RIMS-1696

INTEGRAL SECTIONS OF SOME ELLIPTIC $K3$ SURFACE VIA THE BINARY GOLAY CODE

By

Hisanori OHASHI

May 2010

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

INTEGRAL SECTIONS OF SOME ELLIPTIC $K3$ SURFACE VIA THE BINARY GOLAY CODE

HISANORI OHASHI

Abstract. We study the Mordell-Weil lattice $E(K)$ of the elliptic $K3$ surface $y^2 = x^3 + t^{11} - t$ in characteristic 11. We give an exact description of $E(K)$ by using an embedding into a Niemeier lattice. Then we use the properties of the binary Golay code to enumerate the number of low length vectors. In particular we can compute the kissing number of this lattice (equivalently the number of integral sections) theoretically. We also answer a question posed by Dolgachev and Keum, showing that there are infinitely many wild automorphisms on the surface with an isolated fixed point.

1. Introduction

A $K3$ *surface* is a smooth projective surface S defined over an algebraically closed field k such that $K_S \sim 0$ and $H^1(S, \mathcal{O}_S) = 0$. One remarkable aspect of the theory of $K3$ surfaces is the close connection between finite symplectic automorphisms of $K3$ surfaces and the Mathieu group M_{24}, the oldest finite simple group of sporadic type [8, 7, 5, 6]. In this paper we want to take up a slightly different viewpoint of this special connection. It is concerned with the theory of *Mordell-Weil lattices* [11].

Let $f\colon S \to C$ an elliptic surface with at least one singular fiber and a section (O). Its generic fiber is an elliptic curve $(E/K, O)$ defined over the function field $K = k(C)$. We denote by (P) the section corresponding to a K-rational point $P \in E(K)$.

$$\begin{tikzcd}
P & \in & E \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & S \arrow[d, "f"] & \supset & (P) \\
& & \mathrm{Spec}\,K \arrow[r] \arrow[ull] & C \arrow[urr, "\sim"'] & &
\end{tikzcd}$$

In this setting, one defines the canonical height pairing $(\ ,\ )$ which gives $E(K)/(\text{torsion})$ a structure of (in general $\mathbb{Q}$-valued) positive-definite lattice [11]. $(E(K), (\ ,\ ))$ is called the Mordell-Weil lattice of f.

Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, JAPAN.

In this paper we let S be the unique supersingular $K3$ surface with Artin invariant $\sigma = 1$ in characteristic 11. This surface plays a crucial role in papers [12, 6] in different ways. They both find an elliptic surface structure on S which can be written as

$$y^2 = x^3 + t^{11} - t, \qquad k = \overline{\mathbb{F}_{11}}, \tag{1.1}$$

(see also [6, Lemma 3.5]). Our main theorem gives an exact description of the Mordell-Weil lattice of this elliptic surface in terms of the Niemeier lattice (see Theorem 2.1) $L(A_1^{24})$.

Theorem 1.1. Let $\{\mathsf{e}_1, \cdots, \mathsf{e}_{24}\}$ be the basis of A_1^{24} and we assume that $\{1, \cdots, 12\}$ constitutes an umbral dodecad of the binary Golay code. Then the Mordell-Weil lattice $E(K)$ of (1.1) is isomorphic to the orthogonal complement of the sublattice $N \subset L(A_1^{24})$ generated by

$$\left\{\mathsf{e}_1, \frac{1}{2}(\mathsf{e}_1 + \cdots + \mathsf{e}_{12}), \frac{1}{2}(\mathsf{e}_{13} + \cdots + \mathsf{e}_{24}), \mathsf{e}_{24}\right\}.$$

The *binary Golay code* and an *umbral dodecad* is an important ingredient in the construction of $L(A_1^{24})$, see Section 3 for a summary. The Mathieu group M_{24} appears as the automorphism group of the binary Golay code. We will make a full use of this fact in our computation of the number of integral sections of (1.1), see below. We also apply our study of Mordell-Weil lattice to solve the problem posed in [6].

Before introducing these applications, we would like to include an interpretation of our result into purely lattice-theoretic terms.

Theorem 1.2 (= Theorem 3.1)**.** Let M be an integral even positive-definite lattice with the following numerical invariants. $\mathrm{rank}(M) = 20$, the discriminant group $A_M \simeq (\mathbb{Z}/11\mathbb{Z})^2$, the minimal norm $\mu_M \geq 4$ and $\#O(M)$ is divisible by 11. Then this lattice M can be embedded into $L(A_1^{24})$ in such a way that the orthogonal complement N is generated by

$$\left\{\mathsf{e}_1, \frac{1}{2}(\mathsf{e}_1 + \cdots + \mathsf{e}_{12}), \frac{1}{2}(\mathsf{e}_{13} + \cdots + \mathsf{e}_{24}), \mathsf{e}_{24}\right\},$$

where we put the condition that $\{1, \cdots, 12\}$ is an umbral dodecad of the binary Golay code.

Section 3 is devoted to the proof of this theorem. The reduction of Theorem 1.1 to Theorem 1.2 is verified at the end of Section 2. Via the isomorphism $M \simeq E(K)$, the minimal vectors of M and the integral sections of (1.1) correspond to each other; hence the kissing number (see Section 2) and the number of integral sections coincide. The computation of them is our first application.

An *integral section* of the elliptic surface $f\colon S \to C$ is a section (P) such that $(P) \cap (O) = \emptyset$. It is an analogue of integral points of elliptic curves. In the case of rational elliptic surfaces, they are studied in detail in [13]. The properties of integral sections of elliptic $K3$ surfaces are not known. Especially the problem of finding a $K3$ surface with the largest number of integral sections remains unsolved [13, II, Question 4.3]. The next proposition computes the number of integral sections of (1.1) by using Theorem 1.1 and the connection to Mathieu group M_{24}.

Proposition 1.3 (= Proposition 4.2)**.** The kissing number of the lattice M is 12540. Equivalently, we have 12540 integral points on the elliptic curve (1.1).

Our enumeration is based on the properties of binary Golay code and M_{24}, especially the famous *Steiner property* (Proposition 4.1). Using the same method, we can further compute the number of vectors of next length, see Proposition 4.4.

Our next application is concerned with the automorphisms of S. An automorphism of a $K3$ surface in characteristic p is *wild* if it is of order p. Wild automorphisms are classified in [4, 5] according to the structures of their fixed loci. In characteristic 11, the possibility of the fixed locus is either a connected curve or an isolated one point, but the existence of the latter case has not been confirmed yet. Since for characteristic $p \leq 7$ we have such automorphisms and for characteristic $p \geq 13$ there are no such automorphisms, this problem of existence in characteristic 11 is interesting (see the sentence before Corollary 3.3 of [6]). We will prove the following existence result (Proposition 5.5).

Proposition 1.4. There exist infinitely many $P \in E(K)$ with the associated automorphism $t_P\alpha$ has an isolated fixed point.

Actually we will be able to give a more precise information for P with several byproducts in Section 5. First we will give a slightly different construction of the automorphism group $\mathrm{PSL}(2, \mathbb{F}_{11}) \cdot \mathbb{Z}/12\mathbb{Z}$ of the surface S. It is interesting that it seems that the difference corresponds to the exceptional isomorphism $\mathrm{PSU}_2(11) \simeq \mathrm{PSL}(2, \mathbb{F}_{11})$ of [6, Lemma 3.5]. With the help of [9], we can prove that every element of the Mordell-Weil lattice $E(K)$ is defined over $\mathbb{F}_{11^2}(t)$, Proposition 5.2. These together gives a very explicit description of the isometry group $O(E(K))$, Corollary 5.3. Combining these considerations and [6, Lemma 3.2], we obtain Proposition 5.5.

The strategy of the proof of Theorem 1.2 is as follows. We embed M into *some* Niemeier lattice L by constructing the orthogonal complement N, as in [7]. The difficulty is in determining L. Here the important tool is the existence of isometry of order 11. Together with the structure theory of isometry groups of Niemeier lattices, it excludes 21 of 24 Niemeier lattices. The impossibility of the Leech lattice is easily seen. We show that the lattice $L(A_2^{12})$ can also be excluded by reducing the problem to the condition $\mu_M \geq 4$. Here we have to recall the properties of ternary Golay codes; a summary is included in Section 3 for the convenience. In this way we can show that $L \simeq L(A_1^{24})$. Again we use the condition on μ_M to see the uniqueness of the embedding and we obtain Theorem 1.2.

Perhaps it is interesting to investigate an extension of Theorem 1.2 to other prime p. In fact for $p \equiv 3(\mod 4)$, $p \geq 11$ we have a Mordell-Weil lattice of supersingular $K3$ surface with Artin invariant 1 which has an embedding into some Niemeier lattice. But for $p \neq 11$ our method in this paper is not effective. The author does not know any work related to this direction.

Finally we remark that our lattice $E(K)$ is the one listed in [1] as $(\mathrm{PSL}(2, \mathbb{F}_{11}) \times D_{12}).C_2$.

Acknowledgement. The author is grateful to Professor Shigeru Mukai for introducing him to the papers [5, 6]. The author is grateful to Professor Tetsuji Shioda for the comments on the first draft of this paper and showing his private note. His suggestion of considering integral sections led this paper into this form. The author is grateful to Professor Matthias Schütt for pointing out a mistake in the first form of Theorem 3.1.

The author is supported by global COE program of Kyoto university. This work is supported by KAKENHI 21840031.

2. Lattices

A *lattice* L is a free $\mathbb{Z}$-module of finite rank endowed with a symmetric bilinear form $(\ ,\ )$. We shall restrict ourselves to *integral* lattices in the sense that $(\ ,\ )$ takes values in $\mathbb{Z}$. L is *even* if (l^2) is even for all $l \in L$. The symbol $\oplus$ indicates an orthogonal sum. A sublattice M is said to be *primitive* if L/M is torsion-free. For a positive-definite lattice L, the *minimal norm* μ_L is the number $\inf\{(l^2) \mid L \ni l \neq 0\}$. The number of elements l for which $(l^2) = \mu_L$ is called the *kissing number* of the lattice.

Let L be an (integral) even lattice. L is said to be *nondegenerate* (resp. *unimodular*) if the natural map $L \to L^* = \mathrm{Hom}(L, \mathbb{Z})$ is injective (resp. bijective). These conditions are equivalent to that the determinant $d(L)$ of the Gram matrix is $\neq 0$ (resp. $= \pm 1$). If L is nondegenerate, a canonical quadratic form $q_L \colon A_L \to \mathbb{Q}/2\mathbb{Z}$ is induced on the factor group $A_L = L^*/L$. We call (A_L, q_L) the *discriminant quadratic form* of L. For basic results on discriminant forms, we refer to [10].

We denote by U the hyperbolic lattice defined by the Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. A_m, D_n and E_l $(m \geq 1, n \geq 4, l = 6, 7, 8)$ denotes the positive-definite root lattice associated to the Dynkin diagram of each type.

$O(L)$ denotes the group of self-isometries. An element $l \in L$ of norm $(l^2) = 2$ is called a *root.* A root l determines a reflection $s_l \in O(L)$ by $s_l(x) = x - (x, l)l$. The *Weyl group* $W(L)$ is the normal subgroup of $O(L)$ generated by all reflections in roots.

A positive-definite even unimodular lattice of rank 24 is called a *Niemeier lattice.* They are classified by Niemeier:

Theorem 2.1. There are 24 isomorphism classes of Niemeier lattices. Each of them is uniquely determined by the sublattice R generated by all roots.

In this paper we denote by $L(R)$ the Niemeier lattice whose root sublattice is R. A detailed account of Niemeier lattices is in [3, Chapters 16 and 18]. The construction of $L(A_2^{12})$ and $L(A_1^{24})$ will be recalled in Section 3, too.

Reduction of Theorem 1.1 to Theorem 1.2. The verification is easy. We see that the singular fibers of (1.1) consists of 12 cuspidal fibers (type II in Kodaira's notation) at $t = 0, 1, \cdots, 10, \infty$. In particular all the fibers are irreducible. By the isomorphism $E(K) \simeq NS(S)/(\text{trivial lattice})$ we see that $E(K)$ is torsion-free, $\operatorname{rank} E(K) = 20$ and $A_{E(K)} \simeq (\mathbb{Z}/11\mathbb{Z})^2$ because S is supersingular with $\sigma = 1$. Moreover the canonical height pairing in $E(K)$ takes the form $(P, P) = 4 + 2(P, O)_S$, where $(\ ,\ )_S$ denotes the intersection pairing on S. Thus $E(K)$ is integral valued, even and $\mu_{E(K)} \geq 4$ follows. The last condition of Theorem 1.2 is verified by the existence of the automorphism $\alpha \colon (x, y, t) \mapsto (x, y, t + 1)$ preserving fibers and (O).

This induces an isometry of $E(K)$ of order 11, hence $11 \mid \#O(E(K))$. This completes the reduction.

As a further remark, we see that

$$P \text{ is integral} \Leftrightarrow (P^2) = 4.$$

On the other hand, we see in Section 4 that in fact $\mu_M = 4$. Hence integral sections and minimal vectors coincide via our identification.

3. The embedding theorem

In this section we prove Theorem 1.2.

Theorem 3.1 (=Theorem 1.2)**.** Let M be an integral even positive-definite lattice with the following numerical invariants. $\operatorname{rank}(M) = 20$, the discriminant group $A_M \simeq (\mathbb{Z}/11\mathbb{Z})^2$, the minimal norm $\mu_M \geq 4$ and $\#O(M)$ is divisible by 11. Then this lattice M can be embedded into $L(A_1^{24})$ in such a way that the orthogonal complement N is generated by

$$\left\{\mathsf{e}_1, \frac{1}{2}(\mathsf{e}_1 + \cdots + \mathsf{e}_{12}), \frac{1}{2}(\mathsf{e}_{13} + \cdots + \mathsf{e}_{24}), \mathsf{e}_{24}\right\},$$

where we put the condition that $\{1, \cdots, 12\}$ is an umbral dodecad of the binary Golay code.

We note that for the proof we have to consider also the *ternary* Golay code besides the binary Golay code. We include a summary of both in this section.

We start the proof of the theorem. To begin with, let us consider a lattice N which is generated by $\mathsf{g}_1, \cdots, \mathsf{g}_4$ whose Gram matrix in terms of this basis is given by $\begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix} \oplus \begin{pmatrix} 6 & 1 \\ 1 & 2 \end{pmatrix}$. By the classification of finite quadratic forms [10, Section 1] we see that the discriminant forms of M and N are both isomorphic to $(\mathbb{Z}/11\mathbb{Z})^2$ equipped with the quadratic form $q(l_1) = q(l_2) = 2/11,\ q(l_1 + l_2) = 4/11 \mod 2\mathbb{Z}$, where $\{l_1, l_2\}$ are the standard generators. Let $\{m_1, m_2\}$ and $\{n_1, n_2\}$ be such generators of (A_M, q_M) and (A_N, q_N). Because we have the congruence

$$1^2 + 4^2 + (\pm 4)^2 \equiv 0 \mod 11,$$

the subgroup of $A_M \oplus A_N$ generated by $m_1 + 4n_1 + 4n_2$ and $m_2 + 4n_1 - 4n_2$ is a totally isotropic subgroup. Hence we can take an overlattice L of $M \oplus N$ which is even unimodular of rank 24. Namely L is a Niemeier lattice.

Our next task is to determine L. Let us pick up an isometry ϕ of M of order 11, which exists by the assumption. The group $O(A_M, q_M) \simeq O_{-1}(2, \mathbb{F}_{11})$ is isomorphic to the dihedral group D_{12} of order 24. Hence ϕ extends to an element of $O(L)$, which we still denote by ϕ, that acts on N trivially. Then we use the assumption $\mu_M \geq 4$ to see that ϕ gives a nontrivial element of order 11 in the factor group $O(L)/W(L)$ by [7, Lemma 6]. Let us consult [3, Table 16.1]. There the order of the group $O(L)/W(L)$ is presented as the number $\mid G_1 \mid \cdot \mid G_2 \mid$ except for the case of Leech lattice Λ. As we have seen it is divisible by 11, so we have either $L \simeq L(A_2^{12}), L(A_1^{24})$ or Λ. Obviously N has a root, so that $L = \Lambda$ is excluded.

Impossibility of $L = L(A_2^{12})$. Here we exclude the possibility of $L = L(A_2^{12})$.

Let us recall the structure of the Niemeier lattice of type A_2^{12}. Let e, f be the basis of root lattice A_2 with relations $(\mathsf{e}^2) = (\mathsf{f}^2) = 2, (\mathsf{e}, \mathsf{f}) = -1$. The dual lattice A_2^* is generated by A_2 and the element $\tilde{h} = (\mathsf{e} + 2\mathsf{f})/3$, and the discriminant group A_2^*/A_2 is isomorphic to $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ generated by the residue class h of $\tilde{h}$. We fix this isomorphism. Let $\mathsf{e}_i, \mathsf{f}_i$ $(1 \leq i \leq 12)$ be the basis of 12 copies of A_2 and we regard them as generators of $R = A_2^{12}$. We obtain the isomorphism $R^*/R \simeq \mathbb{F}_3^{12}$; the Niemeier lattice $L(A_2^{12})$ is defined as the overlattice of R, such that $L(A_2^{12})/R = \mathcal{C}_{12} \subset R^*/R$, where the *ternary Golay code* $\mathcal{C}_{12}$ is a particular 6-dimensional subspace of $\mathbb{F}_3^{12}$ with special properties.

To formulate the property of $\mathcal{C}_{12}$, we introduce the following. For an element $x = x_1 h_1 + \cdots + x_{12} h_{12} \in \mathbb{F}_3^{12}$, the *Hamming weight* is by definition

$$\mathrm{wt}(x) = \#\{i \mid x_i \neq 0\}.$$

One of special properties of $\mathcal{C}_{12}$ is that, for elements $x \in \mathcal{C}_{12}$, the Hamming weight takes only values $0, 6, 9$ or 12. In fact the number of elements of each Hamming weight is known, $1, 264, 440$ or 24 respectively, but we don't need these precise numbers.

We prepare two lemmas.

Lemma 3.2. Let A_2 be the root lattice and A_2^* its dual. We can classify all low-length vectors in A_2^* easily and we obtain the following.

(1) Every element $x \in A_2^*$ has either $(x^2) = 0, 2/3, 2$ or $(x^2) \geq 8/3$.
(2) If $(x^2) = 2/3$, then there exists some root $r \in A_2$ such that $(r, x) = 0$.
(3) If $(x^2) = 6$, then there exist no roots $r \in A_2$ such that $(r, x) = 1$.
(4) There exist no elements $x \in A_2^*$ with $(x^2) = 4$.

Lemma 3.3. For a subset $B \subset L(A_2^{12})$, let $n(B)$ be the following:

$$n(B) := \# \left\{ i \;\middle|\; \begin{array}{l} \text{there exist some root } r \text{ in the } i\text{-th component of } A_2^{12} \\ \text{which is orthogonal to every element of } B. \end{array} \right\}.$$

Here the i-th component is the sublattice generated by e_i and f_i. Then, For any root $r \in L(A_2^{12})$ we have $n(B \cup \{r\}) \geq n(B) - 1$.

Proof. Because every root of $L(A_2^{12})$ is contained in one unique component, the inequality holds. □

In the following we show that any embedding k of N into $L(A_2^{12})$ has some root in its orthogonal complement, so that we get a contradiction to the assumption on the minimal norm of M. We put $g_i := k(\mathsf{g}_i)$. Since g_1, g_4 are roots, by Lemma 3.3 it is sufficient to see $n(g_2, g_3) \geq 3$. Let us classify elements x of $L(A_2^{12})$ with norm 6. By Lemma 3.2(1), $\mathrm{wt}(x) = 12$ is not the case. Similarly if $\mathrm{wt}(x) = 9$ then x is the sum of elements from 9 of 12 components, all of which is of norm 2/3. We describe this situation by saying that x is of the form $9 \cdot (2/3)$. In the same way if $\mathrm{wt}(x) = 6$ then x is of the form either $6 \cdot (2/3) + (2)$ or $5 \cdot (2/3) + (8/3)$. If $\mathrm{wt}(x) = 0$ then x is of the form either $3 \cdot (2)$ or (6) by using Lemma 3.2(4). We apply this to $x = g_2$ and g_3. Considering the existence of g_1 and g_4, Lemma 3.2(3) excludes the case of the form (6).

Thus we obtain four possibilities for the form of each g_2 and g_3. In every combination, we will see the minimum possibility of the value $n(g_2, g_3)$ as in the following table.

forms of g_2 and g_3	$9 \cdot (2/3)$	$6 \cdot (2/3) + (2)$	$5 \cdot (2/3) + (8/3)$	$3 \cdot 2$
$9 \cdot (2/3)$	3	5	6	9
$6 \cdot (2/3) + (2)$		4	5	8
$5 \cdot (2/3) + (8/3)$			5	8
$3 \cdot (2)$				6

In the table, because we have a symmetry the entries below the diagonal are kept blank. Let us confirm the table in the case g_2 is of the form $9 \cdot (2/3)$ and g_3 is $6 \cdot (2/3) + (2)$, for example. We prepare 12 boxes which corresponds to the 12 components of $(A_2)^{12}$. For each g_2 or g_3, we write the numbers 2/3, 2 and 8/3 in the box arbitrarily, but in the way obeying the given form of g_2 or g_3.

g_2	2/3	2/3	2/3	2/3	2/3	2/3	2/3	2/3	2/3			
g_3				2/3	2/3	2/3	2/3	2/3	2/3	2		
sum	2/3	2/3	2/3	4/3	4/3	4/3	4/3	4/3	4/3	2	0	0

Below the box we add the "sum" row, whose entry is just the sum in the box. The values $n(g_2, g_3)$ in the table is just the number of entries in the sum which is $\leq 2/3$. It is a consequence of Lemma 3.2 (2). Thus the minimum of $n(g_2, g_3)$ happens exactly when the overlap between 2/3 entries of g_2 and g_3 is maximal and other entries are scattered. The other cases are treated in the same way.

Since the value $n(g_2, g_3)$ is always more than 2, the case $L = L(A_2^{12})$ is excluded.

A summary on $L(A_1^{24})$. Let us recall the structure of $L(A_1^{24})$. Let e_i, $(1 \leq i \leq 24)$ be the basis of $R = A_1^{24}$ with the relation $(\mathsf{e}_i^2) = 2, (\mathsf{e}_i, \mathsf{e}_j) = 0$. We have the isomorphism $R^*/R \simeq \mathbb{F}_2^{24}$. In the vector space $\mathbb{F}_2^{24}$, we have a special 12-dimensional subspace called the *binary Golay code* $\mathcal{C}_{24}$. The Niemeier lattice $L(A_1^{24})$ is defined as $L(A_1^{24})/R = \mathcal{C}_{24} \subset R^*/R$.

We remark that $\mathbb{F}_2^{24} \simeq R^*/R$ has the basis $\{(1/2)\mathsf{e}_i \mid 1 \leq i \leq 24\}$. This space can be identified naturally with the power set 2^Ω of $\Omega = \{1, 2, \cdots, 24\}$, whose addition is given by the symmetric difference $A \ominus B = (A \cup B) - (A \cap B)$ between subsets $A, B \subset \Omega$. For $I \subset \Omega$, if we write $x_I := \sum_{i \in I}(1/2)\mathsf{e}_i$ then the Hamming weight of x_I is just $\# I$. In the following, we identify elements of $\mathcal{C}_{24}$ with subsets of Ω.

It is known that the Hamming weight of elements of the binary Golay code $\mathcal{C}_{24}$ takes only values $0, 8, 12, 16$ and 24. We call an element of weight 8 a *(special) octad*, and weight 12 an *(umbral) dodecad*. It is known that there are 759 octads and 2576 dodecads. Since there exists an element of weight 24, $\mathcal{C}_{24}$ (as a subset of 2^Ω) is closed under taking complements. Permutations of Ω that preserves $\mathcal{C}_{24}$ constitute the *Mathieu group* M_{24}. This is one of the finite simple groups of sporadic type. M_{24} acts on the set of dodecads transitively and the stabilizer subgroup is isomorphic to M_{12}, [2, Theorem 15]. This M_{12} is $1 + 3$ transitive on the dodecad and its complement. We use this fact frequently. For the account of these beautiful facts, we refer to [2].

Conclusion. So far we have proved $L = L(A_1^{24})$. In this case we can show that the embedding of N is unique up to automorphisms, and obtain Theorem 3.1. As in the case of $L(A_2^{12})$ let $k \colon N \to L(A_1^{24})$ be the given embedding such that M is the orthogonal complement of $k(N)$. We put $g_i = k(\mathsf{g}_i)$. An element $x \in L(A_1^{24})$ with $(x^2) = 6$, such as g_2, g_3, is either of the form $12 \cdot (1/2)$ ($\mathrm{wt}(x) = 12$), $8 \cdot (1/2) + (2)$ ($\mathrm{wt}(x) = 8$) or $3 \cdot (2)$. But here it is easy to see that to have no roots in the orthogonal complement, g_2 and g_3 both has to be of the form $12 \cdot (1/2)$ and their underlying dodecads must be complementary, so that there exists a dodecad $\mathcal{D}$ such that $g_2 = (1/2)\sum_{i\in\mathcal{D}}(\pm\mathsf{e}_i)$ and $g_3 = (1/2)\sum_{i\in\Omega-\mathcal{D}}(\pm\mathsf{e}_i)$. We can re-index Ω so that we can assume $\mathcal{D} = \{1, 2, \cdots, 12\}$. On the other hand, by the $1+3$ transitivity, we can assume $g_1 = \pm\mathsf{e}_1$ and $g_4 = \pm\mathsf{e}_{24}$. Finally we can adjust the signature by the Weyl group action, and we obtain Theorem 3.1.

4. Low length vectors

Let $L(A_1^{24})$ be the Niemeier lattice of type A_1^{24} and N be the primitive sublattice generated by $\{\mathsf{e}_1, \frac{1}{2}(\mathsf{e}_1 + \cdots + \mathsf{e}_{12}), \frac{1}{2}(\mathsf{e}_{13} + \cdots + \mathsf{e}_{24}), \mathsf{e}_{24}\}$, where $\mathcal{D}_1 = \{1, \cdots, 12\}$ is a dodecad. We refer to [3] or the previous section for the summary on $L(A_1^{24})$. Let M be the orthogonal complement of N. In this section we compute the number of vectors of norm 4 and 6 in M. The number of norm 4 vectors has a meaning: it is the kissing number of M, or the number of integral points of the elliptic curve $y^2 = x^3 + t^{11} - t$ as we explained in the introduction.

We put $\mathcal{D}_2 = \Omega - \mathcal{D}_1$.

4.1. minimal vectors.

Elements of L of norm 4 is easily seen to be one of the following forms:

- Type I: $\pm\mathsf{e}_j \pm \mathsf{e}_k$ for $j \neq k$,
- Type II: $\sum_{i\in\mathcal{O}} \pm(1/2)\mathsf{e}_i$ for $\mathcal{O}$ an octad.

The condition for a vector of type I to be orthogonal to N is that, either $\{j, k\} \subset \mathcal{D}_1 - \{1\}$ or $\{j, k\} \subset \mathcal{D}_2 - \{24\}$, and it is of the form $\pm(\mathsf{e}_j - \mathsf{e}_k)$. Thus we obtain $2\binom{11}{2} + 2\binom{11}{2} = 220$ vectors.

Next we consider type II vectors. The choice of sign depends on $(\#\mathcal{O}\cap\mathcal{D}_1, \#\mathcal{O}\cap\mathcal{D}_2)$, so in general let us call $\mathcal{O}$ an (a, b)-octad if $(\#\mathcal{O}\cap\mathcal{D}_1, \#\mathcal{O}\cap\mathcal{D}_2) = (a, b)$. There exist $(2, 6)$, $(4, 4)$ and $(6, 2)$-octads.

Let $\mathcal{S}$ be the set of $(6, 2)$-octads. Recall that the *Steiner property* of the binary Golay code is the following proposition.

Proposition 4.1. *For any 5-element subset A of Ω, there exists a unique octad that contains A.*

By this property, for any 5-element set $A \subset \mathcal{D}_1$, we have a unique octad that contains A, which is necessarily a $(6,2)$-octad. This correspondence is clearly 6 to 1, so $\#\mathcal{S} = \begin{pmatrix} 12 \\ 5 \end{pmatrix} /6 = 132$. On the other hand, $\mathcal{S}$ has the involution $\iota\colon \mathcal{O} \mapsto \mathcal{O} \ominus \mathcal{D}_1$, which gives a bijection between the subsets $\mathcal{S}^+ = \{\mathcal{O} \in \mathcal{S} \mid 1 \in \mathcal{O}\}$ and $\mathcal{S}^- = \{\mathcal{O} \in \mathcal{S} \mid 1 \notin \mathcal{O}\}$. Thus $\#\mathcal{S}^+ = \mathcal{S}^- = 66$.

Let us consider next the map $\varphi\colon \mathcal{S} \to T := \{2 \text{ points of } \mathcal{D}_2\}, \mathcal{O} \mapsto \mathcal{O} \cap \mathcal{D}_2$. This is compatible with ι and defines $\mathcal{S}/\iota \simeq \mathcal{S}^- \to T$. Since the stabilizer M_{12} is $1+3$ transitive on $\mathcal{D}_1$ and $\mathcal{D}_2$, φ is surjective. Then the accidental equality $\#T = \begin{pmatrix} 12 \\ 2 \end{pmatrix} = 66$ shows that φ induces a bijection of $\mathcal{S}^-$ and T.

Thus, we see that there are $\begin{pmatrix} 11 \\ 2 \end{pmatrix} = 55$ $(6,2)$-octads which is disjoint from $\{1,24\}$. Since there exists an involution that exchanges $\mathcal{D}_1$ and $\mathcal{D}_2$, the same number of $(2,6)$-octads exist. By [2, Table 10.1], there exist exactly 330 octads which is disjoint from $\{1,24\}$. Hence we have 220 $(4,4)$-octads which is disjoint from $\{1,24\}$. Taking the choice of sign into consideration, we obtain

$$55 \begin{pmatrix} 6 \\ 3 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} + 220 \begin{pmatrix} 4 \\ 2 \end{pmatrix} \begin{pmatrix} 4 \\ 2 \end{pmatrix} + 55 \begin{pmatrix} 2 \\ 1 \end{pmatrix} \begin{pmatrix} 6 \\ 3 \end{pmatrix} = 12320$$

vectors of type II. In sum, we obtain

Proposition 4.2. The kissing number of the lattice M is 12540. Equivalently, we have 12540 integral points on the elliptic curve (1.1).

We summarize the following lemma for the use in the next subsection.

Lemma 4.3. The number of $(6,2)$, $(4,4)$ or $(2,6)$-octads which is disjoint from $\{1,24\}$ is $55, 220$ or 55 respectively.

4.2. **Norm 6 vectors.** We can compute in the same way the number of vectors of norm 6 in M. It might be of another interest, so let us include here. Vectors of norm 6 in $L(A_1^{24})$ are one of the following forms.

- Type I: $\pm \mathsf{e}_j \pm \mathsf{e}_k \pm \mathsf{e}_l$ for $j \neq k \neq l \neq j$,
- Type II: $\pm \mathsf{e}_j + \sum_{i \in \mathcal{O}} \pm (1/2) \mathsf{e}_i$ for $\mathcal{O}$ an octad which doesn't contain j,
- Type III: $\sum_{i \in \mathcal{D}} \pm (1/2) \mathsf{e}_i$ for $\mathcal{D}$ a dodecad.

Type I vectors cannot be orthogonal to N. Type II vectors are easily counted using Lemma 4.3. For example, if $\mathcal{O}$ is a $(6,2)$-octad and $j \in \mathcal{D}_1$ then the choice of j has

5, the sign has $2\begin{pmatrix}6\\2\end{pmatrix}\begin{pmatrix}2\\1\end{pmatrix}$, so there are $5 \cdot 60 \cdot 55 = 16500$ vectors, etc. Here we obtain 220440 vectors.

The counting of Type III vectors can also be reduced to Lemma 4.3. As in the previous subsection, the main point is the number of $(4,8)$-dodecads $\mathcal{D}$ disjoint from $\{1,24\}$. Such $\mathcal{D}$ are in one-to-one correspondence to $(4,4)$-octads $\mathcal{O}$ such that $1 \notin \mathcal{O}$ and $24 \in \mathcal{O}$ by $\mathcal{O} = \mathcal{D} \ominus \mathcal{D}_2$. We denote by $\mathcal{Q}$ the set of these octads.

Let R be the set of 4 element subsets of $\mathcal{D}_1 - \{1\}$. Clearly $\#R = 330$. We have a natural injection $\mathcal{Q} \to R, \mathcal{O} \mapsto \mathcal{O} \cap \mathcal{D}_1$. For an element $A \in R$, $A \cup \{24\}$ defines uniquely an octad $\mathcal{O}'$ by the Steiner property. Moreover $\mathcal{O}' \notin \mathcal{Q}$ if and only if $\mathcal{O}'$ is a $(6,2)$-octad that contains 24. By the bijection $\mathcal{S}/\iota \simeq T$ from the previous subsection, we have eleven such $\mathcal{O}'$ with $1 \in \mathcal{O}'$ and eleven such $\mathcal{O}''$ with $1 \notin \mathcal{O}''$, so we obtain the number $\#\mathcal{Q} = \#R - 11 \cdot 5 - 11 \cdot \begin{pmatrix}6\\4\end{pmatrix} = 110$.

Using [2, table 1.2] as in the previous subsection, we see that the number of $(4,8)$, $(6,6)$ and $(8,4)$-octads disjoint from $\{1,24\}$ is 110, 396 and 110 respectively. Taking the sign into consideration, we obtain

$$110\begin{pmatrix}4\\2\end{pmatrix}\begin{pmatrix}8\\4\end{pmatrix} + 396\begin{pmatrix}6\\3\end{pmatrix}\begin{pmatrix}6\\3\end{pmatrix} + 110\begin{pmatrix}8\\4\end{pmatrix}\begin{pmatrix}4\\2\end{pmatrix} = 250800$$

vectors of Type III. In sum, we obtain

Proposition 4.4. There are 471240 vectors of norm 6 in M.

5. Automorphisms

Let S be the elliptic $K3$ surface defined by $y^2 = x^3 + t^{11} - t$ in characteristic 11. There exist many symmetries on the surface S, as shown in [6]. Let us give a slightly different description. Let α be the automorphism defined by $(x,y,t) \mapsto (x,y,t+1)$, β be defined by $(x,y,t) \mapsto (x/t^4, y/t^6, -1/t)$. Moreover let γ be defined by $(x,y,t) \mapsto (\zeta^2 x, \zeta^3 y, \zeta^6 t)$, where $\zeta = \zeta_{60} \in \mathbb{F}_{11^2}$ is a primitive 60-th root of unity in characteristic 11. We note that they all preserve the zero-section (O).

Let $H = \langle \alpha, \beta \rangle$. The fundamental defining relation for $\mathrm{PSL}(2,\mathbb{F}_{11})$,

$$\mathrm{PSL}(2,\mathbb{F}_{11}) = \langle a, b \mid a^{11} = (a^4 b a^6 b)^2 = 1, (ab)^3 = b^2 \rangle, \tag{5.1}$$

found in ATLAS shows that $H \simeq \mathrm{PSL}(2,\mathbb{F}_{11})$. In particular H is symplectic. Let $G = \langle \alpha, \beta, \gamma \rangle$. By the relation $\gamma^{12} = \alpha^{d^9}\beta\alpha^{d}\beta\alpha^{d^9}\beta$ where $d = \zeta^6$ is an element in $\mathbb{F}_{11}$, and by the fact that γ^5 acts on S purely non-symplectically, we obtain the structure of G:

$$G \simeq \mathrm{PSL}(2, \mathbb{F}_{11}) \cdot \mathbb{Z}/12\mathbb{Z}.$$

Thus G has order 7920. In [6] they use the automorphism group $\mathrm{GU}(2, 11)/\{\pm 1\}$ of the surface S. Although they are isomorphic, $\mathrm{GU}(2, 11)/\{\pm 1\} \simeq \mathrm{PSL}(2, \mathbb{F}_{11}) \cdot \mathbb{Z}/12\mathbb{Z}$, this isomorphism is not canonical and corresponds to the change of variables (done over $\mathbb{F}_{11^4}$) in [6, Lemma 3.5]. We also note that the action of our G is defined over the quadratic extension $\mathbb{F}_{11^2}$, since $\zeta \in \mathbb{F}_{11^2}$.

Remark 5.1. γ^{30} is the inversion of the fibers. Its fixed locus consists of (O) and a curve C of genus 10. C passes through the 12 cusps of the singular fibers. The quotient S/γ^{30} is hence the Hirzebruch surface of degree 4. Since γ^{30} is in the center of G, G/γ^{30} acts on C. This gives one counterexample to the Hurwitz's formula $\# \mathrm{Aut}(C) \leq 84(g-1)$, which is valid in characteristic zero.

Let us combine Theorem 3.1 and these automorphism groups.

Proposition 5.2. Every element of the Mordell-Weil lattice $E(K)$ is defined over $\mathbb{F}_{11^2}(t)$. Namely the minimal splitting field is $\mathbb{F}_{11^2}(t)$.

Proof. Since all the fibers of the fibration are irreducible, we have a natural isomorphism $NS(S) \simeq U \oplus E(K)$. G acts on $E(K)$ as isometries, and since the representation of $\mathrm{Aut}(S)$ on $NS(S)$ is faithful, we see $G \subset O(E(K))$.

Let us consider the Frobenius map η, which acts on a section $(x(t), y(t)) \in E(K)$ by 11-th power on the coefficients, where we regard $x(t), y(t)$ as rational functions in t. This map is well-defined since the equation of S is defined over the prime field. By [11, Proposition 8.13], η acts on $E(K)$ as isometries.

On the other hand, [9, Theorem IX.1] finds a group named $[L_2(11) \overset{2(3)}{\otimes} D_{12}]_{20}$ of order 15840 and maximal in $\mathrm{GL}(20, \mathbb{Q})$, together with the numerical invariants of a lattice on which it acts. Our Theorem 3.1 shows that their lattice coincide with $E(K)$. Therefore $\#O(E(K)) = 15840$. Since any power of η does not come from $\mathrm{Aut}(S)$ except for the identity map, η is at most order 2. This shows that every section is defined over at most $\mathbb{F}_{11^2}(t)$.

In the other direction, obviously γ sends a section defined over $\mathbb{F}_{11}(t)$ to one over $\mathbb{F}_{11^2}(t)$, thus η is not identical on $E(K)$. □

Corollary 5.3. The orthogonal group $O(E(K))$ is generated by G and the Frobenius η.

On a question of Dolgachev and Keum. In [6] they posed the following question: *Is there a $\tau \in E(K)$ such that the fixed locus $S^{\tau\alpha}$ consists of an isolated point?* Here τ is considered as a fiberwise translation automorphism of S. Our arguments give an answer to this question.

In the following, for $P \in E(K)$, the translation automorphism is denoted by t_P. [6, Lemma 3.2] shows that $t_P\alpha$ has order 11.

Lemma 5.4. *$t_P\alpha$ has an isolated fixed point if and only if (P) and (O) do not meet over $t = \infty$.*

Proof. By the definition of α, the fixed point locus of $t_P\alpha$ is contained in the fiber S_∞ over $t = \infty$. S_∞ is a cuspidal curve and therefore its group structure is isomorphic to $\mathbb{G}_a$. Since t_P acts on it by a translation, the lemma is clear. □

Thus every integral section induces such an automorphism. In fact, Proposition 5.2 gives infinitely many such.

Proposition 5.5. *Sections $P \in E(K)$ with $\#S^{t_P\alpha} < \infty$ consist of the set-theoretic complement to a sublattice of $E(K)$ of index 11^2. In particular there exist infinitely many $P \in E(K)$ whose $t_P\alpha$ has an isolated fixed point.*

Proof. We consider the specialization homomorphism

$$sp\colon E(K) \to S_\infty^\# \simeq \mathbb{G}_a, P \mapsto (P) \cap S_\infty.$$

Explicitly, we can write down $sp(x(t), y(t)) = \lim_{t\to\infty}(x/t^4)/(y/t^6)$ under the identification $\mathbb{G}_a = \overline{\mathbb{F}_{11}}$. This is an integer-coefficient rational function in the coefficients of $x(t), y(t)$. By Proposition 5.2 the image of sp is contained in the subfield $\mathbb{F}_{11^2}$. On the other hand, for $P \in E(K)$, we see that $sp(\gamma(P)) = \zeta^{-11}sp(P)$. If P is integral, since $sp(P) \neq 0$, this element and $sp(\gamma(P))$ spans the subfield $\mathbb{F}_{11^2}$. Thus sp is surjective onto $\mathbb{F}_{11^2}$ and the proposition follows. □

References

[1] G. Nebe and N. Sloane, Catalogue of Lattices, http://www2.research.att.com/ njas/lattices/

[2] J. H. Conway, "Three lectures on exceptional groups" in *Finite Simple Groups*, (Proc. Instructional Conf., Oxford, 1969), Academic Press, London, 1971, 215-247. (Also in [3])

[3] J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups, 3rd ed., Grundlehren der Mathematischen Wissenschaften **290**, Springer-Verlag, (1999).

[4] I. V. Dolgachev and J. H. Keum, Wild p-cyclic actions on $K3$-surfaces, J. Algebraic Geometry, **10** (2001), 101-131.

[5] I. V. Dolgachev and J. H. Keum, Finite groups of symplectic automorphisms of $K3$ surfaces in positive characteristic, Ann. of Math., **169** (2009), 269-313.

[6] I. V. Dolgachev and J. H. Keum, $K3$ surfaces with a symplectic automorphism of order 11, J. Eur. Math. Soc., **11** (2009), 799-818.

[7] S. Kondo, Niemeier lattices, Mathieu groups, and finite groups of symplectic automorphisms of $K3$ surfaces, Duke Math. J., **92** (1998), 593-598.

[8] S. Mukai, Finite groups of automorphisms of K3 surfaces and the Mathieu group, Invent. Math., **94** (1988), 183-221.

[9] G. Nebe and W. Plesken, Finite Rational Matrix Groups, Mem. Amer. Math. Soc., **116** (1995), no. 556, viii+144 pp.

[10] V. V. Nikulin, Integral symmetric bilinear forms and some of their applications (English translation). Math. USSR Izv., **14** (1980), 103-167.

[11] T. Shioda, On the Mordell-Weil lattices, Com. Math. Univ. St. Pauli, **39** (1990), 473-489.

[12] T. Shioda, Mordell-Weil lattices and sphere packings, Am. J. Math., **113** (1991), 931-948.

[13] T. Shioda, Gröbner basis, Mordell-Weil lattices and deformation of singularities, I, II, Proc. Jpn. Acad., Ser. A, **86** (2010), I: 21-26, II: 27-32.