5 + A_4 + A_3$, $D_5 + A_{11} + A_2$, $D_5 + A_9 + A_3 + A_1$, $D_5 + A_9 + A_2 + 2A_1$, $D_5 + A_7 + A_4 + 2A_1$, $D_5 + 2A_5 + A_3$, $D_5 + A_5 + A_4 + A_3 + A_1$, $A_{15} + A_2 + A_1$, $A_{13} + A_4 + A_1$, $A_{13} + A_3 + 2A_1$, $A_{13} + 2A_2 + A_1$, $A_{13} + A_2 + 3A_1$, $A_{11} + A_5 + 2A_1$, $A_{11} + A_4 + 3A_1$, $A_{11} + A_3 + A_2 + 2A_1$, $A_9 + A_6 + 3A_1$, $A_9 + A_5 + A_4$, $A_9 + A_5 + A_3 + A_1$, $A_9 + A_5 + A_2 + 2A_1$, $A_9 + A_4 + A_3 + 2A_1$, $A_9 + A_4 + A_2 + 3A_1$, $A_9 + 2A_3 + A_2 + A_1$, $A_9 + A_3 + 2A_2 + 2A_1$, $2A_7 + 2A_2$, $A_7 + A_6 + A_3 + 2A_1$, $A_7 + 2A_5 + A_1$, $A_7 + A_5 + A_4 + 2A_1$, $A_7 + A_5 + A_3 + A_2 + A_1$, $A_7 + A_4 + A_3 + A_2 + 2A_1$, $A_6 + 2A_5 + 2A_1$, $A_6 + A_5 + 2A_3 + A_1$, $2A_5 + A_4 + A_3 + A_1$, $A_5 + A_4 + 2A_3 + A_2 + A_1$.

TABLE 2.7. Cardinalities of $\mathcal{P}_r^G$

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	total
$\lvert\mathcal{P}_r^{[1]}\rvert$	1	2	3	6	9	16	24	39	57	88	127	189	262	360	448	500	416	199	2746
$\lvert\mathcal{P}_r^{[2]}\rvert$	0	0	0	0	0	0	0	1	2	6	13	29	53	92	133	164	155	84	732
$\lvert\mathcal{P}_r^{[3]}\rvert$	0	0	0	0	0	0	0	0	0	0	0	1	2	6	12	21	24	19	85
$\lvert\mathcal{P}_r^{[4]}\rvert$	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	10	15	11	41
$\lvert\mathcal{P}_r^{[2,2]}\rvert$	0	0	0	0	0	0	0	0	0	0	0	1	2	5	10	16	16	11	61

(2) *Let $\mathcal{S}^{[2]}$ be the union of $\mathcal{P}_{18}^{[2]}$ and the following list.*
$2E_7+A_3$, E_7+D_{10}, $E_7+D_5+A_5$, $D_{12}+D_5$, $2D_8+A_1$, $D_7+A_9+A_1$, D_7+2A_5, D_6+A_{11}, $2D_5+A_7$, $A_{15}+A_2$, E_7+A_9, D_{16}, $2D_8$, D_5+A_{11}, A_{15}.
Then an ADE-type Σ is a member of $\mathcal{P}^{[2]}$ if and only if Σ is a member of $\mathcal{S}^{[2]}$ or obtained from a member of $\mathcal{S}^{[2]}$ by applying substitutions listed in Table 2.2 but not in Table 2.3.

Theorem 2.5. (1) *The list $\mathcal{P}_{18}^{[3]}$ consists of 19 elements listed below.*
$3E_6$, $2E_6+A_5+A_1$, $E_6+A_{11}+A_1$, $E_6+A_8+2A_2$, $E_6+A_8+A_2+2A_1$, $E_6+2A_5+A_2$, $E_6+A_5+A_3+2A_2$, $A_{17}+A_1$, $A_{14}+2A_2$, $A_{14}+A_2+2A_1$, $A_{11}+A_5+A_2$, $A_{11}+A_3+2A_2$, $A_{11}+3A_2+A_1$, $2A_8+2A_1$, $A_8+A_5+A_3+A_2$, $A_8+A_5+2A_2+A_1$, $A_8+A_4+3A_2$, $A_8+A_3+3A_2+A_1$, $2A_5+A_4+2A_2$.
(2) *Let $\mathcal{S}^{[3]}$ be $\mathcal{P}_{18}^{[3]}$. Then an ADE-type Σ is a member of $\mathcal{P}^{[3]}$ if and only if Σ is a member of $\mathcal{S}^{[3]}$ or obtained from a member of $\mathcal{S}^{[3]}$ by applying substitutions listed in Table 2.2 but not in Table 2.4.*

Theorem 2.6. (1) *The list $\mathcal{P}_{18}^{[4]}$ consists of 11 elements listed below.*
D_7+A_{11}, $D_7+A_7+A_3+A_1$, $D_7+3A_3+A_2$, $2D_5+A_7+A_1$, $D_5+A_{11}+2A_1$, $D_5+A_7+A_3+A_2+A_1$, $A_{15}+A_3$, $A_{15}+3A_1$, $A_{11}+2A_3+A_1$, $A_{11}+A_3+A_2+2A_1$, $A_7+3A_3+A_2$.
(2) *Let $\mathcal{S}^{[4]}$ be the union of $\mathcal{P}_{18}^{[4]}$ and the following list.*
$2D_5+A_7$, $A_{15}+2A_1$.
Then an ADE-type Σ is a member of $\mathcal{P}^{[4]}$ if and only if Σ is a member of $\mathcal{S}^{[4]}$ or obtained from a member of $\mathcal{S}^{[4]}$ by applying substitutions listed in Table 2.2 but not in Table 2.5.

Theorem 2.7. (1) *The list $\mathcal{P}_{18}^{[2,2]}$ consists of 11 elements listed below.*
$D_{10}+A_5+3A_1$, $D_{10}+2A_3+2A_1$, $2D_8+2A_1$, $D_8+D_6+A_3+A_1$, $D_8+A_5+A_3+2A_1$, $3D_6$, $2D_6+2A_3$, $D_6+2A_5+2A_1$, $D_6+A_5+2A_3+A_1$, $A_7+A_5+A_3+3A_1$, $2A_5+2A_3+2A_1$.
(2) *Let $\mathcal{S}^{[2,2]}$ be the union of $\mathcal{P}_{18}^{[2,2]}$ and the list*
$4D_4$.
Then an ADE-type Σ is a member of $\mathcal{P}^{[2,2]}$ if and only if Σ is a member of $\mathcal{S}^{[2,2]}$ or obtained from a member of $\mathcal{S}^{[2,2]}$ by applying substitutions listed in Table 2.2 but not in Table 2.6.

By these theorems, we can easily generate the complete list $\mathcal{P}^G$ for $G=[1]$, $[2]$, $[3]$, $[4]$, $[2,2]$. Table 2.7 shows the cardinalities of $\mathcal{P}_r^G$.

Case 2. $G\in\{[5],[6],[4,2]\}$. We simply give the table of $\mathcal{P}^G$. In each box, the ADE-types are listed according to the rank and the lexicographical order.

$G = [5]$:

$2A_9$, $A_9 + 2A_4 + A_1$, $4A_4 + 2A_1$, $A_9 + 2A_4$, $4A_4 + A_1$, $4A_4$.

$G = [6]$:

$A_{11}+A_5+2A_1$, $A_{11}+A_3+2A_2$, $A_{11}+2A_2+3A_1$, $3A_5+A_3$, $2A_5+A_3+2A_2+A_1$, $A_{11}+2A_2+2A_1$, $3A_5 + 2A_1$, $2A_5 + A_3 + 2A_2$, $2A_5 + 2A_2 + 3A_1$, $2A_5 + 2A_2 + 2A_1$.

$G = [4, 2]$:

$2A_7 + 4A_1$, $A_7 + 3A_3 + 2A_1$, $A_7 + 2A_3 + 4A_1$, $5A_3 + 2A_1$, $4A_3 + 4A_1$.

Case 3. $G \in \{[7], [8], [6, 2], [3, 3], [4, 4]\}$. In this case, the ADE-type determines the torsion of the Mordell-Weil group uniquely.

Theorem 2.8. *Let $f : X \to \mathbb{P}^1$ be an elliptic $K3$ surface. Then the following hold.*

- $G_f \cong \mathbb{Z}/(7) \iff \Sigma_f = 3A_6$.
- $G_f \cong \mathbb{Z}/(8) \iff \Sigma_f = 2A_7 + A_3 + A_1$.
- $G_f \cong \mathbb{Z}/(6) \times \mathbb{Z}/(2) \iff \Sigma_f = 3A_5 + 3A_1$.
- $G_f \cong \mathbb{Z}/(4) \times \mathbb{Z}/(4) \iff \Sigma_f = 6A_3$.
- $G_f \cong \mathbb{Z}/(3) \times \mathbb{Z}/(3) \iff \Sigma_f \in \{2A_5 + 4A_2, A_5 + 6A_2, 8A_2\}$.

Remark 2.9. Elliptic $K3$ surfaces with $G_f = [7], [8], [6, 2], [4, 4]$ are constructed as elliptic modular surfaces (cf. [17, 14]). The corresponding congruence groups $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ are as follows.

G_f	$[7]$	$[8]$	$[6, 2]$	$[4, 4]$
Γ	$\Gamma_1(7)$	$\Gamma_1(8)$	$\Gamma_0(3) \cap \Gamma(2)$	$\Gamma(4)$

2.3. **From ADE-types to configurations of singular fibers.** The correspondence between the type (in the notation of Kodaira) of a singular fiber of an elliptic fibration and an ADE-type is shown in Table 2.8. There are following ambiguities in recovering the configurations of singular fibers from its ADE-type.

- An irreducible singular fiber is of type either I_1 or II.
- A singular fiber of ADE-type A_1 is of type either I_2 or III.
- A singular fiber of ADE-type A_2 is of type either I_3 or IV.

We present some restrictions on the possibilities of configuration of singular fibers of an elliptic $K3$ surface $f : X \to \mathbb{P}^1$ with a given ADE-type.

Let i_b be the number of singular fibers of f of type I_b. We define similarly i_b^*, ii, ii^*, iii, iii^*, iv, iv^*. Miranda and Persson gave a formula for the degree of the modulus function $J_f : \mathbb{P}^1 \to \mathbb{P}^1 := \mathfrak{H}/\mathrm{SL}_2(\mathbb{Z})$ associated with $f : X \to \mathbb{P}^1$:

$$\deg J_f := \sum_{b \geq 1} b(i_b + i_b^*).$$

By the Hurwitz formula, they obtained the following necessary condition for configurations; if $\deg J_f > 0$, then

$$\deg J_f \leq 6 \sum_{b \geq 1} (i_b + i_b^*) + 4(ii + iv^*) + 3(iii + iii^*) + 2(iv + ii^*) - 12.$$

See [9, §3] for the proof.

The euler number 24 of the $K3$ surface X is equal to the sum of euler numbers of singular fibers of f. The third column of Table 2.8 shows the euler number of a

Table 2.8. Singular fibers of elliptic fibration.

<table>
<tr><th>Singular fiber</th><th>ADE-type</th><th>Euler number</th><th>Possible torsion parts</th></tr>
<tr><td>I_0</td><td>regular</td><td>0</td><td>all</td></tr>
<tr><td>I_1</td><td>irreducible</td><td>1</td><td rowspan="2">$\diamondsuit$</td></tr>
<tr><td>$\mathrm{I}_b \quad (b \geq 2)$</td><td>$A_{b-1}$</td><td>$b$</td></tr>
<tr><td>$\mathrm{I}_b^* \quad (b \geq 0)$</td><td>$D_{4+b}$</td><td>$6+b$</td><td>$\begin{cases} [1],[2],[2,2] & \text{if } b \text{ is even} \\ [1],[2],[4] & \text{if } b \text{ is odd} \end{cases}$</td></tr>
<tr><td>II</td><td>irreducible</td><td>2</td><td>[1]</td></tr>
<tr><td>II^*</td><td>E_8</td><td>10</td><td>[1]</td></tr>
<tr><td>III</td><td>A_1</td><td>3</td><td>[1], [2]</td></tr>
<tr><td>III^*</td><td>E_7</td><td>9</td><td>[1], [2]</td></tr>
<tr><td>IV</td><td>A_2</td><td>4</td><td>[1], [3]</td></tr>
<tr><td>IV^*</td><td>E_6</td><td>8</td><td>[1], [3]</td></tr>
</table>

$$\diamondsuit \begin{cases} [a] \text{ is possible for } a = 1, \dots, 8, \\ [2a, 2] \text{ is possible for } a = 1, \dots, 3 \text{ if and only if } b = 0 \bmod 2, \\ [3,3] \text{ is possible if and only if } b = 0 \bmod 3, \\ [4,4] \text{ is possible if and only if } b = 0 \bmod 4. \end{cases}$$

---

singular fiber of each type. We define the euler number $\mathrm{euler}(\Sigma)$ of an ADE-type $\Sigma := \sum a_l A_l + \sum d_m D_m + \sum e_n E_n$ by

$$\mathrm{euler}(\Sigma) := \sum a_l \cdot (l+1) + \sum d_m \cdot (m+2) + \sum e_n \cdot (n+2).$$

Then $\mathrm{euler}(\Sigma_f)$ is less than or equal to the sum of euler numbers of reducible singular fibers. Hence we always have

$$\mathrm{euler}(\Sigma_f) \leq 24.$$

We can deduce from Table 2.8, for example, that, if $\mathrm{euler}(\Sigma_f) = 24$, then$f : X \to \mathbb{P}^1$ has no irreducible fibers nor fibers of type III or IV.

When G_f is non-trivial, certain types of singular fibers cannot appear. Let $g : S \to \Delta$ be an elliptic fibration over an open unit disk Δ such that g is smooth over $\Delta^\times := \Delta \setminus \{0\}$, and let $E := g^{-1}(p)$ be the fiber over a point $p \in \Delta^\times$. Looking at the monodromy action of $\pi_1(\Delta^\times, p)$ on the set of torsion points of E, we can determine whether a finite abelian group can be embedded into the Mordell-Weil group of g. The fourth column of Table 2.8 shows the groups among the list (2.1) that can be isomorphic to the torsion part of the Mordell-Weil group of an elliptic surface having the singular fiber. We see, for example, that, if G_f is non-trivial, then every irreducible singular fiber must be of type I_1.

TABLE 2.9. Cardinalities of $\mathcal{R}_r$, $\mathcal{E}_r$ and $\mathcal{P}_r$

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	total
$\lvert\mathcal{R}_r\rvert$	1	2	3	6	9	16	24	39	57	88	128	193	276	403	570	815	1137	1599	5366
$\lvert\mathcal{E}_r\rvert$	1	2	3	6	9	16	24	39	57	88	128	193	274	393	531	688	773	712	3937
$\lvert\mathcal{P}_r\rvert$	1	2	3	6	9	16	24	39	57	88	128	193	274	392	518	624	580	325	3279
$\lvert\mathcal{T}_r\rvert$	1	2	3	6	9	16	24	38	55	82	115	162	217	289	362	419	372	188	2360

2.4. **Miscellaneous facts.** For an integer r with $1 \le r \le 18$, we put as follows.

$\mathcal{R}_r := \{\ \Sigma\ ;\ \Sigma$ is an ADE-type with $\operatorname{rank}(\Sigma) = r\ \ \}$,

$\mathcal{E}_r := \{\ \Sigma \in \mathcal{R}_r\ ;\ \operatorname{euler}(\Sigma) \le 24\ \}$, and

$\mathcal{P}_r := \{\ \Sigma \in \mathcal{E}_r\ ;$ there exists an elliptic $K3$ surface $f : X \to \mathbb{P}^1$ with $\Sigma_f = \Sigma\ \} = \cup_G \mathcal{P}_r^G$.

For $\Sigma \in \cup_{r=1}^{18} \mathcal{P}_r$, we denote by $\mathcal{G}(\Sigma)$ the set of isomorphism classes of finite abelian groups G such that $(\Sigma, G) \in \mathcal{P}$. For each r, we denote by $\mathcal{T}_r$ the set of $\Sigma \in \mathcal{P}_r$ such that $\mathcal{G}(\Sigma)$ consists of only the trivial group $[1]$. The cardinalities of these sets are given in Table 2.9. Note that, if $\operatorname{rank}(\Sigma) \le 12$, then $\operatorname{euler}(\Sigma) \le 24$ holds automatically.

Theorem 2.10. *Let* Σ *be an* ADE*-type with* $\operatorname{euler}(\Sigma) \le 24$. *Suppose that* $\operatorname{rank}(\Sigma) \le 13$. *Then there exists an elliptic* $K3$ *surface* $f : X \to \mathbb{P}^1$ *with* $\Sigma_f = \Sigma$.

Remark 2.11. The complement of $\mathcal{P}_{14}$ in $\mathcal{E}_{14}$ consists of a single element $E_6 + 8A_1$. Hence, when $\operatorname{euler}(\Sigma) \le 24$ and $\operatorname{rank}(\Sigma) = 14$, there exists an elliptic $K3$ surface $f : X \to \mathbb{P}^1$ with $\Sigma_f = \Sigma$ if and only if $\Sigma \ne E_6 + 8\ A_1$.

Theorem 2.12. *Suppose that* $\operatorname{rank}(\Sigma) \le 10$. *Then there exists an elliptic* $K3$ *surface* $f : X \to \mathbb{P}^1$ *with* $G_f = [1]$ *and* $\Sigma_f = \Sigma$.

Remark 2.13. The complement $\mathcal{P}_{11} \setminus \mathcal{P}_{11}^{[1]}$ consists of a single element $11A_1$. We have $\mathcal{G}(11A_1) = \{[2]\}$.

Theorem 2.14. *Let* $f : X \to \mathbb{P}^1$ *be an elliptic* $K3$ *surface. If* $\operatorname{rank}(\Sigma_f) \le 7$, *then* G_f *must be trivial.*

Remark 2.15. The complement $\mathcal{P}_8^{[1]} \setminus \mathcal{T}_8$ consists of a single element $8A_1$, and the complement $\mathcal{P}_9^{[1]} \setminus \mathcal{T}_9$ consists of two elements $9A_1$ and $A_3 + 6A_1$. We have

$$\mathcal{G}(8A_1) = \mathcal{G}(9A_1) = \mathcal{G}(A_3 + 6A_1) = \{[1], [2]\}.$$

Remark 2.16. There are several ADE-types Σ with $|\mathcal{G}(\Sigma)| \ge 3$. For example,

$$\mathcal{G}(2A_5 + 2A_2 + 2A_1) = \mathcal{G}(A_{11} + 2A_2 + 2A_1) = \{[1], [2], [3], [6]\}.$$

3. Local invariants of lattices

First we fix some terminologies about lattices.

Let R be either $\mathbb{Z}$ or $\mathbb{Z}_p$. A *lattice* over R is, by definition, a free R-module L of finite rank equipped with a non-degenerate symmetric bilinear form $(\ ,\ ) : L \times L \to R$. For $\alpha \in R \setminus \{0\}$, let αL denote the lattice obtained from L by multiplying the symmetric bilinear form by α. We will denote L^- for $(-1)\, L$. We often express a lattice by the intersection matrix with respect to a certain basis of L. For example, (a) is the lattice of rank 1 generated by a vector e such that $(e, e) = a$. A sublattice N of L is said to be *primitive* if L/N is torsion free. A lattice L over R is said to be *even* if $(v, v) \in 2R$ holds for any $v \in L$. Note that, when R is $\mathbb{Z}_p$ with p an odd prime, every lattice over R is even. The *discriminant* $\mathrm{disc}(L)$ of a lattice L is considered as an element of $(R \setminus \{0\})/(R^\times)^2$. A lattice L is said to be *unimodular* if $\mathrm{disc}(L) \in R^\times/(R^\times)^2$.

Suppose that $R = \mathbb{Z}_p$. Then we have $\mathrm{disc}(L) = p^\nu u$ for some $\nu \geq 0$, where $u \in \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. We denote the element u by $\mathrm{reddisc}(L)$ and call it the *reduced discriminant* of L.

Let k be the quotient field of R. The k-vector space $L \otimes_R k$ has a natural symmetric bilinear form with values in k. We denote by $L^\vee$ the R-submodule of $L \otimes_R k$ consisting of all vectors v such that $(v, w) \in R$ holds for every $w \in L$, and call it the *dual lattice* of L. An R-submodule M of $L^\vee$ is said to be an *overlattice* of L if M contains L and the symmetric bilinear form restricted to M takes values in R. Two lattices L and M over R are said to be *k-equivalent* if $L \otimes_R k$ and $M \otimes_R k$ together with their symmetric k-valued bilinear forms are isomorphic.

For a detailed account of the following definitions and theorems, see Conway and Sloane [6, Chapter 15] and Cassels [5, Chapters 8 and 9].

3.1. **Local invariants.** Let Λ be a lattice over $\mathbb{Z}_p$. Then Λ is decomposed into the orthogonal direct sum $\Lambda = \bigoplus_{\nu \geq 0} p^\nu \Lambda_\nu$ with each Λ_ν being unimodular. This decomposition is called a *Jordan decomposition* of Λ, and each $p^\nu \Lambda_\nu$ is called a *Jordan component* of Λ. Note that the reduced discriminant of Λ is the product of the discriminants of Λ_ν.

Suppose that p is odd. Then a lattice Λ over $\mathbb{Z}_p$ is isomorphic to an orthogonal direct sum $\oplus_i p^{\nu_i}(a_i)$, where $a_i \in \mathbb{Z}_p^\times$. The *$p$-excess* of Λ is defined to be

$$-\mathrm{rank}(\Lambda) + 4m + \sum_i p^{\nu_i} \in \mathbb{Z}/(8),$$

where m is the number of orthogonal direct summands $p^{\nu_i}(a_i)$ such that ν_i is odd and that a_i is not square in $\mathbb{Z}_p^\times$. It is known that the p-excess is a well-defined invariant of $\mathbb{Q}_p$-equivalence classes of lattices over $\mathbb{Z}_p$.

Suppose that $p = 2$. We put

$$U := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad V := \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},$$

both of which are even unimodular lattices of rank 2 over $\mathbb{Z}_2$. Then a lattice over $\mathbb{Z}_2$ is decomposed into the orthogonal direct sum of lattices such that each direct summand is isomorphic to $2^\nu(a)$ $(a \in \mathbb{Z}_2^\times)$, $2^\nu U$ or $2^\nu V$. We define the 2-excesses of these lattices by

$$\begin{aligned}
\text{2-excess}(2^\nu(a)) &= \begin{cases} 1 - a \bmod 8 & \text{if } \nu \text{ is even or } a = \pm 1 \bmod 8, \\ 5 - a \bmod 8 & \text{if } \nu \text{ is odd and } a = \pm 3 \bmod 8, \end{cases} \\
\text{2-excess}(2^\nu U) &= \ 2 \bmod 8, \\
\text{2-excess}(2^\nu V) &= \begin{cases} 2 \bmod 8 & \text{if } \nu \text{ is even}, \\ 6 \bmod 8 & \text{if } \nu \text{ is odd}. \end{cases}
\end{aligned}$$

Then we define the 2-excess of

$$\Lambda \cong \bigoplus_i 2^{\nu_i}(a_i) \oplus \bigoplus_j 2^{\nu_j} U \oplus \bigoplus_k 2^{\nu_k} V \tag{3.1}$$

to be the sum of the 2-excesses of direct summands in the decomposition (3.1). Even though the decomposition (3.1) is not unique in general, it turns out that the 2-excess is a well-defined invariant of $\mathbb{Q}_2$-equivalence classes of lattices over $\mathbb{Z}_2$. (Note that U and V are $\mathbb{Q}_2$-equivalent to $2(1) \oplus 2(7)$ and $2(1) \oplus 2(3)$, respectively.)

3.2. **Existence of lattices over $\mathbb{Z}$ with given local data.** Combining [6, Chapter 15, Theorem 5] and [5, Chapter 9, Theorem 1.2], we obtain the following:

Theorem 3.1. *Let d be a non-zero integer, and (r, s) a pair of non-negative integers such that $n := r + s$ is positive and that $d = (-1)^s|d|$ holds. Suppose that, for each prime divisor p of $2d$, a lattice $\Lambda^{(p)}$ of rank n over $\mathbb{Z}_p$ is given. Then there exists a lattice L over $\mathbb{Z}$ with discriminant d and signature (r, s) such that $L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is isomorphic to $\Lambda^{(p)}$ for each p if and only if the following two conditions are satisfied*:

(i) $\mathrm{disc}(\Lambda^{(p)})$ *is equal to* $d \cdot (\mathbb{Z}_p^\times)^2$ *for each p, and*
(ii) $r - s + \sum_{p|2d} p\text{-excess}(\Lambda^{(p)}) = n \bmod 8$ *holds.* □

4. Theory of discriminant forms

4.1. **Definitions.** Let R and k be as above. Let D be a finite abelian group. A finite symmetric bilinear form on D with values in k/R is, by definition, a homomorphism $b : D \times D \to k/R$ such that $b(x, y) = b(y, x)$ holds for any $x, y \in D$. A finite quadratic form on D with values in $k/2R$ is a map $q : D \to k/2R$ with the following properties:

(i) $q(nx) = n^2 q(x)$ for $n \in \mathbb{Z}$ and $x \in D$, and
(ii) the map $b[q] : D \times D \to k/R$ defined by $(x, y) \mapsto (q(x+y) - q(x) - q(y))/2$ is a finite symmetric bilinear form.

Let H be a subgroup of D. The orthogonal complement $H^\perp$ of H with respect to q is the subgroup of D consisting of elements y such that $b[q](x, y) = 0$ holds for any $x \in H$. We say that q is non-degenerate if $D^\perp = (0)$. Note that, if $D = H \oplus H^\perp$, then q is written as $q|_H \oplus q|_{H^\perp}$, because the homomorphism $a \mapsto a/2$ from $k/2R$ to k/R is injective.

The length of D is, by definition, the minimal number of generators of D. A subset $\{\gamma_1, \dots, \gamma_l\}$ of D is said to be a *reduced set of generators* of D if l is the length of D and $D = \langle\gamma_1\rangle \times \cdots \times \langle\gamma_l\rangle$ holds. Let $\{\gamma_1, \dots, \gamma_l\}$ be a reduced set of generators of D. Then a finite quadratic form q on D is expressed by a symmetric $l \times l$ matrix whose diagonal entries are $q(\gamma_i) \in k/2R$ and whose off-diagonal entries are $b[q](\gamma_i, \gamma_j) \in k/R$.

Let L be a lattice over R. The discriminant group D_L of L is, by definition, the quotient group $L^\vee/L$. We denote by $\Psi_L : L^\vee \to D_L$ the natural projection. Suppose that L is even. Then we can define a finite quadratic form q_L on D_L with values in $k/2R$ by $q_L(x) := (x', x') \bmod 2R$, where x' is a vector of $L^\vee$ such that $\Psi_L(x') = x$. We call q_L the *discriminant form* of L. Because L is non-degenerate, q_L is also non-degenerate. By definition, we have $(D_{L\oplus M}, q_{L\oplus M}) = (D_L, q_L) \oplus (D_M, q_M)$.

TABLE 4.1. Discriminant forms of even lattices over $\mathbb{Z}_p$

Λ	$p^\nu(a)$	$2^\nu U$	$2^\nu V$
D_Λ	$\mathbb{Z}/(p^\nu)$	$(\mathbb{Z}/(2^\nu))^{\oplus 2}$	$(\mathbb{Z}/(2^\nu))^{\oplus 2}$
q_Λ	$\left[\dfrac{a}{p^\nu}\right]$	$\dfrac{1}{2^\nu}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$	$\dfrac{1}{2^\nu}\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}$

4.2. **Discriminant forms and overlattices.** The following two propositions, due to Nikulin, play a central role in making the list $\mathcal{P}$.

Proposition 4.1 ([11] Proposition 1.4.1)**.** *Let L be an even lattice over $\mathbb{Z}$.*

(1) *If $H \subset D_L$ is a subgroup totally isotropic with respect to q_L, then $M := \Psi_L^{-1}(H)$ is an even overlattice of L, and the discriminant form of M is isomorphic to $(H^\perp/H, q_L|_{H^\perp/H})$.*

(2) *The map $H \mapsto \Psi_L^{-1}(H)$ establishes a bijection between the set of totally isotropic subgroups of (D_L, q_L) and the set of even overlattices of L.* □

Proposition 4.2 ([11] Proposition 1.6.1)**.** *Let L and M be even lattices over $\mathbb{Z}$. Then the following are equivalent.*

(i) *The two finite quadratic forms (D_L, q_L) and $(D_M, -q_M)$ are isomorphic.*

(ii) *There exists an even unimodular overlattice of $L \oplus M$ into which L and M are embedded primitively.*

□

4.3. **Localization and discriminant form.** Let L be an even lattice over $\mathbb{Z}$. We decompose D_L into the direct sum of its p-Sylow subgroups $D_L^{(p)}$, where p runs through the set of prime divisors of $|D_L| = |\operatorname{disc}(L)|$. These p-parts are orthogonal to each other with respect to q_L, and hence q_L is also decomposed into the p-parts; $q_L = \oplus_p q_L^{(p)}$, where $q_L^{(p)}$ is the restriction of q_L to $D_L^{(p)}$. By the definition of the discriminant form, we can easily prove the following:

Lemma 4.3. *The image of $q_L^{(p)}$ is contained in $2\,\mathbb{Z}[1/p]/2\,\mathbb{Z} \subset \mathbb{Q}/2\,\mathbb{Z}$. The natural inclusion $2\,\mathbb{Z}[1/p] \hookrightarrow \mathbb{Q}_p$ induces an isomorphism $2\,\mathbb{Z}[1/p]/2\,\mathbb{Z} \cong \mathbb{Q}_p/2\,\mathbb{Z}_p$ Under this identification, $(D_L^{(p)}, q_L^{(p)})$ is isomorphic to $(D_{L\otimes\mathbb{Z}_p}, q_{L\otimes\mathbb{Z}_p})$.* □

The discriminant form of an even lattice Λ over $\mathbb{Z}_p$ is calculated by Table 4.1. In particular, D_Λ is a p-group of length equal to $\operatorname{rank}(\Lambda) - \operatorname{rank}(\Lambda_0)$, where Λ_0 is the first Jordan component of Λ. We also have $\operatorname{disc}(\Lambda) = |D_\Lambda| \cdot \operatorname{reddisc}(\Lambda)$.

5. EXISTENCE OF EVEN LATTICES WITH A GIVEN DISCRIMINANT FORM

5.1. **Over $\mathbb{Z}_p$.** Suppose that a finite abelian p-group D and a non-degenerate finite quadratic form $q : D \to \mathbb{Q}_p/2\,\mathbb{Z}_p$ are given. It is known that, if $n \geq \operatorname{length}(D)$, then there exists an even lattice Λ of rank n over $\mathbb{Z}_p$ such that (D_Λ, q_Λ) is isomorphic to (D, q). The purpose of this subsection is to describe a method to determine the set $\mathcal{L}^{(p)}(n, D, q)$ of all $[\sigma, u] \in \mathbb{Z}/(8) \times \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ such that there exists an even lattice Λ of rank n over $\mathbb{Z}_p$ with $(D_\Lambda, q_\Lambda) \cong (D, q)$, p-excess$(\Lambda) = \sigma$ and $\operatorname{reddisc}(\Lambda) = u$.

Note that

$$\begin{aligned} p\text{-excess}(\Lambda_1 \oplus \Lambda_2) &= p\text{-excess}(\Lambda_1) + p\text{-excess}(\Lambda_2), \quad \text{and} \\ \operatorname{reddisc}(\Lambda_1 \oplus \Lambda_2) &= \operatorname{reddisc}(\Lambda_1) \cdot \operatorname{reddisc}(\Lambda_2). \end{aligned}$$

Taking these into account, for sets $\mathcal{L}$ and $\mathcal{L}'$ of elements of $\mathbb{Z}/(8) \times \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$, we define $\mathcal{L} * \mathcal{L}'$ to be the set

$$\{\ [\sigma + \sigma', uu']\ ;\ [\sigma, u] \in \mathcal{L},\ [\sigma', u'] \in \mathcal{L}'\ \}.$$

We also put $\mathcal{L}_0^{(p)} := \{[0,1]\}$. Then $\mathcal{L} * \mathcal{L}_0^{(p)} = \mathcal{L}$ holds for any $\mathcal{L}$.

Lemma 5.1. *Let l be the length of D. Then we have*

$$\mathcal{L}^{(p)}(n, D, q) = \mathcal{L}^{(p)}(n - l, (0), [0]) * \mathcal{L}^{(p)}(l, D, q). \tag{5.1}$$

If p is odd, then

$$\mathcal{L}^{(p)}(n - l, (0), [0]) = \begin{cases} \emptyset & \text{if } n < l, \\ \mathcal{L}_0^{(p)} & \text{if } n = l, \\ \{[0,1], [0, v_p]\} & \text{if } n > l, \end{cases} \tag{5.2}$$

where v_p is the unique non-trivial element of $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. If $p = 2$, then

$$\mathcal{L}^{(2)}(n - l, (0), [0]) = \begin{cases} \emptyset & \text{if } n < l \text{ or } n - l \bmod 2 = 1, \\ \mathcal{L}_0^{(2)} & \text{if } n = l, \\ \{[n-l, 1], [n-l, 5]\} & \text{if } n > l \text{ and } n - l \bmod 4 = 0, \\ \{[n-l, 3], [n-l, 7]\} & \text{if } n > l \text{ and } n - l \bmod 4 = 2. \end{cases}$$

Proof. Let $\Lambda = \Lambda_0 \oplus \bigoplus_{\nu>0} p^\nu \Lambda_\nu$ be a Jordan decomposition of an even lattice Λ over $\mathbb{Z}_p$ with $(D_\Lambda, q_\Lambda) \cong (D, q)$. We put $\Lambda_{>0} := \Lambda_0^\perp = \bigoplus_{\nu>0} p^\nu \Lambda_\nu$. Then we have $\operatorname{rank}(\Lambda_{>0}) = l$, $(D_{\Lambda_0}, q_{\Lambda_0}) = ((0), [0])$ and $(D_{\Lambda_{>0}}, q_{\Lambda_{>0}}) = (D_\Lambda, q_\Lambda) \cong (D, q)$. Hence (5.1) holds. The statement (5.2) is obvious. A lattice Λ over $\mathbb{Z}_2$ is even if and only if Λ_0 is of even rank and is isomorphic to an orthogonal direct sum of copies of U and V. Because of

$$[2\text{-excess}(U), \operatorname{reddisc}(U)] = [2, 7] \quad \text{and} \quad [2\text{-excess}(V), \operatorname{reddisc}(V)] = [2, 3],$$

we can easily prove the last statement. $\square$

Lemma 5.2. *Let p be a prime integer, and ν a positive integer.*

(1) *Suppose that p is an odd prime, and let v_p be the unique non-trivial element of $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. Let u be an integer prime to p. We put*

$$\chi_p(u) := \left(\frac{u}{p}\right) \ \in \ \{\pm 1\}.$$

Then

$$\mathcal{L}^{(p)}(1, \mathbb{Z}/(p^\nu), \left[\frac{u}{p^\nu}\right]) = \begin{cases} \{[p^\nu - 1, 1]\} & \text{if } \chi_p(u) = 1, \\ \{[p^\nu - 1, v_p]\} & \text{if } \nu \text{ is even and } \chi_p(u) = -1, \\ \{[p^\nu + 3, v_p]\} & \text{if } \nu \text{ is odd and } \chi_p(u) = -1. \end{cases}$$

(2) *Suppose that $p=2$ and a is an odd integer. Then we have*

$$\mathcal{L}^{(2)}(1, \mathbb{Z}/(2^\nu), \left[\frac{a}{2^\nu}\right]) = \begin{cases} \{[1-a, a]\} & \text{if } \nu \text{ is even,} \\ \{[1-a, a]\} & \text{if } \nu \text{ is odd, } \nu \geq 2, \text{ and } a \equiv \pm 1 \bmod 8, \\ \{[5-a, a]\} & \text{if } \nu \text{ is odd, } \nu \geq 2, \text{ and } a \equiv \pm 3 \bmod 8, \\ \{[1-a, a], [1-a, 5a]\} & \text{if } \nu = 1 \text{ and } a \equiv \pm 1 \bmod 8, \\ \{[5-a, a], [5-a, 5a]\} & \text{if } \nu = 1 \text{ and } a \equiv \pm 3 \bmod 8. \end{cases}$$

Let u, v and w be integers with v being odd. Then

$$\mathcal{L}^{(2)}(2, (\mathbb{Z}/(2^\nu))^{\oplus 2}, \frac{1}{2^\nu}\begin{bmatrix} 2u & v \\ v & 2w \end{bmatrix}) = \begin{cases} \{[2,7]\} & \text{if } \nu \text{ is even and } uw \text{ is even,} \\ \{[2,3]\} & \text{if } \nu \text{ is even and } uw \text{ is odd,} \\ \{[2,7]\} & \text{if } \nu \text{ is odd and } uw \text{ is even,} \\ \{[6,3]\} & \text{if } \nu \text{ is odd and } uw \text{ is odd.} \end{cases}$$

Proof. Two non-degenerate quadratic forms $[u/p^\nu]$ and $[u'/p^\nu]$ on $\mathbb{Z}/(p^\nu)$ with values in $\mathbb{Q}_p/2\,\mathbb{Z}_p$ are isomorphic if and only if

$$uu' \in (\mathbb{Z}_p^\times)^2, \qquad \text{or} \qquad (\quad p=2, \quad \nu=1, \quad \text{and} \quad u=u' \bmod 4 \quad)$$

is satisfied. On the other hand, two lattices $p^\nu(u)$ and $p^\nu(u')$ with u, $u' \in \mathbb{Z}_p^\times$ of rank 1 over $\mathbb{Z}_p$ are isomorphic if and only if $uu' \in (\mathbb{Z}_p^\times)^2$ holds. Therefore the first statement follows. The finite quadratic form

$$q = \frac{1}{2^\nu}\begin{bmatrix} 2u & v \\ v & 2w \end{bmatrix} \qquad (v : \text{odd})$$

on $(\mathbb{Z}/(2^\nu))^{\oplus 2}$ with values in $\mathbb{Q}_2/2\,\mathbb{Z}_2$ is isomorphic to $q_{2^\nu U}$ (resp. $q_{2^\nu V}$) if and only if $uw \bmod 2 = 0$ (resp. $uw \bmod 2 = 1$). These two forms can never be isomorphic to $[u'/2^\nu] \oplus [w'/2^\nu]$ with u' and w' being odd. Thus the second statement follows. □

Now we state an algorithm to calculate $\mathcal{L}^{(p)}(n, D, q)$. By Lemma 5.1, it is enough to determine $\mathcal{L}^{(p)}(l, D, q)$. Let $\{\gamma_1, \dots, \gamma_l\}$ be a reduced set of generators of D. We denote the order of γ_i by p^{ν_i}, and arrange the generators in such a way that $\nu_1 \geq \dots \geq \nu_l$ holds. For an element $\alpha \in \mathbb{Q}_p/\mathbb{Z}_p$, we define $\phi_p(\alpha)$ to be the integer such that the order of α is $p^{\phi_p(\alpha)}$. Note that $\phi_p(b[q](\gamma_i, \gamma_j)) \leq \min(\nu_i, \nu_j)$ holds for any γ_i and γ_j.

When $l = 1$, $\mathcal{L}^{(p)}(l, D, q)$ is given by Lemma 5.2. Suppose that $l > 1$.

Case 1. Suppose that there exists a generator γ_i such that $\phi_p(b[q](\gamma_i, \gamma_i)) = \nu_1$. Then we have $\nu_i = \nu_1$. Interchanging γ_1 and γ_i, we will assume that $\phi_p(b[q](\gamma_1, \gamma_1)) = \nu_1$. Let u be an integer such that $b[q](\gamma_1, \gamma_1) = u/p^{\nu_1} \bmod \mathbb{Z}_p$. Then u is prime to p, and hence there is an integer v such that $uv = 1 \bmod p^{\nu_1}$ holds. Since $\phi_p(b[q](\gamma_j, \gamma_1)) \leq \min(\nu_j, \nu_1) = \nu_j$, we can write $b[q](\gamma_j, \gamma_1)$ in the form w_j/p^{ν_1} mod $\mathbb{Z}_p$ by some integer w_j that is divisible by $p^{\nu_1 - \nu_j}$. For $j \geq 2$, we put $\gamma_j' := \gamma_j - v w_j \gamma_1$. Because γ_1 is of order p^{ν_1} in D, γ_j' is independent of the choice of u, v and w_j. Moreover, γ_j' is of order p^{ν_j}, and $\{\gamma_1, \gamma_2', \dots, \gamma_l'\}$ is again a reduced set of generators. By definition, we have $b[q](\gamma_j', \gamma_1) = 0$ for any $j \geq 2$. We put

$$(D_1, q_1) := (\langle \gamma_1 \rangle, q|_{\langle \gamma_1 \rangle}) \cong (\mathbb{Z}/(p^{\nu_1}), [u/p^{\nu_1}])$$

and $(D_2, q_2) := (\langle \gamma_2', \dots, \gamma_l' \rangle, q|_{\langle \gamma_2', \dots, \gamma_l' \rangle})$. Then (D, q) is decomposed into the orthogonal direct sum of (D_1, q_1) and (D_2, q_2).

Let Λ be an even lattice of rank l over $\mathbb{Z}_p$ such that there exists an isomorphism $h : (D_\Lambda, q_\Lambda) \xrightarrow{\sim} (D, q)$. Let $e^* \in \Lambda^\vee$ be a vector such that $h \circ \Psi_\Lambda(e^*) = \gamma_1$, and $\Lambda'_1 \subset \Lambda^\vee$ the $\mathbb{Z}_p$-submodule generated by e^*. Then $\Lambda_1 := \Lambda'_1 \cap \Lambda$ is a sublattice of rank 1 generated by $e := p^{\nu_1} e^*$. Let x be an arbitrary vector of Λ. Because of $\operatorname{ord}_p((x, e)) \geq \nu_1 = \operatorname{ord}_p((e, e))$, the vector

$$x' := x - \frac{(x, e)}{(e, e)} e$$

is in Λ and orthogonal to Λ_1. Hence we obtain an orthogonal decomposition $\Lambda = \Lambda_1 \oplus \Lambda_1^\perp$. The homomorphism $h \circ \Psi_\Lambda : \Lambda^\vee = \Lambda_1^\vee \oplus (\Lambda_1^\perp)^\vee \to D$ induces isomorphisms $(D_{\Lambda_1}, q_{\Lambda_1}) \cong (D_1, q_1)$ and $(D_{\Lambda_1^\perp}, q_{\Lambda_1^\perp}) \cong (D_2, q_2)$. It follows that

$$\mathcal{L}^{(p)}(l, D, q) = \mathcal{L}^{(p)}(1, D_1, q_1) * \mathcal{L}^{(p)}(l-1, D_2, q_2).$$

Thus $\mathcal{L}^{(p)}(l, D, q)$ is calculated by Lemma 5.2 and the induction hypothesis on l.

Case 2. Suppose that $\phi_p(b[q](\gamma_i, \gamma_i)) < \nu_1$ holds for any generator γ_i. Since q is non-degenerate, there exists at least one generator γ_k that satisfies $\phi_p(b[q](\gamma_1, \gamma_k)) = \nu_1$. Because of $\phi_p(b[q](\gamma_1, \gamma_k)) \leq \nu_k$, we have $\nu_k = \nu_1$.

Case 2.1. Suppose that p is odd. We replace γ_1 by $\gamma'_1 := \gamma_1 + \gamma_k$, which is an element of order p^{ν_1}. It is obvious that $\{\gamma'_1, \gamma_2, \dots, \gamma_l\}$ is again a reduced set of generators of D. Moreover we have $\phi_p(b[q](\gamma'_1, \gamma'_1)) = \nu_1$. Therefore we are led to Case 1.

Case 2.2. Suppose that $p = 2$. We replace γ_2 by γ_k. There exist integers u, v and w with v being odd such that

$$b[q](\gamma_1, \gamma_1) = \frac{2\,u}{2^{\nu_1}}, \quad b[q](\gamma_1, \gamma_2) = \frac{v}{2^{\nu_1}}, \quad \text{and} \quad b[q](\gamma_2, \gamma_2) = \frac{2\,w}{2^{\nu_1}}$$

hold modulo $\mathbb{Z}_2$. Note that $q(\gamma_1) = 2\tilde{u}/2^{\nu_1}$ and $q(\gamma_2) = 2\tilde{w}/2^{\nu_1}$ hold modulo $2\,\mathbb{Z}_2$ for some integers $\tilde{u}$ and $\tilde{w}$ with $u = \tilde{u} \bmod 2^{\nu_1 - 1}$ and $w = \tilde{w} \bmod 2^{\nu_1 - 1}$.

If $l = 2$, then $\mathcal{L}^{(2)}(l, D, q)$ is determined by Lemma 5.2. Suppose that $l \geq 3$. There exists an integer t such that $(4uw - v^2)t = 1 \bmod 2^{\nu_1}$ holds. For each $j \geq 3$, we choose integers s_{j1} and s_{j2} such that $b[q](\gamma_j, \gamma_1) = s_{j1}/2^{\nu_1} \bmod \mathbb{Z}_2$ and $b[q](\gamma_j, \gamma_2) = s_{j2}/2^{\nu_1} \bmod \mathbb{Z}_2$ hold, and calculate

$$\begin{pmatrix} \beta_{j1} \\ \beta_{j2} \end{pmatrix} := t \cdot \begin{pmatrix} 2w & -v \\ -v & 2u \end{pmatrix} \cdot \begin{pmatrix} s_{j1} \\ s_{j2} \end{pmatrix}.$$

Then β_{j1} and β_{j2} are divisible by $2^{\nu_1 - \nu_j}$. Hence $\gamma'_j := \gamma_j - \beta_{j1}\gamma_1 - \beta_{j2}\gamma_2$ is an element of order 2^{ν_j}, which is independent of the choice of the integers. The set $\{\gamma_1, \gamma_2, \gamma'_3, \dots, \gamma'_l\}$ is again a reduced set of generators of D, and the two subgroups $\langle \gamma_1, \gamma_2 \rangle$ and $\langle \gamma'_3, \dots, \gamma'_l \rangle$ of D are orthogonal with respect to q. Therefore, putting

$$(D_1, q_1) := (\langle \gamma_1, \gamma_2 \rangle, q|_{\langle \gamma_1, \gamma_2 \rangle}) \cong \left((\mathbb{Z}/(p^{\nu_1}))^{\oplus 2}, \frac{1}{2^{\nu_1}} \begin{bmatrix} 2\tilde{u} & v \\ v & 2\tilde{w} \end{bmatrix} \right)$$

and $(D_2, q_2) := (\langle \gamma'_3, \dots, \gamma'_l \rangle, q|_{\langle \gamma'_3, \dots, \gamma'_l \rangle})$, we obtain an orthogonal decomposition $(D, q) = (D_1, q_1) \oplus (D_2, q_2)$.

Let Λ be an even lattice of rank l over $\mathbb{Z}_2$ such that there exists an isomorphism $h : (D_\Lambda, q_\Lambda) \xrightarrow{\sim} (D, q)$. We pick up two vectors $e_1^*, e_2^* \in \Lambda^\vee$ such that $h \circ \Psi_\Lambda(e_1^*) = \gamma_1$ and $h \circ \Psi_\Lambda(e_2^*) = \gamma_2$. Let $\Lambda'_1 \subset \Lambda^\vee$ be the $\mathbb{Z}_2$-submodule of $\Lambda^\vee$ generated by e_1^* and e_2^*. Then $\Lambda_1 := \Lambda'_1 \cap \Lambda$ is a sublattice of Λ generated by $e_1 := 2^{\nu_1} e_1^*$ and

$e_2 := 2^{\nu_1} e_2^*$. The intersection matrix M_1 of Λ_1 with respect to e_1 and e_2 satisfies $\mathrm{ord}_2(\det M_1^{-1}) = -\nu_1$. Because $\mathrm{ord}_2((x, e_1)) \geq \nu_1$ and $\mathrm{ord}_2((x, e_2)) \geq \nu_1$ hold for any vector $x \in \Lambda$, we have $((x, e_1), (x, e_2)) \cdot M_1^{-1} \in \mathbb{Z}_2^{\oplus 2}$. Therefore Λ is decomposed into the orthogonal direct sum of Λ_1 and $\Lambda_1^\perp$. The homomorphism $h \circ \Psi_\Lambda$ induces isomorphisms $(D_{\Lambda_1}, q_{\Lambda_1}) \cong (D_1, q_1)$ and $(D_{\Lambda_1^\perp}, q_{\Lambda_1^\perp}) \cong (D_2, q_2)$. It follows that

$$\mathcal{L}^{(2)}(l, D, q) = \mathcal{L}^{(2)}(2, D_1, q_1) * \mathcal{L}^{(2)}(l-2, D_2, q_2).$$

Thus $\mathcal{L}^{(2)}(l, D, q)$ is calculated by Lemma 5.2 and the induction hypothesis on l.

5.2. **Over $\mathbb{Z}$.** Let D be a finite abelian group, and $q : D \to \mathbb{Q}/2\,\mathbb{Z}$ a non-degenerate finite quadratic form. Let (r, s) be a pair of non-negative integers such that $n := r + s > 0$. We will describe a criterion to determine whether there exists an even lattice L over $\mathbb{Z}$ with signature (r, s) such that (D_L, q_L) is isomorphic to the given finite quadratic form (D, q).

We put $d := (-1)^s |D|$. Let P be the set of prime divisors of $2\,d$, and let $(D, q) = \oplus_{p \in P} (D^{(p)}, q^{(p)})$ be the orthogonal decomposition of (D, q) into the p-parts. If d is odd, then we put $(D^{(2)}, q^{(2)}) = ((0), [0])$. By Lemma 4.3 and Theorem 3.1, an even lattice L over $\mathbb{Z}$ with signature (r, s) and $(D_L, q_L) \cong (D, q)$ exists if and only if the following claim is verified:

($\sharp$) For each $p \in P$, there exists an even lattice $\Lambda^{(p)}$ of rank n over $\mathbb{Z}_p$ such that
  (i) $\mathrm{disc}(\Lambda^{(p)}) = d \cdot (\mathbb{Z}_p^\times)^2$ and
  (ii) $(D_{\Lambda^{(p)}}, q_{\Lambda^{(p)}}) \cong (D^{(p)}, q^{(p)})$ hold,

and they satisfy

$$r - s + \sum_{p \in P} p\text{-excess}(\Lambda^{(p)}) = n \mod 8.$$

We put $\delta_p := d/p^{\mathrm{ord}_p(d)} \in \mathbb{Z}$. Under the condition (ii), which implies $|D_{\Lambda^{(p)}}| = d/\delta_p$, the condition (i) is equivalent to the condition

$$\mathrm{reddisc}(\Lambda^{(p)}) = \delta_p \cdot (\mathbb{Z}_p^\times)^2.$$

Therefore we can check the claim ($\sharp$) by the following method. First we calculate $\mathcal{L}^{(p)}(n, D^{(p)}, q^{(p)})$ for each $p \in P$. Then we search for an element ($[\sigma_p, u_p]$; $p \in P$) of the Cartesian product of the sets $\mathcal{L}^{(p)}(n, D^{(p)}, q^{(p)})$ that satisfies $u_p = \delta_p \cdot (\mathbb{Z}_p^\times)^2$ for each $p \in P$ and $r - s + \sum \sigma_p = n \bmod 8$. The claim ($\sharp$) is true if and only if we find such an element.

6. Roots

For the following, we refer to [3], [6, Chapter 4] or [12].

6.1. **Root system of a positive-definite even lattice over $\mathbb{Z}$.** Let L be a positive-definite even lattice over $\mathbb{Z}$. A vector of L is said to be a *root* if its norm is 2. We denote by L_{root} the sublattice of L generated by roots. The lattice L is said to be a *root lattice* if $L = L_{\mathrm{root}}$ holds. Let $\mathrm{Roots}(L)$ be the set of roots of L. We define $\sim$ to be the finest equivalence relation on $\mathrm{Roots}(L)$ that satisfies $(v, w) \neq 0 \Longrightarrow v \sim w$. Let $I_1, \dots, I_k$ be the equivalence classes of roots under the relation $\sim$, and let L_i be the sublattice of L_{root} generated by I_i. There exists a basis $B_i \subset I_i$ such that the intersection matrix of L_i with respect to B_i is the Cartan matrix corresponding to a Dynkin diagram of type A_l, D_m or E_n. Let τ_i

FIGURE 6.1. Dynkin diagram

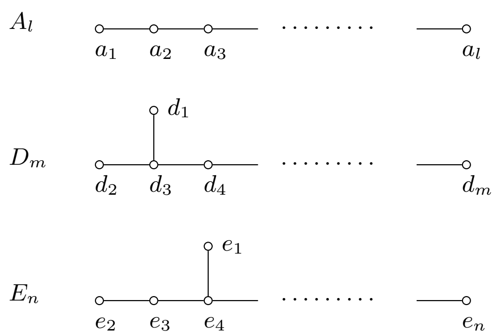

TABLE 6.1. Number of roots and discriminant forms of root lattices

τ	$\lvert\mathrm{Roots}(L(\tau))\rvert$	$D_{L(\tau)}$	$q_{L(\tau)}$
A_l	$l(l+1)$	$\langle \bar{a}_l^* \rangle \cong \mathbb{Z}/(l+1)$	$\left[\dfrac{l}{l+1}\right]$
D_m $(m : \text{even})$	$2m(m-1)$	$\langle \bar{d}_1^* \rangle \oplus \langle \bar{d}_m^* \rangle \cong (\mathbb{Z}/(2))^{\oplus 2}$	$\begin{bmatrix} m/4 & 1/2 \\ 1/2 & 1 \end{bmatrix}$
D_m $(m : \text{odd})$	$2m(m-1)$	$\langle \bar{d}_1^* \rangle \cong \mathbb{Z}/(4)$	$[m/4]$
E_6	72	$\langle \bar{e}_6^* \rangle \cong \mathbb{Z}/(3)$	$[4/3]$
E_7	126	$\langle \bar{e}_7^* \rangle \cong \mathbb{Z}/(2)$	$[3/2]$
E_8	240	(0)	$[0]$

be the type of the Dynkin diagram of the intersection matrix of L_i. We define the root type of L to be $\sum_{i=1}^{k} \tau_i$. Conversely, for an ADE-type Σ, there exists a root lattice $L(\Sigma)$, unique up to isomorphism, whose root type is Σ.

The root type of a positive-definite even lattice L over $\mathbb{Z}$ is therefore determined by the following procedure.

(1) Create the list $\mathrm{Roots}(L)$, and decompose it into $I_1, \dots, I_k$.
(2) Calculate the rank of L_i for $i = 1, \dots, k$.
(3) Determine the type τ_i from $\mathrm{rank}(L_i)$ and $|I_i|$ by using Table 6.1.

6.2. **Discriminant forms of root lattices.** The discriminant form $(D_{L(\tau)}, q_{L(\tau)})$, where τ is A_l, D_m or E_n, is indicated in Table 6.1. In this table, for example, $\{a_1^*, \dots, a_l^*\}$ is the basis of $L(A_l)^\vee$ dual to the basis $\{a_1, \dots, a_l\}$ of $L(A_l)$ given in Figure 6.1, and $\bar{a}_i^* \in D_{L(A_l)}$ is the image of a_i^* by the homomorphism $\Psi_{L(A_l)} : L(A_l)^\vee \to D_{L(A_l)}$.

Let $\Gamma(\tau)$ denote the image of the natural homomorphism from the orthogonal group $O(L(\tau))$ of the lattice $L(\tau)$ to $\mathrm{Aut}(D_{L(\tau)}, q_{L(\tau)})$. The structure of $\Gamma(\tau)$ is given as follows.

- If $\tau = A_1$ or $\tau = E_7$, then $\Gamma(\tau)$ is trivial.

- If $\tau = A_l$ $(l > 1)$ or $\tau = D_m$ $(m : \text{odd})$ or $\tau = E_6$, then $\Gamma(\tau)$ is isomorphic to $\mathbb{Z}/(2)$ generated by the multiplication by -1.
- If $\tau = D_m$ with m being even and > 4, then $\Gamma(\tau)$ is isomorphic to $\mathbb{Z}/(2)$ generated by

$$\bar{d}_1^* \mapsto \bar{d}_1^* + \bar{d}_m^*, \quad \bar{d}_m^* \mapsto \bar{d}_m^*.$$

- If $\tau = D_4$, then $\Gamma(\tau)$ is isomorphic to the full symmetric group acting on the set $\{\bar{d}_1^*, \bar{d}_4^*, \bar{d}_1^* + \bar{d}_4^*\}$ of non-trivial elements of $D_{L(\tau)}$.

7. Existence of an elliptic $K3$ surface with given data

Theorem 7.1. *Let Σ be an ADE-type with* $\operatorname{rank}(\Sigma) \le 18$*, and G a finite abelian group. There exists an elliptic $K3$ surface $f : X \to \mathbb{P}^1$ with $\Sigma_f = \Sigma$ and $G_f \cong G$ if and only if the root lattice $L(\Sigma)$ has an even overlattice M with the following properties.*

(i) *$M/L(\Sigma) \cong G$,*
(ii) *there exists an even lattice N of signature* $(2, 18 - \operatorname{rank}(\Sigma))$ *such that (D_N, q_N) is isomorphic to (D_M, q_M), and*
(iii) *the sublattice M_{root} of M coincides with $L(\Sigma)$.*

Proof. Suppose that a pair (Σ, G) satisfies the condition of Theorem. By Proposition 4.2, the property (ii) implies that there exists an even unimodular overlattice K' of $M^- \oplus N$ into which M^- and N are primitively embedded. Let H denote the hyperbolic lattice;

$$H := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then $K := K' \oplus H$ is an even unimodular lattice with signature $(3, 19)$. Hence K is isomorphic to the $K3$ lattice $L(2E_8)^- \oplus H^{\oplus 2}$ by Milnor's structure theorem (cf. [15]). There exists a 2-dimensional linear subspace V of $N \otimes_{\mathbb{Z}} \mathbb{R}$ such that the bilinear form is positive-definite on V and that, if $N' \subset N$ is a sublattice such that $N' \otimes_{\mathbb{Z}} \mathbb{R}$ contains V, then N' coincides with N. By the surjectivity of the period map on the moduli of $K3$ surfaces, there exists a complex $K3$ surface X and an isomorphism $\alpha : H^2(X; \mathbb{Z}) \xrightarrow{\sim} K$ of lattices such that

$$\alpha_{\mathbb{R}}^{-1}(V) = (H^{0,2}(X) \oplus H^{2,0}(X)) \cap H^2(X; \mathbb{R})$$

holds, where $\alpha_{\mathbb{R}} := \alpha \otimes_{\mathbb{Z}} \mathbb{R}$. Then we have

$$\alpha^{-1}(M^- \oplus H) = \mathrm{NS}_X\,. \tag{7.1}$$

By Kondo's lemma [8, Lemma 2.1], there exists a structure of the elliptic fibration $f : X \to \mathbb{P}^1$ with a section $O : \mathbb{P}^1 \to X$ such that, if F denotes the cohomology class of a general fiber of f, then

$$\mathbb{Z}[F]^{\perp}/\mathbb{Z}[F] \cong M^- \tag{7.2}$$

holds, where $\mathbb{Z}[F]^{\perp}$ is the orthogonal complement of $\mathbb{Z}[F]$ in the Néron-Severi lattice NS_X of X. Let H_f be the sublattice of NS_X spanned by the cohomology classes of the zero section and a general fiber of f, S_f the sublattice of NS_X defined in § 1, and W_f the orthogonal complement of H_f in NS_X. The lattice H_f is isomorphic to the hyperbolic lattice H, and is orthogonal to S_f. By abuse of notation, we denote

$(W_f)_{\mathrm{root}}$ for the sublattice of W_f generated by the vectors of norm -2. From (7.2), we have

$$W_f \cong M^-. \tag{7.3}$$

On the other hand, by Nishiyama's lemma [12, Lemma 6.1], we have

$$W_f/(W_f)_{\mathrm{root}} \cong MW_f, \quad \text{and} \tag{7.4}$$

$$S_f = (W_f)_{\mathrm{root}}. \tag{7.5}$$

Combining these with the properties (i) and (iii) of M and the isomorphism (7.3), we have $S_f \cong L(\Sigma)^-$ and $MW_f \cong G$. Hence $\Sigma = \Sigma_f$ and $G \cong G_f$ hold.

Conversely, suppose that there exists an elliptic $K3$ surface $f : X \to \mathbb{P}^1$ with $\Sigma_f = \Sigma$ and $G_f \cong G$. Using Nishiyama's lemma again, we see that the primitive closure $\overline{S}_f$ of S_f in NS_X satisfies $\overline{S}_f/S_f \cong G$ and $(\overline{S}_f)_{\mathrm{root}} = S_f$. We have an isomorphism $S_f \cong L(\Sigma)^-$. Let M^- be the overlattice of $L(\Sigma)^-$ corresponding to $\overline{S}_f$ via this isomorphism. Then $M := (M^-)^-$ is an even overlattice of $L(\Sigma)$ that possess the properties (i) and (iii). Moreover, $\overline{S}_f \oplus H_f$ is primitive in the even unimodular lattice $H^2(X;\mathbb{Z})$, and hence Proposition 4.2 implies that the orthogonal complement N_f of $\overline{S}_f \oplus H_f$ in $H^2(X;\mathbb{Z})$ satisfies $(D_{N_f}, q_{N_f}) \cong (D_{\overline{S}_f}, -q_{\overline{S}_f}) \cong (D_M, q_M)$. Because the signature of N_f is $(2, 18 - \mathrm{rank}(\Sigma))$, the even overlattice M has the property (ii). □

8. Making the list

Recall that, in order for an ADE-type Σ to be an ADE-type of an elliptic $K3$ surface, it is necessary that $\mathrm{rank}(\Sigma) \le 18$ and $\mathrm{euler}(\Sigma) \le 24$. It is obvious that the torsion part of the Mordell-Weil group of an elliptic surface is of length ≤ 2.

First we list up all ADE-types Σ with $\mathrm{rank}(\Sigma) \le 18$ and $\mathrm{euler}(\Sigma) \le 24$. There are 3937 such ADE-types. For each

$$\Sigma := \sum a_l A_l + \sum d_m D_m + \sum e_n E_n$$

in this list, we carry out the following calculation.

Step 1. We calculate the discriminant form $(D_{L(\Sigma)}, q_{L(\Sigma)})$ using Table 6.1. Note that the product of the wreath products

$$\prod_{a_l > 0} (\Gamma(A_l) \wr \mathfrak{S}_{a_l}) \times \prod_{d_m > 0} (\Gamma(D_m) \wr \mathfrak{S}_{d_m}) \times \prod_{e_n > 0} (\Gamma(E_n) \wr \mathfrak{S}_{e_n})$$

acts on $(D_{L(\Sigma)}, q_{L(\Sigma)})$. Here, for example, the full symmetric group $\mathfrak{S}_{a_l}$ acts on $D_{L(\Sigma)}$ as the permutation group on the a_l components of $D_{L(\Sigma)}$ isomorphic to $D_{L(A_l)}$. We denote this group by $\Gamma(\Sigma)$.

Step 2. We make a complete list of representatives of the quotient set $D_{L(\Sigma)}/\Gamma(\Sigma)$ and pick up from this list elements isotropic with respect to $q_{L(\Sigma)}$. Let $\mathcal{V}_\Sigma = \{\bar{v}_1, \ldots, \bar{v}_N\}$ be the list of isotropic elements of $D_{L(\Sigma)}$ modulo $\Gamma(\Sigma)$. For each $\bar{v}_i \in \mathcal{V}_\Sigma$, we calculate the stabilizer subgroup $St(\Gamma(\Sigma), \bar{v}_i)$ of $\bar{v}_i$ in $\Gamma(\Sigma)$. Then we make a complete list of representatives of $D_{L(\Sigma)}/St(\Gamma(\Sigma), \bar{v}_i)$, and pick up from this list elements isotropic with respect to $q_{L(\Sigma)}$ and orthogonal to $\bar{v}_i$ with respect to $b[q_{L(\Sigma)}]$. Let $\mathcal{W}_{\Sigma,i}$ be the list of isotropic elements orthogonal to $\bar{v}_i$ modulo $St(\Gamma(\Sigma), \bar{v}_i)$.

Next we make the list $\mathcal{G}'_\Sigma$ of all pairs $[\bar{v}_i, \bar{w}_j]$ of $\bar{v}_i \in \mathcal{V}_\Sigma$ and $\bar{w}_j \in \mathcal{W}_{\Sigma,i}$. Then every totally isotropic subgroup of $(D_{L(\Sigma)}, q_{L(\Sigma)})$ with length ≤ 2 is conjugate under the action of $\Gamma(\Sigma)$ to a subgroup $\langle \bar{v}_i, \bar{w}_j \rangle$ generated by $\bar{v}_i$ and $\bar{w}_j$ for some $[\bar{v}_i, \bar{w}_j] \in \mathcal{G}'_\Sigma$. Of course, there are several different pairs that generate a same subgroup. We remove this redundancy from $\mathcal{G}'_\Sigma$, and make a list $\mathcal{G}_\Sigma$.

Step 3. For each $[\bar{v}, \bar{w}] \in \mathcal{G}_\Sigma$, we calculate the subgroup $G := \langle \bar{v}, \bar{w} \rangle$ of $D_{L(\Sigma)}$, its orthogonal complement $G^\perp$ in $(D_{L(\Sigma)}, q_{L(\Sigma)})$, and the finite quadratic form $(D_G, q_G) := (G^\perp/G, q_{L(\Sigma)}|_{G^\perp/G})$.

Step 3.1. By the algorithm described in § 5, we determine whether there exists an even lattice N over $\mathbb{Z}$ of signature $(2, 18 - \mathrm{rank}(\Sigma))$ such that $(D_N, q_N) \cong (D_G, q_G)$. If the answer is affirmative, we go to the next step.

Step 3.2. We calculate the intersection matrix of the even overlattice M_G of $L(\Sigma)$ generated by $L(\Sigma)$ and v, w in $L(\Sigma)^\vee$, where v and w are vectors of $L(\Sigma)^\vee$ such that $\Psi_{L(\Sigma)}(v) = \bar{v}$ and $\Psi_{L(\Sigma)}(w) = \bar{w}$. Then we calculate the root type of M_G by the algorithm described in § 6. If this root type coincides with the initial ADE-type Σ, then we let the pair (Σ, G) be a member of the list $\mathcal{P}$.

By Theorem 7.1, the list $\mathcal{P}$ thus made is the complete list of the data of elliptic $K3$ surfaces.

The following remarks are useful in checking the program.

Remark 8.1. Note that neither $\mathrm{euler}(\Sigma) \le 24$ nor $\mathrm{length}(G) \le 2$ is contained in the conditions of Theorem 7.1. Therefore, if we input Σ with $\mathrm{euler}(\Sigma) > 24$ into the program, then it should return no subgroups G of $D_{L(\Sigma)}$ such that (Σ, G) can be a member of the list $\mathcal{P}$. If we change Step 2 of the program so that it lists up all totally isotropic subgroups of length ≥ 3, then the result should also be an empty set.

Remark 8.2. Suppose that the root type Σ' of M_G is not equal to Σ in Step 3.2 of the program. Let G' be the finite abelian group $M_G/(M_G)_{\mathrm{root}}$. Then (Σ', G') appears in $\mathcal{P}$.

Remark 8.3. For each $(\Sigma, G) \in \mathcal{P}$, there should be at least one configuration that satisfies the conditions given in § 2.3.

References

[1] E. Artal-Bartolo, H. Tokunaga and D. Q. Zhang. *Miranda-Persson's problem on extremal elliptic K3 surfaces.* Pacific J. Math. **202** (2002), no. 1, 37–72.

[2] A. Besser. *Elliptic fibrations of $K3$ surfaces and QM Kummer surfaces.* Math. Z. **228** (1998), no. 2, 283–308.

[3] N. Bourbaki. Éléments de mathématique. Groupes et algèbres de Lie. Chapitre IV-VI. Hermann, Paris, 1968.

[4] D. Burns and M. Rapoport. *On the Torelli problem for kählerian $K{-}3$ surfaces.* Ann. Sci. École Norm. Sup. (4) **8** (1975), no. 2, 235–273.

[5] J. W. S. Cassels. Rational quadratic forms. Academic Press, London, 1978.

[6] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups.* Second edition. Grundlehren der Mathematischen Wissenschaften, **290**, Springer, New York, 1993.

[7] K. Kodaira. *On compact analytic surfaces. II, III.* Ann. of Math. **77** (1963), 563–626; ibid. **78** (1963) 1–40

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

[9] R. Miranda and U. Persson. *On extremal rational elliptic surfaces.* Math. Z. **193** (1986), no. 4, 537–558.

[10] R. Miranda and U. Persson. *Mordell-Weil groups of extremal elliptic $K3$ surfaces.* Problems in the theory of surfaces and their classification (Cortona, 1988), Sympos. Math., XXXII, Academic Press, London, 1991, pp. 167–192.

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

[12] K. Nishiyama. *The Jacobian fibrations on some $K3$ surfaces and their Mordell-Weil groups.* Japan. J. Math. (N.S.) **22** (1996), no. 2, 293–347.

[13] I. Piateskii-Shapiro and I. R. Shafarevich. *A Torelli theorem for algebraic surfaces of type $K3$.* Math. USSR Izv. **35** (1971), 530–572.

[14] A. Sebbar. *Congruence groups, Hauptmoduls and elliptic surfaces.* Talk at "Infinite dimensional Lie algebras, the Monster and related topics". July 1999 Hokkaido Univ.

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

[16] I. Shimada and D. Q. Zhang. *Classification of extremal elliptic $K3$ surfaces and fundamental groups of open $K3$ surfaces.* Nagoya Math. J. **161** (2001), 23–54.

[17] T. Shioda. *On elliptic modular surfaces.* J. Math. Soc. Japan **24** (1972), 20–59.

[18] A. N. Todorov. *Applications of the Kähler-Einstein-Calabi-Yau metric to moduli of $K3$ surfaces.* Invent. Math. **61** (1980), no. 3, 251–265.

[19] T. Urabe. *Elementary transformations of Dynkin graphs and singularities on quartic surfaces.* Invent. Math. **87** (1987), no. 3, 549–572.

[20] T. Urabe. *Tie transformations of Dynkin graphs and singularities on quartic surfaces.* Invent. Math. **100** (1990), no. 1, 207–230.

[21] J.-G. Yang. *Sextic curves with simple singularities.* Tôhoku Math. J. **48** (1996), no. 2, 203-227.

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

[23] Q. Ye. *On extremal elliptic $K3$ surfaces.* J. Korean Math. Soc. **36** (1999), no. 6, 1091–1113.

Department of Mathematics, Faculty of Science, Hokkaido University, Sapporo 060-0810, JAPAN

E-mail address: shimada@math.sci.hokudai.ac.jp