COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 38, No. 2 1989

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

# Frey's Elliptic Curve as an Elliptic Surface over the Fermat Curve

**Dedicated to Professor F. Hirzebruch**

by

Tetsuji SHIODA

(Received April 12, 1989)

## § 0. Introduction

Recently G. Frey found a remarkable connection between Fermat's conjecture and the Shimura-Taniyama-Weil conjecture on elliptic curves over $\mathbb{Q}$, by associating with a non-trivial solution $(z_1, z_2, z_3)$ of the Fermat equation

$$z_1^m + z_2^m = z_3^m \tag{1}$$

an elliptic curve defined by

$$y^2 = x(x+z_1^m)(x-z_2^m)\,. \tag{2}$$

We refer to Frey [F1], [F2], Ribet [R] for this subject.

In this paper, we look at the equation (2) from a slightly different angle. Namely, letting $(z_1 : z_2 : 1)$ $(z_3 = 1)$ be the generic point of the Fermat curve (1), we can view (2) as the defining equation of an eqlliptic surface over the Fermat curve.

The properties of these elliptic surfaces can be studied by using the general theory of elliptic surfaces due to Kodaira [K]. The singular fibres and the numerical characters are easily determined. One noteworthy property is that the Mordell-Weil group of these elliptic surfaces is always finite and, more precisely, it is isomorphic to either

$$\mathbb{Z}/\mathbb{Z}2\oplus\mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$$

according as $m$ (= the degree of the Fermat curve) is odd or even (Theorems 3, 4 in § 2). This suggests that the elliptic surface in question might be an elliptic modular surface attached to some discontinuous group $\Gamma$ in the sense of our earlier paper [S1]. We show that this is indeed the case (Theorem 7, § 3). The group $\Gamma$ is isomorphic to the fundamental group of the Fermat curve (1) deleted the $3m$ cusps (i.e. the points with $z_1 z_2 z_3 = 0$); according to Klein-Fricke [KF], $\Gamma$ is *not* a congruence subgroup if $m \neq 1$, 2, 4 or 8. Thus we obtain some elliptic modular surfaces attached to non-congruence subgroups which have a simple algebraic definition. It may be suggestive to call $\Gamma$ *the Fermat modular group of F-level m*, and the elliptic surface in question *the Fermat modular surface of F-level m*.

We expect that the Fermat modular surfaces may provide an interesting class of algebraic surfaces, just as did the elliptic modular surfaces attached to congruence subgroups.

## § 1. The elliptic surface $F_m$ and its singular fibres

Fix a positive integer $m$. Let $C_m$ denote the Fermat curve of degree $m$:

$$C_m : z_1^m + z_2^m = z_3^m \tag{1}$$

in a projective plane $\mathbb{P}^2$ with homogeneous coordinates $(z_1 : z_2 : z_3)$. The ground field is the field of complex numbers $\mathbb{C}$, unless otherwise stated. There are $3m$ points of $C_m$ satisfying $z_1 z_2 z_3 = 0$, and they are called the *cusps* of $C_m$. Let

$$C'_m = C_m - \{\text{cusps}\} \subset C_m \cap \{z_3 \neq 0\} .$$

Any point of $C'_m$ is written as $(z_1 : z_2 : 1)$ with $z_1^m + z_2^m = 1$.

Consider the open elliptic surface, say $F'_m$, over $C'_m$ defined by

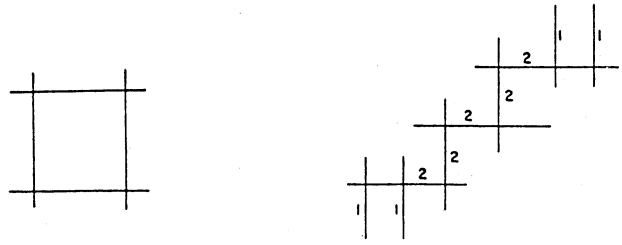
$$y^2 = x(x + z_1^m)(x - z_1^m) \qquad (z_1^m + z_2^m = 1) , \tag{2}$$

and let $F_m$ be the elliptic surface over $C_m$ extending $F'_m$ over $C'_m$. As is well-known, there is a unique such $F_m$ which is a smooth, complete algebraic surface containing no exceptional curves of the first kind in fibres. The surface $F_m$ is obtained from $F'_m$ by adjoining singular fibres over the $3m$ cusps.

PROPOSITION 1. *The types of the singular fibres of $F_m$ are given as folloes*: (i) *If $m$ is odd, the singular fibres over the finite cusps (i.e. the cusps where $z_3 \neq 0$) are all of type $I_{2m}$, while those over the infinite cusps (the cusps with $z_3 = 0$) are of type $I^*_{2m}$.*

(ii) *If $m$ is even, all the singular fibres are of type $I_{2m}$.*

Before the proof, let us recall that the Kodaira symbol $I_b$ ($b > 0$) denotes a cycle of $b$ lines (a "$b$-gon") and $I^*_b$ denotes a configuration of $(b+5)$ lines (cf. [K]):




$I_b$ $\qquad\qquad$ $I^*_b$

Further, the absolute invariant (the functional invariant in the terminology of [K]) has a pole of order $b$ at the point of the base curve supporting a singular fibre of type $I_b$ or $I^*_b$, and the distinction between these two can be read off from the local monodromy: the conjugacy class of the local monodromy in $SL_2(\mathbb{Z})$ is represented by

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad -\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

according as the singular fibre is of type $I_b$ or $I_b^*$.

*Proof.* First consider the case $m=1$. By the change of coordinates

$$\lambda = z_1, \qquad X = x + z_1, \qquad Y = y,$$

the elliptic surface $F_1$ over $C_1$ takes a familiar form

$$y^2 = X(X-1)(X-\lambda)$$

which is an elliptic surface over $\mathbb{P}^1$ ($\lambda$-line) with the singular fibres over $\lambda = 0$, 1 and $\infty$. It is easy to see that the singular fibres are of type $I_2$ at $\lambda = 0$, 1 and of type $I_2^*$ at $\lambda = \infty$. Moreover the monodromy representation of the fundamental group $\pi_1(C_1') = \pi_1(\mathbb{P}^1 - \{0, 1, \infty\})$ can be normalized so that the small positively oriented loops around $\lambda = 0$, 1, $\infty$ are respectively represented by the matrices

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}, \quad \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix}.$$

In the general case $m > 1$, one should note that the open surface $F_m'$ over $C_m'$ is induced from $F_1' \to C_1'$ via the morphism

$$C_m \to C_1 \qquad (z_1 : z_2 : z_3) \mapsto (z_1^m : z_2^m : z_3^m).$$

In other words, $F_m'$ is just the fibre product of $F_1'$ and $C_m'$ over $C_1'$, the map $C_m' \to C_1'$ being the restriction of the morphism $C_m \to C_1$ above and unramified. Hence the local monodromy at the cusps of $C_m$ over $\lambda = 0$ (resp. $\lambda = 1$ or $\lambda = \infty$) is given by

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}^m \underset{\text{conj.}}{\sim} \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix}$$

$$\left( \text{resp.} \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}^m \underset{\text{conj.}}{\sim} \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix} \right.$$

$$\left. \text{or} \quad \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix}^m = (-1)^m \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix} \right),$$

because the ramification index at each cusp is $m$. Since the type of a singular fibre is determined by the conjugacy class of local monodromy in $SL_2(\mathbb{Z})$, we conclude that the singular fibre at a finite cusp of $C_m$ is of type $I_{2m}$, while the singular fibre at an infinite cusp is of type $I_{2m}$ or $I_{2m}^*$ according as $m$ is even or odd.

PROPOSITION 2. *The numerical characters of the elliptic surface $F_m$ are given as follows*:

$$
\begin{aligned}
q &= \textit{the irregularity of } F_m \\
&= \textit{the genus of } C_m \\
&= (m-1)(m-2)/2 \\
b_1(F_m) &= b_1(C_m) = 2q \\
p_g &= \textit{the geometric genus of } F_m \\
&= \begin{cases} m^2 - \frac{3}{2}m & (m: \textit{even}) \\ m^2 - m & (m: \textit{odd}) \end{cases} \\
c_2 &= \begin{cases} 6m^2 & (m: \textit{even}) \\ 6m^2 + 6m & (m: \textit{odd}) \end{cases} \\
b_2 &= \begin{cases} 8m^2 - 6m + 2 & (m: \textit{even}) \\ 8m^2 + 2 & (m: \textit{odd}) \end{cases} \\
h^{1,1} &= \begin{cases} 6m^2 - 3m + 2 & (m: \textit{even}) \\ 6m^2 + 2m + 2 & (m: \textit{odd}) \end{cases}
\end{aligned}
$$

(*Here* $b_\nu = \nu$*-th Betti number,* $h^{i,j} =$ *the Hodge numbers,* $c_2 =$ *the Euler number.*)

*Proof.* This is a simple exercise, using [K], once one knows the types of singular fibres. □

## § 2. The Mordell-Weil group of $F_m$

The generic fibre of the elliptic surface $F_m$ over $C_m$ can be regarded as an elliptic curve, say $E$, defined over the function field $K = \mathbb{C}(C_m)$ of the Fermat curve $C_m$. Explicitly, $E$ is the elliptic curve

$$y^2 = x(x + z_1^m)(x - z_2^m)$$

over $K = \mathbb{C}(z_1, z_2)$, with $(z_1, z_2)$ being the generic point of $z_1^m + z_2^m = 1$ over $\mathbb{C}$.

As usual, we take the point at infinity of $E$ as the origin of the group law on $E$. Then, by the Mordell-Weil theorem, the group $E(K)$ of $K$-rational points of $E$ is a finitely generated abelian group. It is canonically isomorphic to the group of holomorphic sections of $F_m$ over $C_m$, and so it will be also called *the Mordell-Weil group of the elliptic surface* $F_m$ (over $C_m$).

The Mordell-Weil rank of $F_m$, say $r$, which is defined as the free rank of the group $E(K)$, is related to the Picard number $\rho = \rho(F_m)$ of the surface $F_m$ by a general formula

$$\rho = r + 2 + \sum_{v \in C_m} (m_v - 1) \tag{3}$$

where $m_v$ is the number of irreducible components in the fibre over a point $v$ of $C_m$

(cf. [S1]).

THEOREM 3. *For the elliptic surface $F_m$ over $C_m$, the following equivalent statements hold:*

(i) $\rho = h^{1,1}$,

(ii) $r=0$ (*i.e. the Mordel-Weil group of $F_m$ is finite*).

*Proof.* By Proposition 1, the singular fibre over a cusp $v$ of $C_m$ is of type $I^*_{2m}$ or $I^*_{2m}$, and so the number of irreducible components is $2m$ or $2m+5$ accordingly. By the formula (3), we have

$$\rho = r+2+\begin{cases}(2m-1)\cdot 3m\\ (2m-1)\cdot 2m+(2m+4)\cdot m\,.\end{cases}$$

Comparing with the value of $h^{1,1}$ in Proposition 2, we see that

$$\rho = r+h^{1,1}\,.$$

But, since we have $\rho \le h^{1,1}$ (we are working over $\mathbb{C}$) and $r\ge 0$, we conclude that

$$\rho = h^{1,1} \quad \text{and} \quad r=0\,.$$

□

THEOREM 4. *The Mordell-Weil group of $F_m$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ or $(\mathbb{Z}/4\mathbb{Z})^{\oplus 2}$ according as $m$ is odd or even.*

*Proof.* First, note that the Mordell-Weil group $E(K)$ contains all 2-torsion points:

$$(x, y)=(0, 0)\,, \qquad (-z_1^m, 0)\,, \qquad (z_2^m, 0)$$

for any $m$. Next, let

$$\varphi=\varphi_m : \pi_1(C'_m, u)\to SL_2(\mathbb{Z})$$

denote the monodromy representation associated with the elliptic surface $F_m\to C_m$, $u\in C'_m$ being a reference point. Identify the first homology group of the fibre over $u$ with $\mathbb{Z}\oplus\mathbb{Z}$, and then any torsion point of that fibre is represented by some $(a, b)\in(\mathbb{Q}/\mathbb{Z})^{\oplus 2}$. If this torsion point comes from a global section of $F_m$ over $C_m$ (i.e. from a torsion element of $E(K)$), then it should be invariant under arbitrary monodromy. In other words, we should have

$$(a, b)(\gamma-1_2)\in\mathbb{Z}\oplus\mathbb{Z}$$

for any $\gamma$ in the image of $\varphi$.

New assume that $m$ is odd. Then, as we saw in the proof of Proposition 1, we can take

$$\gamma=\begin{pmatrix}-1 & -2\\ 0 & -1\end{pmatrix}^m=\begin{pmatrix}-1 & -2m\\ 0 & -1\end{pmatrix}$$

so that

$$\gamma - 1_2 = \begin{pmatrix} -2 & -2m \\ 0 & -2 \end{pmatrix}.$$

This implies that every torsion of $E(K)$ must be 2-torsion. Therefore we have $E(K)_{\mathrm{tor}} \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ if $m$ is odd.

Finally consider the case $m$=even. As we noted before, $F'_m$ is the fibre product of $F'_1$ and $C'_m$ over $C'_1$. Since $C'_m \to C'_1$ is a Galois covering with an abelian Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{\oplus 2}$, any commutator $[\gamma_1, \gamma_2]$, $\gamma_1, \gamma_2$ in the image of the monodromy representation of $\pi_1(C'_1)$, belongs to the image of $\varphi_m$. Taking

$$\gamma_1 = \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix}, \qquad \gamma_2 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \in \mathrm{Im}(\varphi_1),$$

we have

$$\gamma_1\gamma_2 - \gamma_2\gamma_1 = \begin{pmatrix} 4 & 0 \\ 0 & -4 \end{pmatrix}.$$

This implies that every torsion of the Mordell-Weil group $E(K)$ must be 4-torsion. (We have not so far used the assumption $m$=even.)

If we can show that $E(K)_{\mathrm{tor}}$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^{\oplus 2}$ for $m=2$, then the same will be the case for any $m$ even, because we have

$$F'_m = F'_2 \times_{C'_2} C'_m \qquad (m: \text{even}),$$

the map $C'_m \to C'_2$ being $(z_1, z_2) \mapsto (z_1^{m/2}, z_2^{m/2})$. □

Thus it suffices to prove the following proposition.

PROPOSITION 5. *The elliptic surface $F_m$ for $m=2$ is isomorphic to the elliptic modular surface of level 4 (attached to the principal congruence subgroup $\Gamma(4)$ of $SL_2(\mathbb{Z})$) as elliptic surfaces over $\mathbb{P}^1$. In particular, the Mordel-Weil group of $F_2$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$.*

*Proof.* Recall that the elliptic modular surface of level 4, denoted $B(4)$, is an elliptic $K3$ surface over $\mathbb{P}^1$ ($\sigma$-line) whose generic fibre is given by

$$Y^2 = X(X-1)(X-\lambda), \qquad \lambda = \left(\frac{1}{2}(\sigma + \sigma^{-1})\right)^2.$$

(cf. [S2], [S3]). On the other hand, the elliptic surface $F_2$ over $C_2$ is defined by the equation

$$y^2 = x(x+z_1^2)(x-z_2^2), \qquad z_1^2 + z_2^2 = 1.$$

First we can identify $C_2$ with $\mathbb{P}^1$ ($\sigma$-line) by the isomorphism:

$$\sigma=\frac{z_1+1}{iz_2}=\frac{iz_2}{z_1-1} \qquad (i=\sqrt{-1})\,.$$

Then we have $\lambda=-(z_1/z_2)^2$, and the change of variables

$$X=x/z_2^2\,, \qquad Y=y/z_2^3$$

defines an isomorphism between the generic fibres of $F_2$ and $B(4)$ over $\mathbb{P}^1$. Hence the two surfaces $F_2$ and $B(4)$ are birational, and since they are both $K3$ surfaces, $F_2$ and $B(4)$ are isomorphic as elliptic surfaces over $\mathbb{P}^1$. For the last assertion of Proposition 5, we refer to [S1], [S2], [S3]. □

We can rephrase Theorem 4 in the following way.

THEOREM 6. *Let $k$ be an algebraically closed field of characteristic 0, and let $\lambda$* be a variable over $k$. For any $m$, let $K_m=k(\sqrt[m]{\lambda}, \sqrt[m]{1-\lambda})$ *in a fixed algebraic closure of $k(\lambda)$. Then the Mordell-Weil group of the elliptic curve*

$$E: Y^2=X(X-1)(X-\lambda)$$

*over $K_m$ is finite and isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ or $(\mathbb{Z}/4\mathbb{Z})^{\oplus 2}$ according to the parity of $m$. Consequently, for any abelian extension $K/k(\lambda)$ unramified outside $\lambda=0, 1, \infty$, the Mordell-Weil group $E(K)$ is a torsion group of order at most* 16.

Going back to our elliptic surface $F_m$, we have:

PROPOSITION 7. *The Néron-Severi group of the surface $F_m$ has the discriminant given by*

$$\det NS(F_m)=\begin{cases} -2^{4(m-1)}m^{2m} & (m: odd) \\ -2^{3m-8}m^{3m} & (m: even)\,. \end{cases}$$

*Proof.* Since we know the singular fibres, the finiteness of the Mordell-Weil group and its order, we have only to apply a general formula proved in [S1, § 1]. The minus sign comes from the Hodge index theorem. □

## § 3. The relation to elliptic modular surfaces

We shall show in this section that the elliptic surface $F_m$ over $C_m$ we have been considering so far is an *elliptic modular surface* attached to certain discontinuous subgroup $\Gamma$ of $SL_2(\mathbb{Z})$ in the sense of [S1].

First the open Fermat curve $C'_m=C_m-\{3m \text{ cusps}\}$ is an unramified Galois covering of $C'_1=C_1-\{3 \text{ cusps}\}$ with the Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{\oplus 2}$. As in the proof of Proposition 1, $C'_1$ can be identified with the $\lambda$-line $\mathbb{P}^1$ deleted the three points $\{0, 1, \infty\}$. The universal covering of $C'_1=\mathbb{P}^1-\{0, 1, \infty\}$ is the upper half plane $H$, and the fundamental group $\pi_1(C'_1)$ is realized as the covering transformation group of $H$ as the group

$$\overline{\Gamma(2)} \subset PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\},$$

the image of $\Gamma(2)$ (the principal congruence group of level 2) under $SL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z})$. group of level 2) under $SL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z})$.

Thus we have a projective representation of $\pi_1(C_1')$:

$$\bar{\varphi} : \pi_1(C_m') \subsetneq \pi_1(C_1') \twoheadrightarrow \overline{\Gamma(2)} \subsetneq PSL_2(\mathbb{Z}).$$

Let $\bar{\Gamma}$ = the image of $\bar{\varphi}$. Then $\bar{\Gamma}$ is of index $m^2$ in $\overline{\Gamma(2)}$, with the quotient $\overline{\Gamma(2)}/\bar{\Gamma} \simeq (\mathbb{Z}/m\mathbb{Z})^{\oplus 2}$. The cusps of $C_m$ become exactly the cusps associated with $\bar{\Gamma}$ in the sense of automorphic functions.

These discontinuous groups $\bar{\Gamma}$, indexed by $m$, have been studied by Klein-Fricke [KF]. According to [KF], $\bar{\Gamma}$ is *not* an congruence subgroup of $PSL_2(\mathbb{Z})$ if $m \neq 1$, 2, 4 or 8 (cf. [KL], p. 196).

Now we have an elliptic surface $F_m$ over $C_m$ whose absolute invariant $j$ has the familiar expression in $\lambda : j = \text{const.}\ (\lambda^2 - \lambda + 1)^3/(\lambda(1-\lambda))^2$. Its monodromy representation on the first homology of a fibre gives a homomorphism

$$\varphi : \pi_1(C_m') \to SL_2(\mathbb{Z})$$

which lifts the projective representation $\bar{\varphi}$ above. In fact, by Kodaira's general theory [K], to give the following data (i) or (ii) is equivalent to each other:

(i) an elliptic surface over $C_m$ with the given absolute invariant, having a global section;

(ii) a lifting of $\bar{\varphi}$ to a representation in $SL_2(\mathbb{Z})$.

Letting

$$\Gamma = \text{the image of } \varphi \subset SL_2(\mathbb{Z}),$$

we see that $\Gamma$ is a subgroup of finite index in $SL_2(\mathbb{Z})$, not containing $-1_2$ (note that $\bar{\varphi}$ is injective) such that $\Gamma \simeq \bar{\Gamma}$.

To such a $\Gamma$, we can attach an *elliptic modular surface* in the sense of [S1].

THEOREM 7. *The elliptic surface $F_m$ over $C_m$ (defined by Frey's construction) is the elliptic modular surface attached to $\Gamma$.*

*Proof.* Call $\overline{\varphi_1}$ and $\varphi_1$ the maps $\bar{\varphi}$, $\varphi$ for $m=1$. Then, since we have $F_m' \simeq F_1' \underset{C_1'}{\times} C_m'$ (fibre product) and $\bar{\varphi}$, $\varphi$ factor through $\overline{\varphi_1}$, $\varphi_1$, we are reduced to the case $m=1$. In this case, $\pi_1(C_1')$ is a free group on two generators $l_0$ and $l_\infty$, represented by the positively oriented loops around $\lambda = 0$ and $\lambda = \infty$. Given the projective representation $\overline{\varphi_1}$ of $\pi_1(C_1')$, there are exactly 4 liftings of $\overline{\varphi_1}$ to a representation of $\pi_1(C_1')$ into $SL_1(\mathbb{Z})$. Among them, there is a unique one mapping $l_\infty$ to $\begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix}$ and $l_0$ to $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$. And this coincides with $\varphi_1$, because the type of singular fibres over $\lambda = \infty$,

0 (of type $I_2^*$ and $I_2$) forces this choice of sign (cf. § 1). It coincides also with the monodromy representation associated to the elliptic modular surface attached to $\Gamma$ (for $m=1$), for the same reason. Hence we have proved the assertion. □

DEFINITION 8. With the same notation as above, let us call $\Gamma\,(=\mathrm{Im}(\varphi)\subset SL_2(\mathbb{Z})$ the Fermat modular group of $F$-level $m$ and write $\Gamma=\Gamma_F(m)$.

Thus Theorem 7 says that the elliptic surface $F_m$ (over the Fermat curve $C_m$) is the elliptic modular surface attached to $\Gamma_F(m)$.

The following is a consequence of Proposition 5, and it refines a result of Klein-Fricke [KF] that $\overline{\Gamma_F(2)}$ is a congruence subgroup.

COROLLARY 9. *The Fermat modular group of F-level* 2 *coincides with the principal congruence subgroup of level* 4, *i.e.* $\Gamma_F(2)=\Gamma(4)$.

Now a nice property of elliptic modular surfaces is that the space of holomorphic 2-forms is canonically isomorphic to the cusp forms of weight 3 (cf. [S1]). We can study these spaces for the elliptic surfaces $F_m$ over $C_m$ using the automorphisms of $C_m$. We hope to come back to this subject in some other occasion.

*Remark.* This work was done during the author's stay at the Mathematical Science Research Institute, Berkeley, in the summer of 1987 and distributed as preprint from MSRI.

In the spring of 1988 at the Max-Planck Institue für Mathematik, Bonn, D. Zagier pointed out that the last step in the proof of Theorem 4 can be directly shown, without using Proposition 5; namely, the standard argument in the proof of the weak Mordell-Weil theorem for $m$-division of a point (here $m=2$) is sufficient. Of course, Proposition 5 is of independent interest as shown in the last section, and so our original proof is given in the text.

## References


[F1] Frey, G.; Modular elliptic curves and Fermat's conjecture, Preprint, 1985.

[F2] Frey, G.; Links between elliptic curves and solutions of $A-B=C$, *J. Indian Math. Soc.* **51** (1987), 117–145.

[KF] Klein, F. and Fricke, R., Vorlesungen über die Theorie der elliptischen Modulfunktionen, Vol. 2, Teubner, 1890; Johnson reprint Corp. 1966.

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

[R] Ribet, K.; On modular representations of Gal $(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Preprint, *MSRI*, 1987.

[KL] Kubert, D. and Lang, S.; Modular units, Springer, 1981.

[S1] Shioda, T.; On elliptic modular surfaces, *J. Math. Soc. Japan*, **24** (1972), 20–59.

[S2] Shioda, T.; On rational points of the generic elliptic curve with level N structure over the field of modular functions of level, N, *J. Math. Soc. Japan*, **25** (1973), 144–157.

[S3] Shioda, T., Algebraic cycles on certain $K3$ surfaces in characteristic p, In: Manifolds, Tokyo 1973, Univ. Tokyo Press, 1975, 357–364.

Department of Mathematics
Rikkyo University
Tokyo