TOKYO J. MATH.
VOL. 19, NO. 2, 1996

Quadratic Residue Graph and Shioda Elliptic Modular Surface $S(4)$

Hirotachi ABO, Nobuo SASAKURA and Tomohide TERASOMA

Tokyo Metropolitan University

Dedicated to the memory of Professor M. Ishida*

0. Introduction

For each prime number $p \equiv 1 \pmod 4$, one attaches a graph without direction to the prime field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ by means of the Legendre symbol (cf. §1.1). This graph leads naturally to a rank two reflexive sheaf, denoted $\mathfrak{E}_p$, on the $(p-1)$-dimensional complex projective space $\mathbf{P}_{p-1}(\mathbf{C})$ (cf. [SEK 1], [SEK 2]). If $p=5$, then it coincides with the Horrocks-Mumford bundle (cf. [H-M]). The sheaf is both arithmetic and combinatorial in nature and it is seen that invariants of the graph are useful to describe the structure of the sheaf $\mathfrak{E}_p$. As a typical example, which is our main result in [SEK 2], the fourth Chern class $c_4(\mathfrak{E}_p)$ $(\in \mathbf{Z})$ is given by

$$c_4(\mathfrak{E}_p) = -40\mathcal{N}\,, \tag{C1}$$

where (cf. §1.1)

$$\mathcal{N} = \#\{I \subset \mathbf{F}_p \mid \#I = 4 \text{ and whose graph is isomorphic to the square}\}\,.$$

The set is related explicitly to a $K3$ surface, denoted V, which is defined to be the locus of the following quadratic relations in the five dimensional projective space $\mathbf{P}_5(\mathbf{F}_p)$ with homogeneous coordinates $z_{\alpha\beta}$ $(1 \le \alpha \le \beta \le 4)$ (cf. [SEK 1])

$$z_{\alpha\beta}^2 + z_{\beta\gamma}^2 = z_{\alpha\gamma}^2 \qquad (1 \le \alpha < \beta < \gamma \le 4)\,. \tag{C2}$$

Now, it is known that the Shioda elliptic modular surface $S(4)$ of level 4 is birationally equivalent to a certain Kummer surface (cf. [Sh 3]). In §1 we see that V is biregularly equivalent to the Kummer surface. By a structure theorem of $S(4)$ (cf. [Sh 3]), the zeta function of $S(4)$ (and so that of V) is expressed by means of the Gaussian sum. Using this we give the following explicit form for (C1)

Received January 19, 1995

* To the memory of his generosity for younger mathematicians and to his high regard for the reciprocity law in the quadratic residue theory.

(C3) $$c_4(\mathfrak{E}_p)=(-5/64)p(p-1)(p^2-6p+1+4a^2),$$

where a is an odd integer determined by the equation

$$p=a^2+b^2 \qquad \text{with an even integer } b.$$

We also give an interesting graph theoretical interpretation of the formula (cf. §3). Next we see that V is a contraction of $S(4)$ and study the contraction closely. Define a divisor on $S(4)$

$$D=\sum_{(\rho,\sigma)=(\pm a_4,\pm b_4)} \tilde{r}_{\rho,\sigma}+\sum_{s_1=0,\infty}\sum_{t_1=0,\infty}(\tilde{\Psi}_{\mathbf{P}_1}^{-1}(s_1)-\Theta_{s_1t_1}),$$

where $\tilde{r}_{\rho,\sigma}$ are 4-torsion sections of the elliptic surface $\tilde{\Psi}: S(4)\to\mathbf{P}_1$ and a_4 and b_4 are the basis of the level 4 structure of a generic fibre. The surface $S(4)$ admits another structure of an elliptic fibration $S(4)\to\mathbf{P}_1$ and t_1 denotes a local coordinate of the base space. The curve $\Theta_{s_1t_1}$ is determined by the two structures (cf. §2). Also we fix a sublinear system $\mathfrak{L}$ of dimension 6 of $H^0(S(4), \mathcal{O}_{S(4)}(D))$. In Theorem 2.5 we contract $S(4)$ to V by means of $\mathfrak{L}$, by making clear a combinatorial property of the contraction. Concerning Theorem 2.5, we make the following remark. The fact that the Kummer surface is a contraction of $S(4)$ may have been known. By the simple form of V we may regard it as a suitable projective model of the Kummer surface. This fact and the combinatorial property of the linear system $\mathfrak{L}$ is our key point. Next, in [B-H], W. Barth and K. Hulek discussed projective models of the Shioda modular surface $S(n)$ $(3\leq n)$ and found a good model for the case of $n=5$. (See also [B-H-M] for the application to the Horrocks-Mumford bundle.) In the case of $n=4$, the situation is complicated (cf. p. 96, [B-H]). They did not give an appropriate model. The surface V may be used to find the nice projective model of $S(4)$.

REMARK. This note consists of arithmetic and algebro-geometric parts. In the first part we mainly work with a prime field $\mathbf{F}_p$, p being a prime $\equiv 1 \pmod 4$ (cf. §1.1, §1.2 and §3). In the other parts we work with a field k satisfying the following condition

(a) the characteristic of $k\neq 2$, and k contains a 4-th primitive root ζ_4 of 1.

1. Quadratic residue graph.

1.1. Quadratic residue graph. Let p be a prime number $\equiv 1 \pmod 4$ so that $\left(\frac{-1}{p}\right)=1$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol, and let $\mathbf{F}_p$ be the prime field $\mathbf{Z}/p\mathbf{Z}$. Then we attach to $\mathbf{F}_p$ a graph without direction as follows:

$$\mathbf{F}_p=\text{the set of vertices},$$

$$\left\{(i,j)\in\mathbf{F}_p\times\mathbf{F}_p \,\middle|\, \left(\frac{i-j}{p}\right)=1\right\}=\text{the set of edges}.$$

To each $i \in \mathbf{F}_p$, we attach subsets of $\mathbf{F}_p$

$$S_i^+ = \left\{ j \in \mathbf{F}_p \,\middle|\, \left(\frac{i-j}{p}\right) = 1 \right\}, \qquad S_i^- = \left\{ j \in \mathbf{F}_p \,\middle|\, \left(\frac{i-j}{p}\right) = -1 \right\}.$$

Let $i_1, i_2, \cdots, i_d$ be distinct elements of $\mathbf{F}_p$, and let $\mu_k \in \{\pm 1\}$ $(1 \leq k \leq d)$. We set

$$S_{i_1}^{\mu_1} \cdots {}_{i_d}^{\mu_d} = \bigcap_{k=1}^{k=d} S_{i_k}^{\mu_k}. \tag{1.1}$$

The semidirect product $\mathbf{F}_p \rtimes \mathbf{F}_p^\times$, $\mathbf{F}_p^\times = \mathbf{F}_p - \{0\}$, acts on $\mathbf{F}_p$

$$x \to ax + b \qquad ((b, a) \in \mathbf{F}_p \times \mathbf{F}_p^\times)$$

and acts on the set of all subsets of $\mathbf{F}_p$. Denote by $j_1, \cdots, j_d$ the image of $i_1, \cdots, i_d$ by the action of the element (b, a). Then we have

$$(b, a)(S_{i_1}^{\mu_1} \cdots {}_{i_d}^{\mu_d}) = S_{j_1}^{\nu_1} \cdots {}_{j_d}^{\nu_d} \tag{1.2}$$

with $\nu_k = \left(\frac{a}{p}\right)\mu_k$ $(k = 1, \cdots, d)$, where we identify $\mu_k = \pm$ with ± 1.

Next we introduce certain collections of subsets of $\mathbf{F}_p$. For each integer d, $1 \leq d \leq p$, let $\mathscr{P}_d(\mathbf{F}_p)$ denote the collection of subsets I of $\mathbf{F}_p$ whose cardinality $\#I = d$. Two elements $I, J \in \mathscr{P}_d(\mathbf{F}_p)$ are *equivalent* or *complementary* (with respect to the graph) if there is a bijection $\theta : I \to J$ so that

$(\theta(i), \theta(j))$ is an edge if and only if (i, j) is an edge (resp. is not an edge).

This equivalence divides $\mathscr{P}_d(\mathbf{F}_p)$ into disjoint classes. Clearly $\mathscr{P}_2(\mathbf{F}_p)$ and $\mathscr{P}_3(\mathbf{F}_p)$ consist of two and four equivalence classes respectively. We write them $\mathscr{C}_{2;d}$ $(d = 0, 1)$ and $\mathscr{C}_{3;d}$ $(d = 0, 1, 2, 3)$ so that each representative of the class in question has exactly d edges. Next $\mathscr{P}_4(\mathbf{F}_p)$ consists of at most eleven classes. A representative $I = \{i, j, l, m\}$ of a class is of the following shape;

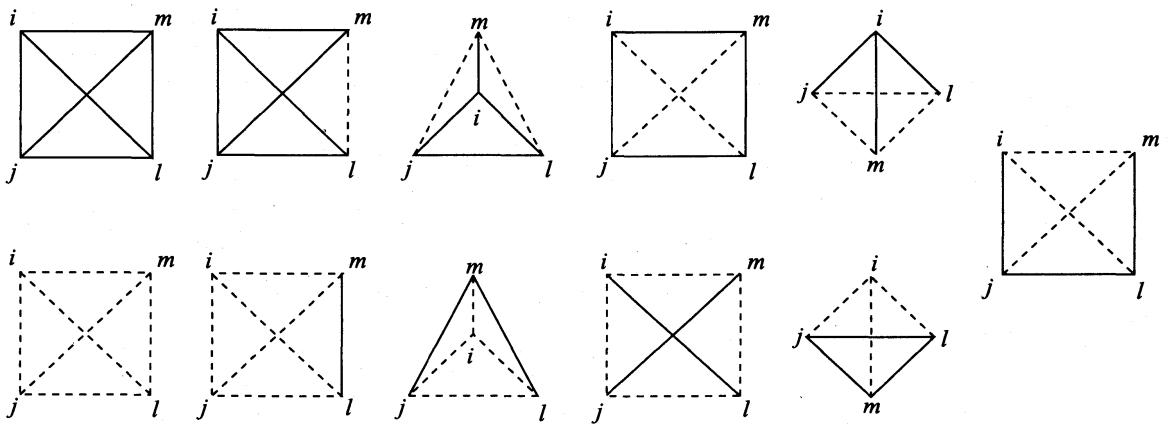

FIGURE 1

For each equivalence class $\mathscr{C}$ we write $m_{\mathscr{C}}$ for its cardinality. It is clear that

$$m_{\mathscr{C}_{2:1}}=m_{\mathscr{C}_{2:0}}=p(p-1)/4\,.$$

PROPOSITION 1.1. *For $\mathscr{P}_3(\mathbf{F}_p)$ we have the following.*

$$m_{\mathscr{C}_{3:3}}=m_{\mathscr{C}_{3:0}}=p(p-1)(p-5)/48\,,$$

$$m_{\mathscr{C}_{3:2}}=m_{\mathscr{C}_{3:1}}=p(p-1)^2/16\,.$$

The key point for the proof is the lemma below. In the lemma and arguments soon below it, we use the notation

$$(\mu_1, \mu_2)=(+, +),\ (+, -),\ (-, +) \text{ or } (-, -)\,.$$

LEMMA 1.2. *We have the following relation*

$$\#S_0^{\mu_1\mu_2}{}_1=(p-5)/4 \text{ or } (p-1)/4 \quad \textit{according as } (\mu_1, \mu_2)=(+, +) \textit{ or not.}$$

Lemma 1.2 implies Proposition 1.1. Actually an element $I=\{i, j, l\}$ of $\mathscr{C}_{3:3}$ is obtained by taking an element $\{i, j\}\in\mathscr{C}_{2:1}$ and an element $l\in S_i^{+}{}_j^{+}$. Considering the action of $\mathbf{F}_p\rtimes\mathbf{F}_p^{\times}$, we have $\#S_i^{+}{}_j^{+}=\#S_0^{+}{}_1^{+}$. The element $I\in\mathscr{C}_{3:3}$ is counted three times and we have $m_{\mathscr{C}_{3:3}}=(p(p-1)/4)((p-5)/12)$. The other case is checked similarly.

REMARK 1.3. This lemma is well known (cf. [D-M]). In order to arrange some data later, we give a short proof of it.

Fix a $(p-1)$-th primitive root ρ of unity of $\mathbf{F}_p^{\times}=\mathbf{F}_p-\{0\}$ and consider the following quadratic curves

$$C_0^{+}{}_1^{+}: x^2=y^2+1\,, \qquad C_0^{+}{}_1^{-}: x^2=\rho y^2+1\,,$$
$$C_0^{-}{}_1^{+}: \rho x^2=y^2+1\,, \qquad C_0^{-}{}_1^{-}: \rho x^2=\rho y^2+1\,.$$

We write $C'=C'^{\mu_1\mu_2}_0{}_1$ for the open part of $C=C_0^{\mu_1\mu_2}{}_1$ defined by

$$C'=C-\{(x, y)\mid xy=0\}\,.$$

Let $\mathrm{rat}(C')$ denote the set of $\mathbf{F}_p$-rational points of C'. Then considering the map $\mathrm{rat}(C')\to S_0^{\mu_1\mu_2}{}_1$ defined by

$$\mathrm{rat}(C')\ni(x, y)\mapsto\begin{cases}x^2\in S_0^{\mu_1\mu_2}{}_1 & (\mu_1=+)\\ \rho x^2\in S_0^{\mu_1\mu_2}{}_1 & (\mu_1=-)\,,\end{cases}$$

it is clear that

$$\#S_0^{\mu_1\mu_2}{}_1=\#\mathrm{rat}(C'^{\mu_1\mu_2}_0{}_1)/4\,.$$

On the other hand, we set

$$\mathbf{F}_p'=\begin{cases}\mathbf{F}_p^{\times}-\{s\mid s^4=1\} & \text{if } (\mu_1, \mu_2)=(+, +)\\ \mathbf{F}_p^{\times} & \text{otherwise}\,,\end{cases}$$

and

$$(1.3)\quad \begin{cases} x(s)=\dfrac{s^2+1}{2s} \quad y(s)=\dfrac{s^2-1}{2s} & (\mu_1,\mu_2)=(+,+) \\ x(s)=\dfrac{\rho s^2+1}{\rho s^2-1} \quad y(s)=\dfrac{2s}{\rho s^2-1} & (\mu_1,\mu_2)=(+,-) \\ x(s)=\dfrac{2(\rho^{(p-1)/4})s}{\rho s^2-1} \quad y(s)=\dfrac{\rho^{(p-1)/4}(\rho s^2+1)}{\rho s^2-1} & (\mu_1,\mu_2)=(-,+) \\ x(s)=\dfrac{s^2+\rho^{-1}}{2s} \quad y(s)=\dfrac{s^2-\rho^{-1}}{2s} & (\mu_1,\mu_2)=(-,-)\,. \end{cases}$$

Then the correspondence

$$\mathbf{F}_p' \ni s \mapsto (x(s), y(s)) \in \operatorname{rat} C'^{\mu_1\mu_2}_{0\ 1}$$

gives a bijection between $\mathbf{F}_p'$ and $\operatorname{rat} C'$. Thus we have

$$(1.4)\quad \#\operatorname{rat}(C')=\begin{cases} p-5 & \text{if } (\mu_1,\mu_2)=(+,+) \\ p-1 & \text{otherwise}, \end{cases}$$

and we have the lemma. (Note that, according to the nature of (μ_1, μ_2), the function $x(s)^2$ (or $\rho x(s)^2$ according to (μ_1, μ_2)) is invariant by the action

$$(1.5)\quad s \to (\pm s, \pm 1/s),\ (\pm s, \pm 1/\rho s),\ (\pm s, \pm 1/\rho s),\ \text{or}\ (\pm s, \pm \rho/s),$$

and $S_{0\ 1}^{\mu_1\mu_2}$ is identified with the quotient of $\mathbf{F}_p^\times$ by this action.)

Now let the set $S_{i_1\ i_2}^{\mu_1\mu_2} \cdots {}_{i_d}^{\mu_d}$ be as in (1.1). We assume that $3 \le d$ and generalize Lemma 1.2 to this set. Considering the action of $\mathbf{F}_p \rtimes \mathbf{F}_p^\times$ one can assume that the elements 0 and 1 appear in the indices $\{i_1, \cdots, i_d\}$. We rewrite it (with a slice change of presentation) as

$$S_{0\ 1\ i_1}^{\mu_1\mu_2\nu_1} \cdots {}_{i_d}^{\nu_d} \qquad (1 \le d),$$

where $i_1, \cdots, i_d$ are elements of $\mathbf{F}_p - \{0, 1\}$ and $\mu_1, \cdots, \nu_d \in \{\pm\}$.

First we consider the simplest case where the set is of the form $S_{0\ 1\ i}^{+\ +\ +}$. Let $C = C_{0\ 1\ i}^{+\ +\ +}$ denote the (affine) elliptic curve

$$u^2 = (s^2+1)^2 - 4is^2$$

and let $C' = C'^{+\ +\ +}_{0\ 1\ i}$ denote the open part of C defined by

$$C' = C - \{(s, u) \mid su = 0 \text{ or } s^4 = 1\}.$$

This curve admits an action of the form

$$(1.6)\quad (s, u) \to (\pm s, \pm u),\ (\pm 1/s, \pm u/s^2).$$

LEMMA 1.4. *We have the relation*

$$\#S_{0\ 1\ i}^{+\ +\ +} = \#\mathrm{rat}(C'^{+\ +\ +}_{0\ 1\ i})/8\,.$$

PROOF. Define a map from $\mathrm{rat}(C')$ to $S_{0\ 1}^{+\ +}$ by (cf. (1.3))

$$(s, u) \to x(s)^2 = (s^2+1)^2/4s^2\,.$$

Since $x^2 - i = u^2/4s^2$, the right-hand side is in $S_{0\ 1\ i}^{+\ +\ +}$. One checks easily that the map is surjective and unramified of degree eight. □

Now we return to the general case. Consider a $(d+1)$-dimensional affine space with coordinates (s, u), $u=(u_1, \cdots, u_d)$. Let $C_{0\ 1\ i_1 \cdots i_d}^{\mu_1\mu_2\nu_1 \cdots \nu_d} = C$ denote the algebraic curve defined by the following d equations

$$\rho^{\omega_\alpha} u_\alpha^2 = \rho^{\omega_{\mu_1}}(f'_{\mu_1\mu_2}(s))^2 - i_\alpha (f''_{\mu_1\mu_2}(s))^2 \qquad (1 \le \alpha \le d)\,,$$

where $f'_{\mu_1\mu_2}$ and $f''_{\mu_1\mu_2}$ are the numerator and the denominator of the rational function $x(s)$ in (1.3). (Thus if $(\mu_1, \mu_2)=(+, +)$, then $f'(s)=(s^2+1)$ and $f''(s)=2s$.) Moreover,

$$\omega_\alpha \text{ (resp. } \omega_{\mu_1}) = 0 \text{ or } 1 \text{ according as } \nu_\alpha \text{ (resp. } \mu_1) = + \text{ or } -\,.$$

REMARK 1.5. One sees readily that, by adding 2^d-points to C we get a complete curve of genus $1+2^d(d-1)$. (Use the Hurwitz formula.)

Denote by $C' = C'^{\mu_1\mu_2\nu_1 \cdots \nu_d}_{0\ 1\ i_1 \cdots i_d}$ the open part of C defined by

$$C' = C - \{(s, u_1, \cdots, u_d) \mid su_1 \cdots u_d = 0 \text{ or } s^4 = 1\} \qquad \text{if } (\mu_1, \mu_2) = (+, +)\,,$$

$$C' = C - \{(s, u_1, \cdots, u_d) \mid su_1 \cdots u_d = 0\} \qquad \text{if } (\mu_1, \mu_2) \neq (+, +)\,.$$

LEMMA 1.6. *We have the relation*

$$\#S_{0\ 1\ i_1 \cdots i_d}^{\mu_1\mu_2\nu_1 \cdots \nu_d} = (1/2^{(d+2)})\#C'^{\mu_1\mu_2\nu_1 \cdots \nu_d}_{0\ 1\ i_1 \cdots i_d}\,.$$

Using (1.4) this is checked similarly to Lemma 1.4.

REMARK 1.7. The quadratic residue graph was introduced to define the reflexive sheaf $\mathfrak{E}_p$ (cf. [SEK 1]). In spite of plausibility, we do not know if such a graph was used already. In connection with this we point out that a similar set was considered by Gauss for the biquadratic residue (instead of the quadratic residue) (cf. [G]).

1.2. Cocycle $K3$ surface. Now we will generalize Proposition 1.1 to $\mathscr{P}_4(\mathbf{F}_p)$. First we show the following fact, which is due to Enta. In the following we write the integer $m_{\mathscr{C}_{4:6}}$ as $m_{4:6}$. The similar abbreviation is used for the other equivalence classes.

PROPOSITION 1.8. *The following relations hold*

$$12m_{4:6} + 2m_{4:5} = p(p-1)(p-5)(p-9)/4^3\,,$$

$$2m_{4:5} + m_{4:4(a)} = p(p-1)^2(p-5)/4^3\,, \quad m_{4:4(a)} + 3m_{4:3(a)} = p(p-1)^2(p-5)/4^3\,,$$

$$2m_{4:5} + 4m_{4:4(b)} = p(p-1)^2(p-5)/4^3\,, \quad 4m_{4:4(b)} + m_{4:3(b)} = p(p-1)^3/4^3\,.$$

PROOF. The check of the first relation is as follows. Take an element $J \in \mathscr{C}_{3:3}$ and an element $L \in \mathscr{P}_2(J)$ with $L=\{l_1, l_2\}$. We write $J-L$ as $\{\alpha\}$. An element $\beta \in S_{l_1 l_2 \alpha}^{+\,+\,+}$ (resp. $\gamma \in S_{l_1 l_2 \alpha}^{+\,+\,-}$) defines an element

$$J \cup \{\beta\} \in \mathscr{C}_{4:6} \qquad (\text{resp. } J \cup \{\gamma\} \in \mathscr{C}_{4:5}) .$$

Each element of $\mathscr{C}_{4:6}$ (resp. $\mathscr{C}_{4:5}$) appears in this manner and is counted twelve times (resp. twice). Thus we have

$$12m_{4:6} + 2m_{4:5} = 3(\#\mathscr{C}_{3:3})((p-9)/4) .$$

This implies the first relation. (See also Proposition 1.1). For the other relations we start with the data

$$\{J \in \mathscr{C}_{3:2},\ L \in \mathscr{P}_2(J)\} .$$

Then one gets the relations in the proposition in a similar manner to the first one. □

We determine $m_{\mathscr{C}_{4:6}}$. Consider the five dimensional projective space $\mathbf{P}_5(\mathbf{F}_p)$ with homogeneous coordinates $z_{\alpha\beta}$ $(1 \le \alpha < \beta \le 4)$ and the following four quadratic relations in it:

$$z_{\alpha\beta}^2 + z_{\beta\gamma}^2 = z_{\alpha\gamma}^2 \qquad (1 \le \alpha < \beta < \gamma \le 4) . \tag{1.7}$$

One checks easily that each single relation is a consequence of the other three, and the locus of (1.7) is a complete intersection. We see that it has 16 ordinary singular points and the locus of (1.7) is a $K3$ surface. This surface may be called cocycle $K3$ surface and is written as $V = V_{\mathscr{C}_{4:6}}$. The singular points of V are described as follows. For each sequence $1 \le \alpha < \beta < \gamma \le 4$, we have four singular points with

$$z_{\alpha\beta} = z_{\beta\gamma} = z_{\alpha\gamma} = 0 . \tag{1.8}$$

We describe the singular points in the following manner. First note that, according to the nature of the triple (α, β, γ), there is a singular point of V, denoted by $P_{\alpha\beta\gamma}$, which is characterized by (1.8) and the following condition

$$P_{123} : (z_{14} : z_{24} : z_{34}) = (1 : 1 : 1) \qquad P_{124} : (z_{13} : z_{23} : z_{34}) = (1 : 1 : \zeta_4)$$

$$P_{134} : (z_{12} : z_{23} : z_{24}) = (\zeta_4 : 1 : 1) \qquad P_{234} : (z_{12} : z_{13} : z_{23}) = (1 : 1 : 1) .$$

Next fix a triplet (α, β, γ), and take a subset $\{\delta, \varepsilon\}$ of $\{1, 2, 3, 4\}$ which differs from $\{\alpha, \beta\}$, $\{\alpha, \gamma\}$, $\{\beta, \gamma\}$. We define a point $P_{\alpha\beta\gamma}(\delta\varepsilon)$ of V from $P_{\alpha\beta\gamma}$ by changing $z_{\delta\varepsilon}$ to $-z_{\delta\varepsilon}$ and by leaving the other coordinates of $P_{\alpha\beta\gamma}$ unchanged. (For example $P_{123}(14)$ is characterized by (1.8) and the condition $(z_{14} : z_{24} : z_{34}) = (-1 : 1 : 1)$.) Next let $V' = V'_{\mathscr{C}_{4:6}}$ denote the open part of V:

$$V' = V - \{z \mid \textstyle\prod_{1 \le \alpha < \beta \le 4} z_{\alpha\beta} = 0\} .$$

LEMMA 1.9 ([H]). *We have the relation*

$$m_{\mathscr{C}_{4:6}} = (1/64 \times 24)p(p-1)\#\mathrm{rat}(V'_{\mathscr{C}_{4:6}}) .$$

PROOF. An element I of $\mathscr{C}_{4:6}$ is formed in the following manner. First take an element $i_1 \in \mathbf{F}_p$ arbitrarily. Then find an element $z_{\alpha\beta}$ $(1 \leq \alpha < \beta \leq 4)$ in the affine cone of V. Setting

$$i_\alpha = i_1 + z_{1\alpha}^2 \qquad (\alpha = 2, 3, 4) ,$$

the element $\{i_1, i_2, i_3, i_4\}$ is in $\mathscr{C}_{4:6}$ and each element of $\mathscr{C}_{4:6}$ is formed in this manner. The above procedure yields the term $p(p-1)\#\mathrm{rat}(V')$. The term 24×64 appears by considering the action of the 4-th symmetric group and the action of $\pm$ to $z_{\alpha\beta}$. □

1.3. Kummer surface. Hitherto in this section all the varieties are defined over the prime field $\mathbf{F}_p$. In this subsection we work with a field k satisfying the condition (a) in Introduction. We consider the five dimensional projective space $\mathbf{P}_5(k)$ with homogeneous coordinates $z_{\alpha\beta}$ $(1 \leq \alpha < \beta \leq 4)$. Define a $K3$ surface, denoted also V, by the same equation (1.7). The points $P_{\alpha\beta\gamma}$ and $P_{\alpha\beta\gamma}(\delta\varepsilon)$ are defined by the same equation as in the case of $k = \mathbf{F}_p$; these 16-points exhaust all singular points of V.

In order to investigate the surface V, let $\mathbf{P}_3 = \mathbf{P}_3(k)$ be the three dimensional projective space with homogeneous coordinates $(x_0 : x_1 : x_2 : x_3)$. We consider an elliptic curve A_0 in $\mathbf{P}_3$

$$A_0 : x_2^2 = x_1^2 + x_0^2 , \quad x_3^2 = x_1^2 - x_0^2 .$$

To each element $\varepsilon = (\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3) \in (\mathbf{Z}/2\mathbf{Z})^{\oplus 4}$ we attach an element of $PGL(3, k)$

$$(x_0 : x_1 : x_2 : x_3) \to (\varepsilon_0 x_0 : \varepsilon_1 x_1 : \varepsilon_2 x_2 : \varepsilon_3 x_3) .$$

This defines a homomorphism from $(\mathbf{Z}/2\mathbf{Z})^{\oplus 4}$ to $PGL(3, k)$. We write the image as G'_8 $(\simeq (\mathbf{Z}/2\mathbf{Z})^{\oplus 3})$. We use the notation $\varepsilon = (\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ for the corresponding element of G'_8. This group acts on A_0. An element ε acts freely on A_0 if and only if

$$\varepsilon_0\varepsilon_1\varepsilon_2\varepsilon_3 = 1 . \tag{1.9}$$

Such an element is the identity or an element satisfying the condition: i-th and j-th components of it $= -1$ and the other components $= 1$. We write this element as $\varepsilon(i, j)$. Moreover, for each $i \in \{0, 1, 2, 3\}$, let $\varepsilon(i)$ denote the element characterized by $\varepsilon_i = -1$ and $\varepsilon_j = 1$ $(i \neq j)$ $(0 \leq i \leq 3)$. It has four fixed points characterized by $x_i = 0$. (If $i = 2$ or 3, then the fixed point is defined over $k(\sqrt{2})$.) We write the set of these four fixed points as $\mathscr{Q}_i$.

$$\mathscr{Q}_0 = \{(0 : 1 : \pm 1 : \pm 1)\} , \qquad \mathscr{Q}_1 = \{(1 : 0 : \pm 1, \pm\zeta_4)\} ,$$

$$\mathscr{Q}_2 = \{(1 : \pm\zeta_4 : 0 : \pm\sqrt{2}\zeta_4)\} , \qquad \mathscr{Q}_3 = \{(1 : \pm 1 : \pm\sqrt{2}\zeta_4 : 0)\} .$$

For later convenience we set

$$Q_0=(0:1:1:1)\,,\qquad Q_1=(1:0:1:\zeta_4)\,,$$
$$Q_2=(1:\zeta_4:0:\sqrt{2}\zeta_4)\,,\qquad Q_3=(1:1:\sqrt{2}\zeta_4:0)\,.$$

Consider the subgroup of G_8' consisting of those elements ε satisfying

$$\varepsilon_0\varepsilon_1=\varepsilon_2\varepsilon_3=1\,. \tag{1.10}$$

This is isomorphic to $\mathbf{Z}/2\mathbf{Z}$. The quotient of A_0 by this group is the elliptic curve

$$A_1 : t^2=s^4-1$$

where the morphism $A_0\to A_1$ is given by $s=x_1'$ and $t=x_2'x_3'$ with $x_i'=x_i/x_0$ $(i=1, 2, 3)$. (Precisely A_1 is the complete curve obtained from the above affine curve by adding two points (cf. [Sh 2]).)

$$\begin{array}{ccc} A_0 & \xrightarrow{G_8'} & A_0 \\ \downarrow & & \downarrow \\ A_1 & \longrightarrow & A_1 \end{array}$$

The group G_8' induces a group action in the second line, which is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$:

$$(s, t)\to(\pm s, \pm t)\,. \tag{1.11}$$

We write an element of this group by $(\varepsilon, \varepsilon')$ where

$$\varepsilon=(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3) \qquad \text{and} \qquad \varepsilon'=(\varepsilon_0', \varepsilon_1', \varepsilon_2', \varepsilon_3')\,.$$

Form a series of subgroups of $G_{64}=G_8'\oplus G_8'$ $(\simeq(\mathbf{Z}/2\mathbf{Z})^{\oplus 6})$

$$G_4\subset G_8\subset G_{16}$$

in the following manner

$$G_{16}=\{(\varepsilon, \varepsilon')\mid \varepsilon_0\varepsilon_1=\varepsilon_0'\varepsilon_1',\ \varepsilon_2\varepsilon_3=\varepsilon_2'\varepsilon_3'\}\,,$$
$$G_8=\{(\varepsilon, \varepsilon')\mid \varepsilon_0\varepsilon_1=\varepsilon_0'\varepsilon_1'=\varepsilon_2\varepsilon_3=\varepsilon_2'\varepsilon_3'\}\,,$$
$$G_4=\{(\varepsilon, \varepsilon')\mid \varepsilon_0\varepsilon_1=\varepsilon_0'\varepsilon_1'=\varepsilon_2\varepsilon_3=\varepsilon_2'\varepsilon_3'=1\}\,.$$

More explicitly these groups are as follows:

$$G_4=\{id\times id,\ id\times\varepsilon(2, 3),\ \varepsilon(2, 3)\times id,\ \varepsilon(2, 3)\times\varepsilon(2, 3)\}\,,$$
$$G_8-G_4=\{\varepsilon(1, 2)\times\varepsilon(1, 2),\ \varepsilon(1, 2)\times\varepsilon(1, 3),\ \varepsilon(1, 3)\times\varepsilon(1, 2),\ \varepsilon(1, 3)\times\varepsilon(1, 3)\}\,,$$
$$G_{16}-G_8=\{\varepsilon(i)\times\varepsilon(j)\mid \{i, j\}=\{0, 1\}\ \text{or}\ \{2, 3\}\}\,.$$

These groups act on $A_0\times A_0$. By (1.9) the group G_8 acts freely on it. Each element $\varepsilon(i)\times\varepsilon(j)\in G_{16}-G_8$ has sixteen fixed points $\mathcal{Q}_i\times\mathcal{Q}_j$. This set is stable by the action of

G_8 and consists of two orbits. We write these by R_{ij} and R'_{ij} so that R_{ij} contains the point $Q_i \times Q_j$. Next the action of G_4 is isomorphic to $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$, where the group $(\mathbf{Z}/2\mathbf{Z})$ is the one defined by (1.11). Thus $A_1 \times A_1 \simeq (A_0 \times A_0)/G_4$. The action of G_{16}/G_4 on $A_1 \times A_1$ is of the form

$$\begin{aligned}(s, t) \times (s, t') \rightarrow \quad & (s, t) \times (s', t'), \qquad (-s, t) \times (-s', t'), \\ & (s, -t) \times (s', -t'), \quad (-s, -t) \times (-s', -t').\end{aligned}$$

The last element acts freely on $A_1 \times A_1$. This is the translation $T_{(v,v)}$ in [Sh 3] and the quotient $(A_1 \times A_1)/T_{(v,v)}$ is an abelian surface denoted A. Thus we have the isomorphism

$$(A_0 \times A_0)/G_8 \simeq (A_1 \times A_1)/T_{(v,v)} = A .$$

The generator of G_{16}/G_8 is nothing else than the involution ι_A of A in [Sh 3] and, therefore, $A/(G_{16}/G_8)$ is the Kummer surface $Km(A)$ whose non-singular model is the surface $S(4)$; see the following diagram

$$\begin{array}{lccc} & A_0 \times A_0 & & \\ & \downarrow & & \\ A_0 \times A_0/G_4 \cong & A_1 \times A_1 & \cdots & G_4 \\ & \downarrow & & \cap \\ A_0 \times A_0/G_8 \cong & A & \cdots & G_8 \\ & \downarrow & & \cap \\ A_0 \times A_0/G_{16} \cong & Km(A) & \cdots & G_{16} . \end{array}$$

Now we prove the following

LEMMA 1.10. *The surface V is isomorphic to $(A_0 \times A_0)/G_{16}$ and so is isomorphic to the Kummer surface $Km(A)$.*

PROOF. We form a morphism from $A_0 \times A_0$ to V. Let us consider another three dimensional projective space $\mathbf{P}_3(k)$ with homogeneous coordinates $(y_0 : y_1 : y_2 : y_3)$. We think of the second factor A_0 of the product $A_0 \times A_0$ as the elliptic curve in this projective space:

$$y_2^2 = y_1^2 - y_0^2 , \qquad y_3^2 = y_1^2 - y_0^2 .$$

A morphism from $A_0 \times A_0$ to V is defined as follows

$$\begin{aligned} & z_{12} = x_2 x_3 y_2 y_3 , \quad z_{13} = x_1^2 y_1^2 - x_0^2 y_0^2 , \quad z_{14} = x_1^2 y_1^2 + x_0^2 y_0^2 , \\ & z_{23} = x_0^2 y_1^2 - y_0^2 x_1^2 , \quad z_{24} = x_0^2 y_1^2 + y_0^2 x_1^2 , \quad z_{34} = 2 x_0 x_1 y_0 y_1 . \end{aligned}$$

Noting that the polynomials in this expression are linear combinations of the monomials

$$x_0 x_1 y_0 y_1 , \quad x_2 x_3 y_2 y_3 , \quad x_0^2 y_0^2 , \quad x_1^2 y_1^2 , \quad x_0^2 y_1^2 , \quad x_1^2 y_0^2 ,$$

we see that, for two points on $A_0 \times A_0$, they are mapped to the same point on V if and

only if they are equivalent under the action of G_{16}. □

REMARK 1.11. The fixed points on $A_0 \times A_0$ by the action of G_{16} is mapped to the singular points of V as follows

$$\begin{aligned} &Q_i \times Q_i \to z_{23}=z_{24}=z_{34}=0 && (i=0, 1), \\ &Q_i \times Q_j \to z_{13}=z_{14}=z_{34}=0 && ((i,j)=(0, 1), (1, 0)), \\ &Q_i \times Q_i \to z_{12}=z_{13}=z_{23}=0 && (i=2, 3), \\ &Q_i \times Q_j \to z_{12}=z_{14}=z_{24}=0 && ((i,j)=(2, 3), (3, 2)). \end{aligned}$$

1.4. An additional lemma. Here we again assume that $k=\mathbf{F}_p$, p being a prime $\equiv 1 \pmod 4$; the surfaces V and V' are as in §1.2. We conclude this section by the following fact which is used in §3.

LEMMA 1.12. *We have the following relation*

$$\#\mathrm{rat}(V')=\#\mathrm{rat}(V)-24p+80.$$

PROOF. Set $Z=\bigcup_{1\le\alpha<\beta\le 4} Z(z_{\alpha\beta})$. Clearly the relation just above is equivalent to the one:

$$\#\mathrm{rat}(Z)=24p-80. \tag{1.12}$$

To see this, let (α, β) denote (1, 2), (1, 3) or (1, 4) and denote by $\mathscr{W}_{\alpha\beta}$ the set of eight (smooth) points of V characterized by the condition

$$z_{\alpha\beta}=z_{\gamma\delta}=0$$

where $\{\gamma, \delta\}=\{1, 2, 3, 4\}-\{\alpha, \beta\}$. We set $\mathscr{W}=\mathscr{W}_{12}\cup\mathscr{W}_{13}\cup\mathscr{W}_{14}$. For the proof of (1.12) it suffices to see the following:

(i) Each $Z(z_{\alpha\beta})$ consists of four smooth rational curves, which are defined over k.
(ii) For each singular point of V, there are exactly six irreducible components of Z passing through it.
(iii) For each point of $\mathscr{W}$, there are exactly two irreducible components of Z passing through the point.
(iv) Take two distinct irreducible components of Z. Then the common points of them are contained in $\mathrm{Sing}(V)\cup\mathscr{W}$.

Actually (1.11) follows from (i)–(iv) once we note that the number of the $\mathbf{F}_p$-rational point of each component of Z equals $(p+1)$. The check of (i)–(iv) is as follows. First we see that $Z(z_{34})$ consists of four smooth rational curves

$$z_{34}=0, \quad z_{13}=\pm z_{14}, \quad z_{23}=\pm z_{24}, \quad z_{12}^2+z_{23}^2=z_{13}^2. \tag{1.13}$$

Remarking that each element of the 4-th permutation group π_4 acts on V through the action on the indices $(\alpha\beta)$, (1.13) leads immediately to (i). Denote by $Z_{\mu_1\mu_2}$ the rational curve in (1.13) characterized by $z_{13}=\mu_1 z_{14}$, $z_{23}=\mu_2 z_{24}$, where $\mu_1, \mu_2 = +$ or $-$. We

see readily that

$$\text{(v)} \quad \begin{cases} Z_{++} \cap Z_{+-} = \{P_{234}, P_{234}(12)\}, & Z_{++} \cap Z_{-+} = \{P_{134}, P_{134}(12)\}, \\ Z_{++} \cap Z_{--} = Z_{+-} \cap Z_{-+} = \varnothing, & Z_{+-} \cap Z_{--} = \{P_{134}(23), P_{134}(24)\}, \\ Z_{-+} \cap Z_{--} = \{P_{234}(13), P_{234}(14)\}. \end{cases}$$

This implies that the set of points on V which appear in the intersection of distinct components of $Z(z_{34})$ coincides with the set of 8 singular points characterized by

$$z_{23}=z_{24}=z_{34}=0 \quad \text{or} \quad z_{13}=z_{14}=z_{34}=0.$$

Next, for the singular point P_{234}, we see readily that the following six curves exhaust all irreducible components of Z passing through it:

$$\begin{cases} z_{34}=0, & z_{13}=z_{14}, & z_{23}=\pm z_{24}, \\ z_{24}=0, & z_{12}=z_{14}, & z_{23}=\pm z_{34}, \\ z_{23}=0, & z_{12}=z_{13}, & z_{24}=\pm z_{34}. \end{cases}$$

Similarly to the above this leads to (ii). Take different pairs $\{\alpha, \beta\}$ and $\{\gamma, \delta\}$ of $\{1, 2, 3, 4\}$. We see that if these pairs have a common element, say γ, then

$$\text{(vi)} \qquad Z_{\alpha\beta} \cap Z_{\gamma\delta} \subset \{z \mid z_{\alpha\beta}=z_{\alpha\gamma}=z_{\beta\gamma}=0\} \subset \mathrm{Sing}(V).$$

Assume that they do not have a common point and that $\{\alpha, \beta\}=\{1, 2\}$. Then $\mathcal{W}_{12}$ consists of eight points

$$(z_{12} : z_{13} : z_{14} : z_{23} : z_{24} : z_{34}) = (0 : \pm 1 : \pm 1 : \pm 1 : \pm 1 : 0)$$

and, for each point of $\mathcal{W}_{12}$, we see that (cf. (1.12))

(vii) there is exactly one irreducible component of $Z(z_{12})$ (resp. $Z(z_{34})$) passing through it.

It is easy to see that (v)–(vii) implies (iii) and (iv), and we have the lemma. □

2. Shioda modular surface of level 4 and cocycle $K3$ surface.

In this section, we investigate the relation between the Shioda modular surface of level 4 and cocycle $K3$ surface.

2.1. Shioda modular surface of level 4. Here we recall some facts on the surface $S(4)$ from [Sh 1], [Sh 2] and [Sh 3]. As before k denotes a field satisfying (a) in Introduction. We denote by $\mathbf{P}_n$ the k-projective space of dimension n. Let E be an elliptic curve and E_4 the group of the points of order 4 of E. Let a_4, b_4 be an ordered basis of E_4 with $e_4(a_4, b_4)=\zeta_4$, where e_4 is the Weil pairing. The triple (E, a_4, b_4) is called an elliptic curve *with level* 4 *structure*. Then there exists a unique pair (x, y) of rational functions on E, defined over k, giving an isomorphism from E onto the non-singular cubic curve

$$y^2 = x(x-1)\left(x - \frac{1}{4}\left(s_1 + \frac{1}{s_1}\right)^2\right), \tag{2.1}$$

where the level 4 structure invariant $s_1 = x(a_4) + \zeta_4(x(b_4)+1)$ of E is an element of $\Delta = \mathbf{P}_1 - \{0, \pm 1, \pm\zeta_4, \infty\}$. (Precisely the cubic curve is the compactification of (2.1) in $\mathbf{P}_2$:

$$ZY^2 = X(X-Z)\left(X - \frac{Z}{4}\left(s_1 + \frac{1}{s_1}\right)^2\right),$$

where $(X : Y : Z)$ are homogeneous coordinates of $\mathbf{P}_2$.) We write $S(4)'$ for the corresponding elliptic surface to (2.1). Let Ψ' denote the restriction of the projection $\mathbf{P}_2 \times \Delta \to \Delta$ to $S(4)'$. Then the fibre system $\Psi' : S(4)' \to \Delta$ is the universal family of elliptic curves with level 4 structure and the Shioda modular surface $S(4)$ is a suitable compactification of $S(4)'$ (cf. [Sh 2]). The surface $S(4)$ has the natural projection $\tilde{\Psi} : S(4) \to \mathbf{P}_1$ which is an extension of Ψ'. At each point $s_1 \in \mathbf{P}_1 - \Delta$, the singular fibre $\tilde{\Psi}^{-1}(s_1)$ is of type I_4 in the notation of Kodaira (cf. [K]).

In [Sh 3] another birational model of $S(4)$ was given by using the Jacobi quartic:

$$u_{11}^2 = (t_1^2 - s_1^2)(1 - s_1^2 t_1^2)\,. \tag{2.2}$$

This admits a graph theoretical interpretation. Assume that $k = \mathbf{F}_p$, p being a prime $\equiv 1$ (mod 4). Take an element $I \in \mathscr{C}_{4:6}$ (cf. §1.1). Considering the action of $\mathbf{F}_p \rtimes \mathbf{F}_p^\times$ one can assume that I is of the form $\{0, 1, i, j\}$. Since i and j are in $S_0^+{}_1^+$ one can write

$$i = (s_1^2+1)^2/4s_1^2\,, \qquad j = (t_1^2+1)^2/4t_1^2$$

with elements $s_1, t_1 \in \mathbf{F}_p^\times - \{\zeta_4^\alpha \mid \alpha = 0, 1, 2, 3\}$. The relation $i - j \in S_0^+$ leads to the relation

$$u_{11}^2 = t_1^2(s_1^2+1)^2 - s_1^2(t_1^2+1)^2\,,$$

with an element u_{11} of $\mathbf{F}_0^\times$. This coincides with (2.2).

Now we return to the general case where the field k is as in the beginning of this section. We consider an affine surface, defined over k, which is defined by the same equation (2.2). We compactify this surface in the following manner. Form a product $\mathbf{P} = \mathbf{P}_1 \times \mathbf{P}_1$. For notational reason we write M and N, respectively, for the first and the second factor of the product and write homogeneous coordinates of M and N by $[\mathscr{S}_0 : \mathscr{S}_1]$ and $[\mathscr{T}_0 : \mathscr{T}_1]$, respectively. Define a section $v \in H^0(\mathbf{P}, \mathscr{O}_{\mathbf{P}}(2, 2)^{\otimes 2})$ by

$$v = (\mathscr{S}_1^2\mathscr{T}_0^2 - \mathscr{S}_0^2\mathscr{T}_1^2)(\mathscr{S}_1^2\mathscr{T}_1^2 - \mathscr{S}_0^2\mathscr{T}_0^2)$$

and denote by B the zero locus of v. Let L be the total space of $\mathscr{O}_{\mathbf{P}}(2, 2)$ and $\mathfrak{p} : L \to \mathbf{P}$ the bundle projection. For the tautological section

$$u \in H^0(L, \mathfrak{p}^*\mathscr{O}_{\mathbf{P}}(2, 2))$$

we can define a 2-cyclic covering S of $\mathbf{P}$, branched along B, to be the zero locus of

$\mathfrak{p}^*v-u^2$ (cf. [B-P-V]). In fact, we denote by U_i, V_j open sets of M, N determined by the conditions $\mathscr{S}_i\neq 0$, $\mathscr{T}_j\neq 0$ $(i,j=0,1)$. Then the subvariety S of L is defined in $\mathfrak{p}^{-1}(U_i\times V_j)$ $(i,j=0,1)$ to be the zero locus of the rational function

$$u_{ij}^2-(t_j^2-s_i^2)(1-s_i^2t_j^2)$$

on L, where

$$s_1=\mathscr{S}_0/\mathscr{S}_1\,,\quad s_0=\mathscr{S}_1/\mathscr{S}_0\,,\quad t_1=\mathscr{T}_0/\mathscr{T}_1\,,\quad t_0=\mathscr{T}_1/\mathscr{T}_0\,,\quad u_{ij}=u\mathscr{S}_i^{-2}\mathscr{T}_j^{-2}\,.$$

The composition of the projection from $\mathbf{P}$ to M (resp. N), composed with $\mathfrak{p}$, defines a projection L onto M (resp. N). We denote by Ψ_M (resp. Ψ_N) the restriction to S.

PROPOSITION 2.1. *Let Δ_M denote $M-\{0,\pm 1,\pm\zeta_4,\infty\}$. Then $S'_M=\Psi_M^{-1}(\Delta_M)$ is the universal family of elliptic curves with level 4 structure.*

PROOF. Let (E,a,b) be the elliptic curve with level 4 structure defined by the equation (2.1). For an arbitrary element s_1 of Δ_M, there is a unique pair (t_1,u_{11}) of rational functions on E defined over k, which is characterized by

$$x=\frac{(s_1^2+1)(t_1-s_1)}{2s_1(s_1t_1-1)}\,,\qquad y=\frac{\zeta_4(s_1^4-1)u_{11}}{4s_1^2(s_1t_1-1)^2}\,. \tag{2.3}$$

The pair (t_1,u_{11}) satisfies (2.2) and gives the isomorphism onto the subvariety of the total space of $\mathscr{O}_N(2)$ defined by (2.2). Therefore we get this proposition. □

In this connection we remark that, by [Sh 2], the ordered basis (a_4,b_4) of E_4 is expressed in terms of (2.1) by

$$\begin{cases} a_4=\left(\dfrac{s_1^2+1}{2s_1},\dfrac{\zeta_4(s_1^2+1)(s_1-1)^2}{4s_1^2}\right)\\ b_4=\left(\dfrac{(s_1+\zeta_4)^2}{2\zeta_4 s_1},\dfrac{\varepsilon(s_1^2-1)(s_1+\zeta_4^2)}{4s_1^2}\right)\end{cases}$$

where the sign $\varepsilon=\pm 1$ is determined by $e_4(a_4,b_4)=\zeta_4$. Moreover, in terms of (2.2), it is written as

$$\begin{cases} a_4=(-1,s_1^2-1)\\ b_4=(-\zeta_4,\varepsilon\zeta_4(s_1^2+1))\,.\end{cases}$$

REMARK 2.2. The similar fact to Proposition 2.1 holds for $S'_N=\Psi_N^{-1}(\Delta_N)$.

Now the existence of the two projections Ψ_M and Ψ_N leads to a configuration of 12-curves; see Figure 2. Each curve $\Psi_M^{-1}(s_1)$ (resp. $\Psi_N^{-1}(t_1)$) consists of two rational curves, where s_1, $t_1=0,\pm 1,\pm\zeta_4$ or ∞. We write them by $C_{s_1,m}$(resp. $C_{t_1,m}$) $(m=1,2)$. Define 12-points $P_{s_1t_1}$ by the condition

$$P_{s_1t_1}\Psi_M^{-1}(s_1)\cap\Psi_N^{-1}(t_1)$$

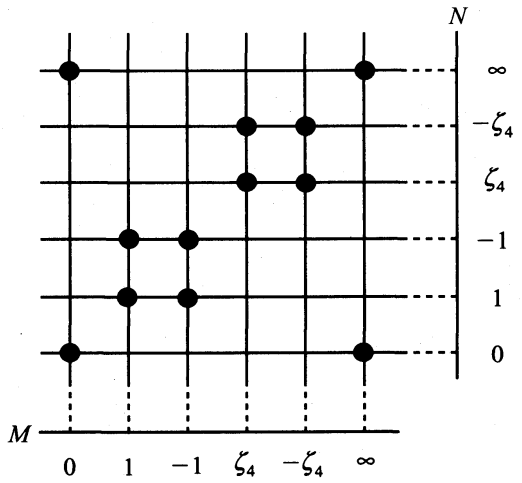

FIGURE 2

where $\{s_1, t_1\}$ is one of the following three sets

$$\{s_1, t_1\} = \{0, \infty\}, \ \{\pm 1\} \text{ or } \{\pm\zeta_4\}.$$

We see that these twelve points exhaust all singular points of S and each of them is an ordinary double point. Denote by $\pi : \tilde{S} \to S$ the resolution which is the blow-up of S at the twelve points. We write $\tilde{\Psi}_M : \tilde{S} \to M$ for $\Psi_M \circ \pi$ and $\Theta_{s_1t_1}$ for the exceptional curve on $\tilde{S}$ which is contracted to $P_{s_1t_1}$ by π. Moreover we write $\Theta_{s_1,m}$ and $\Theta_{t_1,m}$ $(m = 1, 2)$, respectively, for the proper transform of $C_{s_1,m}$ and $C_{t_1,m}$. Then, for each point s_1 as above, the singular fiber $\tilde{\Psi}_M^{-1}(s_1)$ consists of four rational curves $\Theta_{s_1t_1}$ and $\Theta_{s_1,m}$, respectively, which are defined as above.

PROPOSITION 2.3. *The elliptic surface $\tilde{\Psi}_M : \tilde{S} \to M$ is isomorphic to the Shioda modular surface $S(4) \to M$. (The similar fact holds for the projection $\tilde{\Psi}_N$.)*

PROOF. By Proposition 2.1, $S(4)$ is a suitable compactification of S'_M. Therefore, by the uniqueness of a relatively minimal model, it is sufficient to check that each singular fibre $\tilde{\Psi}_M^{-1}(s_1)$ $(s_1 = 0, \pm 1, \pm\zeta_4, \infty)$ of $\tilde{S}$ is of type I_4. In order to prove this fact we first check the following at each s_1,

(b) each component of $\tilde{\Psi}_M^{-1}$ is smooth and 4 components intersect like "#".

Also we construct a global section of $\tilde{S}$ over M to see that each singular fibre is not a multiple fibre. This means that each singular fiber is of type I_4.

We prepare some notations. Let $\Sigma_{s_1t_1}$ be a neighborhood of $P_{s_1t_1}$ and $\tilde{\Sigma}_{s_1t_1} \to \Sigma_{s_1t_1}$ a blowing-up of $\Sigma_{s_1t_1}$. To see (b), we first blow up the singular point P_{00} and $P_{0\infty}$ lying on $\Psi_M^{-1}(0)$. (The coordinates of them are $(u_{11}, t_1, s_1) = (0, 0, 0)$ and $(u_{10}, t_0, s_1) = (0, 0, 0)$.) Then $\tilde{\Sigma}_{00}$ is the subvariety of $\Sigma_{00} \times \mathbf{P}_2$ defined by

$$\text{(2.4)} \qquad \begin{cases} u_{11}X_1 = t_1X_0 \\ u_{11}X_2 = s_1X_0 \\ t_1X_2 = s_1X_1\,, \end{cases}$$

where $(X_0 : X_1 : X_2)$ are homogeneous coordinates of $\mathbf{P}_2$. The blowing-up at $P_{0\infty}$ is obtained similarly by considering the transformation:

$$X_0' = X_0/t_1^2\,, \quad X_1' = X_1/t_1^2\,, \quad X_2' = X_2\,.$$

The curves $\Theta_{s_1,m}$ $(s_1 = 0,\ m = 1, 2)$ are given by

$$\text{(2.5)} \qquad X_2 = 0\,, \qquad X_0 + X_1 = 0\,;$$

$$\text{(2.6)} \qquad X_2 = 0\,, \qquad X_1 - X_0 = 0$$

on $\tilde{\Sigma}_{00}$, while Θ_{00}, $\Theta_{0\infty}$ are given by

$$(u_{11}, t_1, s_1) = (0, 0, 0)\,, \qquad X_0^2 + X_2^2 = X_1^2\,;$$

$$(u_{10}, t_0, s_1) = (0, 0, 0)\,, \qquad X_0'^2 + X_2'^2 = X_1'^2\,.$$

From the shape of the above curves it is clear that $\Psi_M^{-1}(0)$ satisfies the condition (b). Secondly we blow up the singular points P_{11}, P_{1-1} lying on $\Psi_M^{-1}(1)$. The coordinates of P_{11} are $(u_{11}, t_1, s_1) = (0, 1, 1)$. Then $\tilde{\Sigma}_{11}$ is the subvariety of $\Sigma_{11} \times \mathbf{P}_2$ defined by

$$\text{(2.7)} \qquad \begin{cases} u_{11}Y_1 = (t_1 - 1)Y_0 \\ u_{11}Y_2 = (s_1 - 1)Y_0 \\ (t_1 - 1)Y_2 = (s_1 - 1)Y_1\,, \end{cases}$$

where $(Y_0 : Y_1 : Y_2)$ are homogeneous coordinates in $\mathbf{P}_2$. If we replace $(t_1 - 1)$ by $(t_1 + 1)$ and set

$$Y_0' = Y_0\,, \quad Y_1' = (t_1 + 1)Y_1/(t_1 - 1)\,, \quad Y_2' = Y_2\,,$$

then we get the blowing-up of P_{1-1}. The curves Θ_{11}, Θ_{1-1} are given by

$$\text{(2.8)} \qquad (u_{11}, t_1, s_1) = (0, 1, 1)\,, \qquad Y_0^2 + 4Y_1^2 = 4Y_2^2\,;$$

$$\text{(2.9)} \qquad (u_{11}, t_1, s_1) = (0, -1, 1)\,, \qquad Y_0'^2 + 4Y_1'^2 = 4Y_2'^2\,,$$

while the curves $\Theta_{s_1,m}$ $(s_1 = 1,\ m = 1, 2)$ are given by

$$Y_2 = 0\,, \qquad \mathscr{T}_1 Y_0 = -\zeta_4(\mathscr{T}_0 + \mathscr{T}_1)T_1\,;$$

$$Y_2 = 0\,, \qquad \mathscr{T}_1 Y_0 = \zeta_4(\mathscr{T}_0 + \mathscr{T}_1)Y_1\,.$$

Thus the condition (b) is also clear for the singular fiber at $s_1 = 1$. The condition (b) is checked for the other singular fiber similarly to the above argument (or by reducing to the above argument by considering the suitable group action on S.)

Finally, we construct a global section of $\tilde{S}$ over M. Let o be the divisor of S defined

by $\mathscr{S}_0\mathscr{T}_0=\mathscr{S}_1\mathscr{T}_1$. Then $o'=o_{|S'}$ is the unit of the group of global sections of S'. Then the proper transform $\tilde{o}$ of o is defined as the zero locus of the following equation

$$\begin{cases} \mathscr{S}_0\mathscr{T}_0=\mathscr{S}_1\mathscr{T}_1\,, & X_1'=X_2' & \text{in } \tilde{\Sigma}_{0\infty} \\ \mathscr{S}_0\mathscr{T}_0=\mathscr{S}_1\mathscr{T}_1\,, & Y_1-Y_2=2 & \text{in } \tilde{\Sigma}_{11}\,, \end{cases}$$

in $\tilde{S}$ and $\tilde{o}$ is extended to the singular fibres at $s_1=0, 1$. In the same way, $\tilde{o}$ can be extended over $s_1=-1, \pm\zeta_4, \infty$. This completes the proof. □

By Proposition 2.3 we identify the surface $S(4)$ with $\tilde{S}$.

2.2. Contraction of $S(4)$ to V. In §1.2 and §2.1 we saw that V and $S(4)$ parametrize the equivalence class $\mathscr{C}_{4:6}$ when the field k in question is the prime field $\mathbf{F}_p$. A comparison of these two parameterization leads to a rational map from S to V (cf. (1.3))

$$z_{13}/z_{34}=(s_1^2-1)/2s_1\,, \qquad z_{14}/z_{34}=(s_1^2+1)/2s_1\,,$$

$$z_{23}/z_{34}=(t_1^2-1)/2t_1\,, \quad z_{24}=(t_1^2+1)/2t_1 \quad \text{and} \quad z_{12}=u_{11}/2s_1t_1$$

and we give the relation of these two parametrization by the following figure;

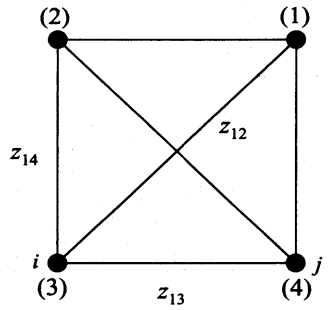

FIGURE 3

Now we return to a general field k satisfying the condition (a) in Introduction. Using six sections of $\mathfrak{p}_{|S}^*\mathscr{O}_{\mathbf{p}}(2, 2)$

$$\text{(2.10)} \qquad \begin{cases} l_0=u/2\,, \\ l_1=(\mathscr{S}_1^2-\mathscr{S}_0^2)\mathscr{T}_0\mathscr{T}_1/2\,, \qquad l_2=(\mathscr{S}_0^2+\mathscr{S}_1^2)\mathscr{T}_0\mathscr{T}_1/2\,, \\ l_3=(\mathscr{T}_1^2-\mathscr{T}_0^2)\mathscr{S}_0\mathscr{S}_1/2\,, \quad l_4=(\mathscr{T}_0^2+\mathscr{T}_1^2)\mathscr{S}_0\mathscr{S}_1/2\,, \\ l_5=\mathscr{S}_0\mathscr{S}_1\mathscr{T}_0\mathscr{T}_1\,, \end{cases}$$

we form a rational map Φ from S to V as follows

$$(z_{12}:z_{13}:z_{14}:z_{23}:z_{24}:z_{34})=(l_0:l_1:l_2:l_3:l_4:l_5)\,.$$

PROPOSITION 2.4. *The rational map Φ is regular on $S-\{P_{00}, P_{0\infty}, P_{\infty 0}, P_{\infty\infty}\}$. Moreover, it gives a biregular map between $S-Z(\mathscr{S}_0\mathscr{S}_1\mathscr{T}_0\mathscr{T}_1)$ and $V-Z(z_{34})$.*

PROOF. The inverse of such a rational map is given by

$$s_1=\frac{z_{14}-z_{13}}{z_{34}}, \qquad t_1=\frac{z_{24}-z_{23}}{z_{34}}, \quad u_{11}=\frac{2s_1t_1z_{12}}{z_{34}}.$$

This ensures the second assertion. The first one is clear from (2.10). □

To construct the birational morphism from $S(4)$ to V, we prepare some notation. Let $r_{a_4,\varepsilon b_4}$, $r_{-a_4,-\varepsilon b_4}$, $r_{a_4,-\varepsilon b_4}$, $r_{-a_4,\varepsilon b_4}$ ($\varepsilon=\pm 1$ is determined by $e_4(a_4, b_4)=\zeta_4$) be divisors of S defined locally by

$$\text{(2.11)} \qquad \begin{cases} t_1=0, & u_{11}-\zeta_4 s_1=0; \\ t_1=0, & u_{11}+\zeta_4 s_1=0; \\ t_0=0, & u_{10}-\zeta_4 s_1=0; \\ t_0=0, & u_{10}+\zeta_4 s_1=0, \end{cases}$$

and let $\tilde{r}_{a_4,\varepsilon b_4}$, $\tilde{r}_{-a_4,-\varepsilon b_4}$, $\tilde{r}_{a_4,-\varepsilon b_4}$, $\tilde{r}_{-a_4,\varepsilon b_4}$ be the proper transform of them. From [Sh 2], we know that divisors of $S(4)'$ defined by

$$(x, y)=\left(\frac{s_1^2+1}{2}, \frac{s_1^4-1}{4s_1}\right), \quad \left(\frac{s_1^2+1}{2}, -\frac{s_1^4-1}{4s_1}\right),$$
$$\left(\frac{s_1^2+1}{2s_1^2}, \frac{s_1^4-1}{4s_1^3}\right), \quad \left(\frac{s_1^2+1}{2s_1^2}, \frac{-(s_1^4-1)}{4s_1^3}\right)$$

are corresponding to elements of the group of global sections of $S(4)'$ of order 4 which are generated by $a_4+\varepsilon b_4$, $-a_4-\varepsilon b_4$, $a_4-\varepsilon b_4$, $-a_4+\varepsilon b_4$, where $\varepsilon=\pm 1$ is determined by $e_4(a_4, b_4)=\zeta_4$. Note that the divisors determined by such sections are mapped by (2.3) to the ones defined by (2.11) and, therefore the proper transforms of them are corresponding to the global sections of $S(4) \to M$. Putting

$$D=\sum_{(\rho,\sigma)=(\pm a_4, \pm b_4)} \tilde{r}_{\rho,\sigma}+\sum_{s_1=0,\infty}\sum_{t_1=0,\infty}(\tilde{\Psi}_M^{-1}(s_1)-\Theta_{s_1t_1}),$$

we consider the invertible sheaf $\mathcal{O}_{S(4)}(D)$. It has six sections $\tilde{l}_k$ ($k=0, 1, 2, 3, 4, 5$) which are the proper transform of l_k and we denote by $\mathcal{L}$ the sublinear system of $|\mathcal{O}_{S(4)}(D)|$ spanned by such six sections. Then $\mathcal{L}$ defines the birational map $\Phi_{\mathcal{L}}$ from $S(4)$ onto V. In view of the structure of the fibre system $\tilde{\Psi}_M : S(4) \to M$, we give the main result of this section as follows.

THEOREM 2.5. *The birational map $\Phi_{\mathcal{L}} : S(4) \to V$ is the contraction which sends the* 16 *rational curves of* $S(4)$

$$\begin{cases} \Theta_{s_1,m} & (s_1=0, \infty, m=1, 2) \\ \Theta_{s_1t_1} & ((s_1, t_1)=(\pm 1, \pm 1), (\pm\zeta_4, \pm\zeta_4)) \\ \tilde{r}_{\rho,\sigma} & ((\rho, \sigma)=(\pm a, \pm b)) \end{cases}$$

to the 16 *singular points of* V.

PROOF. By Proposition 2.4 it is sufficient to write $\Phi_{\mathscr{L}}$ in a neighborhood of 12-exceptional curves $\Theta_{s_1t_1}$ in Figure 1. We will do it for the curves Θ_{00} and $\Theta_{s_1t_1}$, where $(s_1, t_1)=(\pm 1, \pm 1)$ or $(\pm\zeta_4, \pm\zeta_4)$. We use the notation in the proof of Proposition 2.3. For the first curve, let $\alpha_l=X_l/X_0$ $(l=1, 2)$ and $\tilde{\Sigma}^0_{00}$ the open set of $\tilde{\Sigma}_{00}$ determined by $X_0\neq 0$. On $\tilde{\Sigma}^0_{00}$, by definition of the linear system $\mathscr{L}$, the rational map $\Phi_{\mathscr{L}}$ is given by

$$(2.12)\qquad \begin{cases} z_{12}=\mathscr{S}_1^2\mathscr{T}_1^2/2, \\ z_{13}=(1-\alpha_2^2u_{11}^2)\alpha_1\mathscr{S}_1^2\mathscr{T}_1^2/2\,, \qquad z_{14}=(1+\alpha_2^2u_{11}^2)\alpha_1\mathscr{S}_1^2\mathscr{T}_1^2/2\,, \\ z_{23}=(1-\alpha_1^2u_{11}^2)\alpha_2\mathscr{S}_1^2\mathscr{T}_1^2/2\,, \qquad z_{24}=(1+\alpha_1^2u_{11}^2)\alpha_2\mathscr{S}_1^2\mathscr{T}_1^2/2\,, \\ z_{34}=\alpha_1\alpha_2u_{11}\mathscr{S}_1^2\mathscr{T}_1^2\,. \end{cases}$$

Clearly $\Phi_{\mathscr{L}}$ is a morphism $S(4)\cap\tilde{\Sigma}_{00}$ and sends the curve Θ_{00}, which is defined to be $Z(u_{11})$, to the rational curve (cf. (1.12))

$$z_{34}=0\,,\quad z_{13}=z_{14}\,,\quad z_{23}=z_{24}\,,\quad z_{12}^2+z_{23}^2=z_{13}^2$$

on V. On the other hand $\Theta_{0,1}\cup\Theta_{0,2}$ is defined by $X_2=0$ and its image by $\Phi_{\mathscr{L}}$ is

$$z_{23}=z_{24}=z_{34}=0\,.$$

By (2.5) and (2.6), this means that

$\Theta_{s_1,m}$ $(s_1=0, m=1, 2)$ are contracted to the singular points $P_{234}(12)$, P_{234}.

In the similar manner,

$\Theta_{s_1,m}$ $(s_1=\infty, m=1, 2)$ are mapped to the singular points $P_{234}(14)$, $P_{234}(13)$ and the rational curves $\Theta_{0\infty}$, $\Theta_{\infty 0}$, $\Theta_{\infty\infty}$ on $S(4)$ are sent to the rational curves

$$z_{34}=0\,,\quad z_{12}^2+z_{23}^2=z_{13}^2 \quad\text{and}\quad \begin{cases} z_{13}=z_{14}\,, \quad z_{23}=-z_{24}\,, \\ z_{13}=-z_{14}\,, \quad z_{23}=z_{24}\,, \\ z_{13}=-z_{14}\,, \quad z_{23}=-z_{24}\,. \end{cases}$$

Next, we consider expressions of $\Phi_{\mathscr{L}}$ on neighborhoods of exceptional curves $\Theta_{\delta\varepsilon}$, where $(\delta, \tau)=(\pm 1, \pm 1)$, $(\pm\zeta_4, \pm\zeta_4)$. Let $\beta_l'=Y_l/Y_1$ $(l=0, 2)$ and let $\tilde{\Sigma}^1_{\delta\tau}$ be the open set of $\tilde{\Sigma}^1_{\delta\tau}$ defined by $Y_1\neq 0$. Then, on $\tilde{\Sigma}^1_{\delta\tau}$, the contraction $\Phi_{\mathscr{L}}$ is given as follows:

$$(2.13)\qquad \begin{cases} z_{12}=\beta_0'(t_1-\tau)\,, \\ z_{13}=\{1-(\beta_2'(t_1-\tau)-\delta)^2\}t_1/2\,, \qquad z_{14}=\{1+(\beta_2'(t_1-\tau)-\delta)^2\}t_1/2\,, \\ z_{23}=(1-t_1^2)(\beta_2'(t_1-\tau)+\delta)/2\,, \qquad z_{24}=(1+t_1^2)(\beta_2'(t_1-\tau)+\delta)/2\,, \\ z_{34}=t_1(\beta_2'+\delta)^2\,. \end{cases}$$

Since $\Theta_{s_1t_1}$ $(s_1=\delta, t_1=\tau)$ are defined by $t_1=\tau$, they are sent to points

$$(z_{12} : z_{13} : z_{14} : z_{23} : z_{24} : z_{34}) = (0 : \tau - \tau\delta^2 : \tau + \tau\delta^2 : \delta - \delta^3 : \delta + \delta^3 : 2\tau\delta) .$$

Hence we have the contraction

$$\Theta_{11} \to P_{123} , \quad \Theta_{1-1} \to P_{123}(24) , \quad \Theta_{-11} \to P_{123}(13) ,$$
$$\Theta_{-1-1} \to P_{123}(34) , \quad \Theta_{\zeta_4\zeta_4} \to P_{124}(34) , \quad \Theta_{\zeta_4-\zeta_4} \to P_{124}(12) ,$$
$$\Theta_{-\zeta_4\zeta_4} \to P_{124}(14) , \quad \Theta_{-\zeta_4-\zeta_4} \to P_{124} .$$

Finally, by (2.10), (2.12) and (2.13), we see that,

$$\tilde{r}_{a_4,\varepsilon b_4},\ \tilde{r}_{-a_4,-\varepsilon b_4},\ \tilde{r}_{a_4,-\varepsilon b_4},\ \tilde{r}_{-a_4,\varepsilon b_4} \text{ are mapped to}$$
$$P_{134},\ P_{134}(12),\ P_{134}(23),\ P_{134}(24) .$$

Thus we have the theorem. □

REMARK 2.6. In terms of the fibre system $\tilde{\Psi}_N : S(4) \to N$, the 16 rational curves in Theorem 2.5 are described as follows: They consist of 12 non-singular rational curves

$$\Theta_{t_1,m} \ (t_1 = 0, \infty, m = 1, 2) , \qquad \Theta_{s_1 t_1} \ ((s_1, t_1) = (\pm 1, \pm 1), (\pm\zeta_4, \pm\zeta_4)) ,$$

which appear in the singular fibres of $\tilde{\Psi}_N : S(4) \to N$ and 4 sections of this fibre system. These sections have the corresponding meaning to $\tilde{r}_{a_4,\varepsilon b_4}$, $\tilde{r}_{-a_4,-\varepsilon b_4}$, $\tilde{r}_{a_4,-\varepsilon b_4}$ and $\tilde{r}_{-a_4,\varepsilon b_4}$, which are the sections of the fibre system in Theorem 2.5.

REMARK 2.7. Using $\Phi_{\mathscr{L}}$, the structure of the surface V as the elliptic surface is written in terms of $z_{\alpha\beta}$. Define a conic $M' : z_{13}^2 + z_{34}^2 = z_{14}^2$ in $\mathbf{P}_2$ with homogeneous coordinates $(z_{13} : z_{14} : z_{23})$. By the proof of Proposition 2.4, the conic is biregular to a projective line M. This implies that $\tilde{\Psi}_M : S(4) \to M$ determines the fibre system $V \to M$ whose regular fibre is defined by

$$\begin{cases} z_{12}^2 + z_{23}^2 = \dfrac{(s_1^2+1)^2}{4s_1^2} z_{34}^2 , \\ z_{12}^2 + z_{24}^2 = z_{14}^2 . \end{cases}$$

Consider also a conic $N' : z_{23}^2 + z_{34}^2 = z_{24}^2$ in $\mathbf{P}_2$. By Remark 2.6, it is biregular to a projective line N and the fibre system $\tilde{\Psi}_N : S(4) \to N$ determines $V \to N$ whose regular fibre is defined by

$$\begin{cases} z_{12}^2 + \dfrac{(t_1^2+1)^2}{4t_1^2} z_{34}^2 = z_{13}^2 , \\ z_{12}^2 + z_{24}^2 = z_{14}^2 . \end{cases}$$

These induce the following commutative diagram

$$\begin{array}{ccccc} N & \xleftarrow{\tilde{\Psi}_N} & S(4) & \xrightarrow{\tilde{\Psi}_M} & M \\ \downarrow & & \downarrow{\scriptstyle \Phi_{\mathscr{L}}} & & \downarrow \\ N' & \longleftarrow & V & \longrightarrow & M' \end{array} .$$

This diagram occurs by taking a pair from the following four conics

$$\begin{cases} z_{12}^2+z_{23}^2=z_{13}^2 , & z_{12}^2+z_{24}^2=z_{14}^2 , \\ z_{13}^2+z_{34}^2=z_{14}^2 , & z_{23}^2+z_{34}^2=z_{24}^2 . \end{cases}$$

Thus, by the choice of pairs, we have $6=\binom{4}{2}$ diagrams similar to the one soon above.

3. Chern class formula.

In this section, we investigate the number of the $\mathbf{F}_p$-rational points of the variety V defined in §1.

3.1. Rational points of the surface V. Let p be a prime congruent to 1 mod 4 and χ_4 be a multiplicative character of $\mathbf{F}_p^\times$ of order 4. The square χ_4^2 of χ_4 is denoted by χ_2. We define the Jacobi sum $J=J(\chi_2, \chi_4)$ as

$$J(\chi_2, \chi_4)=\sum_{-\xi+\eta+1=0} \chi_2(\xi)\chi_4(\eta) .$$

Since the character $\chi_2(y)$ is real valued, we have $\overline{J(\chi_2, \chi_4)}=J(\chi_2, \overline{\chi_4})$. It is known that $J\bar{J}=p$ (cf. [L]). Since $J\in\mathbf{Z}[\sqrt{-1}]$, we have

$$Nm_{\mathbf{Q}(\sqrt{-1})/\mathbf{Q}}(J)=p . \tag{3.1}$$

Let A_1 be the non-singular projective model of the curve $y^2-x^4+1=0$ and l a prime number relatively prime to 2. Using this Jacobi sum, the trace of the Frobenius action on the *étale* cohomology group $H^1(\bar{A}_1, \mathbf{Q}_l)$ can be expressed as follows. Here $\bar{A}_1$ denotes $A_1\otimes\bar{\mathbf{F}}_p$. By Grothendieck's Lefschetz trace formula, we have

$$\sum_{i=0}^{2} (-1)^i \operatorname{tr}(F_r \mid H^i(\bar{A}_1, \mathbf{Q}_l))=\#\mathrm{rat}(A_1) .$$

The number $\#\mathrm{rat}(A_1)$ can be computed using the result of Weil [W] as

$$\#\mathrm{rat}(A_1)=1+p+(J+\bar{J}).$$

Since $\operatorname{tr}(F_r \mid H^0(\bar{A}_1, \mathbf{Q}_l))=1$, $\operatorname{tr}(F_r \mid H^2(\bar{A}_1, \mathbf{Q}_l))=p$, we have

$$\operatorname{tr}(F_r \mid H^1(\bar{A}_1, \mathbf{Q}_l))=-(J+\bar{J}) . \tag{3.2}$$

Now we compute the number of the $\mathbf{F}_p$-rational points $\#\mathrm{rat}(V)$.

PROPOSITION 3.1. $\#\mathrm{rat}(V)=1+2p+p^2+(J+\bar{J})^2$.

PROOF. Let $A_2=A_1/(\mathbf{Z}/2\mathbf{Z})$ be the elliptic curve defined in §1. Since the action of $\mathbf{Z}/2\mathbf{Z}$ on A_1 is $\mathbf{F}_p$-rational, the natural isogeny $A_1 \to A_2$ is defined over $\mathbf{F}_p$. The abelian variety $A=(A_2\times A_2)/(\mathbf{Z}/2\mathbf{Z})$ is also the quotient of an involution defined over $\mathbf{F}_p$, the natural isogeny $A_2\times A_2 \to A$ is also defined over $\mathbf{F}_p$. Therefore, the natural homomorphism

$$H^i(\bar{A}, \mathbf{Q}_l) \to H^i(\bar{A}_2\times \bar{A}_2, \mathbf{Q}_l) \tag{3.3}$$

is a $Gal(\bar{\mathbf{F}}_p/\mathbf{F}_p)$-equivariant homomorphism. Since the variety V is the quotient of A by the inversion of abelian surfaces, we have

$$H^i(\bar{V}, \mathbf{Q}_l)=\begin{cases} H^i(\bar{A}, \mathbf{Q}_l)\cong \bigwedge^i H^1(\bar{A}, \mathbf{Q}_l) & (i=0, 2, 4) \\ 0 & (i=1, 3,\ i\geq 5)\,. \end{cases}$$

By the isomorphism (3.3), we have

$$\begin{aligned} H^2(\bar{V}, \mathbf{Q}_l)&=H^0(\bar{A}_2, \mathbf{Q}_l)\otimes H^2(\bar{A}_2, \mathbf{Q}_l) \\ &\quad \oplus H^1(\bar{A}_2, \mathbf{Q}_l)\otimes H^1(\bar{A}_2, \mathbf{Q}_l) \\ &\quad \oplus H^2(\bar{A}_2, \mathbf{Q}_l)\otimes H^0(\bar{A}_2, \mathbf{Q}_l) \\ &\cong \mathbf{Q}_l(-1)^{\oplus 2}\oplus (H^1(\bar{A}_2, \mathbf{Q}_l)\otimes H^1(\bar{A}_2, \mathbf{Q}_l))\,, \\ H^0(\bar{V}, \mathbf{Q}_l)&\cong \mathbf{Q}_l\,, \qquad H^4(\bar{V}, \mathbf{Q}_l)\cong \mathbf{Q}_l(-2)\,. \end{aligned}$$

By using the relation (3.2), we have the proposition. □

By using the following result of Davenport and the fact (3.1), we can calculate $\#\mathrm{rat}(V)$ more explicitly.

LEMMA 3.2 ([D-H]).

$$J\equiv 1 \pmod{2+2\sqrt{-1}}\,. \tag{3.4}$$

REMARK 3.3. Using (3.1) and (3.4), J is determined uniquely.

COROLLARY 3.4. *Let p be a prime number congruent to* 1 (mod 4). *Let, a, b be integers such that $a^2+b^2=p$ and a odd. Then $(J+\bar{J})^2=4a^2$.*

PROOF. If we write $J=a+b\sqrt{-1}$ $(a, b\in\mathbf{Z})$, then we have $a+b\sqrt{-1}\equiv 1 \pmod 2$ and $a^2+b^2=p$. Therefore a should be an odd number and we get the corollary. □

COROLLARY 3.5. *Under the notation as above, we have*

$$\#\mathrm{rat}(V)=1+2p+p^2+4a^2\,.$$

From this we derive some interesting facts. First the cardinal number $m_{4:6}$ of $\mathscr{C}_{4:6}$ is given by

COROLLARY 3.6.

$$m_{4:6}=(1/64\times 24)p(p-1)(p^2-22p+81+4a^2)\,.$$

PROOF. Clear from Corollary 3.5, Lemma 1.9 and Lemma 1.12. □

By an observation it is expected that $m_{4:6}=\#\mathscr{C}_{4:6}$ satisfies the relation

$$\lim_{p\to\infty} m_{4:6}\Big/\binom{p}{4}=1/64\,.$$

THEOREM 3.7. *We have the following formula*

$$m_{4:6}-\binom{p}{4}\Big/64=(64\times 24)^{-1}p(p-1)(-17p+75+4a^2)\,.$$

We add the following

COROLLARY 3.8. *The cardinality* $m_{4:4(b)}=\#\mathscr{C}_{4:4(b)}$ *is given by*

$$m_{4:4(b)}=(128\times 4)^{-1}p(p-1)(p^2-6p+1+4a^2)\,.$$

PROOF. By Proposition 1.8 we have

$$4m_{4:4(b)}=12m_{4:6}+(1/8)p(p-1)(p-5)$$

and Corollary 3.6 ensures the present corollary. □

This gives the following characterization of the prime number $p=5$ among all prime numbers p which are congruent to 1 modulo 4.

COROLLARY 3.9. *There is no subset* I *of* $\mathbf{F}_p$, $\#I=4$, *whose graph is isomorphic to the square* (*cf.* §1.1) *if and only if* $p=5$.

3.2. Chern number formula. Consider the $(p-1)$-dimensional complex projective space $\mathbf{P}_{p-1}=\mathbf{P}_{p-1}(\mathbf{C})$ with homogeneous coordinates $x=(x_i)$ $(i\in\mathbf{F}_p)$. Denote by X_i^1 the hyperplane $Z(x_i)$. We set

$$X^1=\bigcup_{i\in\mathbf{F}_p} X_i^1 \quad\text{and}\quad X^2=\bigcup_{i,j\in\mathbf{F}_p}(X_i^1\cap X_j^1)\,.$$

(In the second definition we assume that $i\neq j$.) For each $i\in F_p$ take an open neighborhood N_i of $\dot{X}_i^1=X_i^1-X^2$ in $\dot{\mathbf{P}}_{p-1}=\mathbf{P}_{p-1}-X^2$ so that

$$N_i\cap N_j=\varnothing \qquad \text{if } i\neq j\,.$$

Moreover, form monomials

$$f_i^+=\prod_j x_j\,,\qquad f_i^-=\prod_k x_k\,,$$

where j and k exhaust respectively all elements of $\mathbf{F}_p$ satisfying $\left(\frac{j-i}{p}\right)=1$ and $\left(\frac{k-i}{p}\right)=-1$.

Form a matrix

$$A_{|N_i}=\begin{pmatrix} 1 & (-f_i^-/f_i^+)_{|N_i} \\ 0 & (x_i/x_{i+1})_{|N_i} \end{pmatrix}.$$

This matrix defines a locally free sheaf $\dot{\mathfrak{E}}_p$ of rank two over $\dot{\mathbf{P}}_{p-1}$. Define a reflexive sheaf $\mathfrak{E}_p$ over $\mathbf{P}_{p-1}(\mathbf{C})$ by $\mathfrak{E}_p=\iota_*\dot{\mathfrak{E}}_p$ where ι is the injection $\dot{\mathbf{P}}_{p-1}\subset\mathbf{P}_{p-1}$. Then we know (cf. [SEK 1], [SEK 2]) that the Chern classes $c_i(\mathfrak{E}_p)$ $(1\leq i\leq 3)$ are given by

$$c_1(\mathfrak{E}_p)=p\,,\quad c_2(\mathfrak{E}_p)=p(p-1)/2\,,\quad c_3(\mathfrak{E}_p)=0$$

and the fourth Chern class $c_4(\mathfrak{E}_p)$ is given by (C1) in Introduction. By Corollary 3.8 we have

THEOREM 3.10. $c_4(\mathfrak{E}_p)=-(5/64)p(p-1)(p^2-6p+1+4a^2)$.

By Corollary 3.9 we have

COROLLARY 3.11. $c_4(\mathfrak{E}_p)=0$ *if and only if* $p=5$.

Thus the reflexive sheaf $\mathfrak{E}_p$ is locally free if and only if $p=5$. When one of the authors began the research in [SEK 1], [SEK 2], his hope was that there may be some small prime numbers p for which $\mathfrak{E}_p$ has no singularity at codimension 4. However, this is false by a characteristic fact, Corollary 3.10. We hope that the content here gives a hint to consider the existence or non existence of a non indecomposable reflexive sheaf of rank two on $\mathbf{P}_n(\mathbf{C})$ $(4\leq n)$, which do not have singularity at codimension 4 and are different from the Horrocks-Mumford bundle.

4. Appendix.

In the first place, using results of §3, we calculate the fourth Chern class $c_4(\mathfrak{E}_p)$ in the case of $p\equiv 1 \pmod 4$, $p<100$ and give the following table:

p	5	13	17	29	37	41
a	1	3	1	5	1	5
$m_{4:6}/p$	0	0	0	7	15	25
$c_4(\mathfrak{E}_p)/p$	0	−120	−240	−1680	−3240	−4800
p	53	61	73	89	97	
a	7	5	3	5	9	
$m_{4:6}/p$	65	100	180	352	480	
$c_4(\mathfrak{E}_p)/p$	−10920	−16200	−27720	−51480	−68640	

In the second place, we give quadratic residue graphs with respect to $p=5$, 13, 17; see Figure 4.

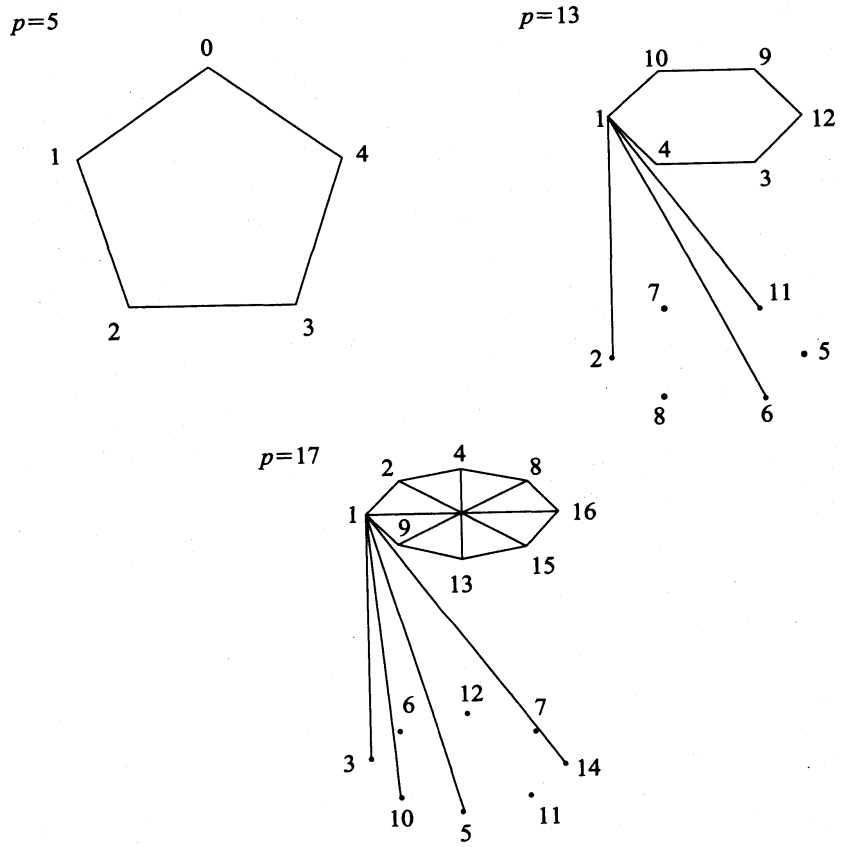

FIGURE 4

References

[B-H] W. BARTH and K. HULEK, Projective models of Shioda modular surface, Manuscripta Math. **50** (1985), 73–132.

[B-H-M] W. BARTH, K. HULEK and R. MOORE, Shioda's modular surface S(5) and the Horrocks-Mumford bundle, *Proc. Tate Conf. Algebraic Vector Bundles over Algebraic Varieties* (1984), Bombay.

[B-P-V] W. BARTH, C. PETERS and VAN DE VEN, *Compact Complex Surface*, Springer (1984).

[D-H] H. DAVENPORT and H. HASSE, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math. **172** (1935), 151–182.

[D-M] E. DICKSON and W. MAGNUS, *Linear Groups: with Exposition of the Galois Field Theory*, Dover (1958).

[G] F. GAUSS, Theorie der biquadratische Reste erste Abhandlung, Arithmétische Untersuchungen, 511–533.

[H] T. HIRANE, Quadratic residue and cocycle K3 *surface*, Master Thesis, Tokyo Metropolitan Univ. (1992).

[H-M] G. HORROCKS and D. MUMFORD, A rank 2 vector bundle on $\mathbf{P}_4$ with 15000 symmetries, Topology **12** (1973), 63–81.

[K] K. KODAIRA, On compact analytic surfaces II, Ann. of Math. **77** (1963), 562–626.

[L] S. LANG, *Cyclotomic Fields*, Springer (1984).

[SEK 1] N. SASAKURA, Y. ENTA and M. KAGESAWA, Construction of rank two reflexive sheaves which are constructed from the prime field $\mathbf{F}_p$, Proc. Japan. Acad. Ser A **69** (1993), 144–148.

[SEK 2] N. SASAKURA, Y. ENTA and M. KAGESAWA, Construction of rank 2 reflexive sheaves by means of quadratic residue graph, preprint (1993).

[Sh 1] T. SHIODA, On elliptic modular surfaces, J. Math. Soc. Japan **24** (1972), 20–59.

[Sh 2] T. SHIODA, On rational points of the generic elliptic curves with level N structure over the field of modular functions of level N, J. Math. Soc. Japan **25** (1973), 144–157.

[Sh 3] T. SHIODA, Algebraic cycles on certain $K3$ surfaces in characteristic p, *Proc. Int. Congr. on Manifolds*, Univ. Tokyo Press (1975), 357–364.

[W] A. WEIL, Number of solutions of equations in finite fields, Bull. Amer. Math. Soc. **55** (1949), 497–508.

Present Address:
DEPARTMENT OF MATHEMATICS, TOKYO METROPOLITAN UNIVERSITY,
MINAMI-OHSAWA, HACHIOJI-SHI, TOKYO, 192–03 JAPAN.