J. Math. Soc. Japan
Vol. 25, No. 1, 1973

On rational points of the generic elliptic curve with level N structure over the field of modular functions of level N*

By Tetsuji SHIODA

(Received April 10, 1972)

Introduction.

For a natural number $N \geqq 3$, let E denote the generic elliptic curve with level N structure in characteristic p ($p \nmid N$), cf. § 1. E is an elliptic curve defined over the field, K, of elliptic modular functions of level N in characteristic p (cf. Igusa [4]). We are interested in the group, $E(K)$, of K-rational points of E, which is finitely generated by Mordell-Weil theorem. By the definition of E, $E(K)$ contains the group, E_N, of points of E of order (dividing) N, and it can be shown that

$$E(K)_{\mathrm{tor}} = E_N .$$

Moreover we proved in our previous work [12] (cited as [EMS]) that, if the characteristic p is zero, then $E(K)$ itself is finite and therefore

$$E(K) = E_N \cong (\boldsymbol{Z}/N\boldsymbol{Z})^2 .$$

One might expect that the same would hold in the case $p > 0$, which is known to be true for $N=3$. However this is not true in general as we explain below for $N=4$.

We recall that, as to the rank of the group of rational points of an elliptic curve defined over a global field, there is a famous conjecture of Birch, Swinnerton-Dyer and Tate relating the rank with the zeta function of the elliptic curve (cf. Tate [13]). In our case, assuming that the constant field k of K is a finite field containing a primitive N-th root of unity, we see that the zeta function of E over K is essentially equal to the Hecke polynomial of level N and of weight 3, cf. [EMS], Appendix. In particular, we get an upper bound for the rank of $E(K)$:

---

* Some results in this paper were reported at "U. S.-Japan Seminar on Modern Methods in Number Theory", Tokyo, Aug. 30–Sept. 5, 1971, under the title "Rational points of Jacobi's quartic curve $y^2=(1-\sigma^2x^2)(1-x^2/\sigma^2)$ over $k(\sigma)$".

$$\operatorname{rank} E(K) \leqq \frac{(N-3)}{3N}\mu(N), \qquad \mu(N)=\frac{1}{2}N^3 \prod_{\substack{l \mid N \\ \text{prime}}}\left(1-\frac{1}{l^2}\right).$$

The purpose of this paper is to study the first non-trivial case $N=4$ more closely. We have (cf. [EMS] p. 56–57):

THEOREM. *Assume* $N=4$. *Then*

i) $E(K)_{\mathrm{tor}}=E_4$ *and* rank $E(K)\leqq 2$.

ii) *If* $p\equiv 1 \bmod 4$, *then* $E(K)=E_4$.

The conjecture of Birch, Swinnerton-Dyer and Tate suggests:

CONJECTURE. If $p\equiv 3 \bmod 4$, then rank $E(K)=2$.

We shall prove a special case of this conjecture:

THEOREM. *If* $p=3$, *then* rank $E(K)=2$.

We can also state these results as follows. Let B_p denote the elliptic modular surface of level 4 in characteristic $p\neq 2$; it is the Kodaira-Néron model of E over K [EMS]. The surface B_0 is a $K3$ surface with Picard number $\rho(B_0)=20$ (and Betti number $b_2=22$), and B_p is a reduction of B_0 mod p. Then we have

$$\rho(B_p)=\begin{cases} 20 & \text{for } p\equiv 1 \bmod 4, \\ 22 & \text{for } p=3, \end{cases}$$

and, conjecturally, $\rho(B_p)=22$ for all $p\equiv 3 \bmod 4$.

The contents of this paper are as follows. In § 1, we recall the definition of elliptic curves with level N structure, and in § 2 and § 3, we consider the special cases $N=2$ and 4. In particular, we shall explicitly construct the universal family of elliptic curves with level 4 structure in § 3. The generic elliptic curve E in this case is given by the Legendre cubic

$$Y^2=X(X-1)(X-\lambda), \qquad \lambda=\frac{1}{4}\left(\sigma+\frac{1}{\sigma}\right)^2,$$

or by the Jacobi quartic

$$y^2=(1-\sigma^2x^2)(1-x^2/\sigma^2),$$

both defined over $K=k(\sigma)$, σ being a variable over a field k. After discussing the relation of our problem to the theory of surfaces in § 4, we prove the above theorems in § 5. Our proof of the second theorem (for $p=3$) is rather computational, and we think that there should be a theoretical proof which clarifies the meaning of the appearance of rational points of infinite order on the generic elliptic curve with level N structure in certain characteristic p.

§ 1. Elliptic curves with level N structure.

Let E be an elliptic curve, i. e. an abelian variety of dimension one, defined over a field k. For each natural number N relatively prime to the characteristic of k, the group, E_N, of points of order N of E is a product of 2 cyclic groups of order N. There is a natural skew-symmetric pairing e_N of E_N with itself (Weil [**14**]). It follows that, if all points of order N are k-rational, then k contains a primitive N-th root of unity.

In the following, we fix once for all a primitive N-th root of unity, ζ, in k; (k, ζ) can be called a level N structure on k. An elliptic curve with level N structure is, by definition, a triple (E, r, s) consisting of an elliptic curve E together with an ordered basis r, s of E_N such that $e_N(r, s)=\zeta$. We say that (E, r, s) is defined over k if E, r, s are all defined over k. Two such triples (E, r, s) and (E', r', s') are called isomorphic if there is an isomorphism of E onto E' mapping r, s to r', s'. An elliptic curve with level N structure has no non-trivial automorphism if $N \geqq 3$. Therefore, given an elliptic curve E and $N \geqq 3$, there exist

$$\mu(N)=\frac{1}{2}N^3 \prod_{\substack{l \mid N \\ \text{prime}}} \left(1-\frac{1}{l^2}\right) \qquad (N \geqq 3)$$

distinct level N structures on E up to isomorphism.

Finally it is known that, for $N \geqq 3$, there exists a universal family of elliptic curves with level N structure parametrized by an affine curve, whose function field K is the field of elliptic modular functions of level N in the sense of Igusa [**4**] (cf. Igusa [**5**], Deligne [**1**], Mumford [**9**]). We call the generic member of this universal family *the generic elliptic curve with level N structure*, which is an elliptic curve defined over K. For the case $N=4$, we shall explicitly construct the universal family in § 3.

§ 2. Level 2 structures.

Let k be a field of characteristic $\neq 2$ and let E be an elliptic curve with origin o. We denote by $[u]$ the divisor corresponding to a point u of E. Then a divisor $\sum m_i[u_i]$ is a principal divisor if and only if $\sum m_i=0$ and $\sum m_i u_i=0$ (Abel's theorem). Moreover if a principal divisor is k-rational, it is the divisor of a function defined over k.

Now let (E, v, w) be a level 2 structure on E, defined over k (cf. Igusa [**4**] p. 454-455). Then there exists a unique function X on E (defined over k) such that

$$(X)=2[v]-2[o], \qquad X(w)=1. \tag{2.1}$$

If we put

$$\lambda=\lambda(E, v, w)=X(v+w), \tag{2.2}$$

then $\lambda \neq 0, 1, \infty$ and we have

$$(X-1)=2[w]-2[o], \qquad (X-\lambda)=2[v+w]-2[o]. \tag{2.3}$$

On the other hand, there is a function Y on E (defined over k) such that

$$(Y)=[v]+[w]+[v+w]-3[o]. \tag{2.4}$$

Hence we have

$$cY^2=X(X-1)(X-\lambda), \tag{2.5}$$

with some constant $c \in k$, $c \neq 0$. (Note that c may not be a square in k.) The map

$$u \longmapsto (X(u), Y(u), 1)$$

defines an imbedding of E into $\boldsymbol{P}^2$, the image being the non-singular cubic curve (2.5) considered in $\boldsymbol{P}^2$. The origin o is mapped to the (unique) point at infinity (0, 1, 0), and the points of order 2 v, w and $v+w$ of E are mapped respectively to the points with coordinates

$$(X, Y)=(0, 0),\ (1, 0),\ (\lambda, 0).$$

The inversion and translations by points of order 2 of E are represented as follows in the coordinates X, Y:

$$X(-u)=X(u), \qquad Y(-u)=-Y(u); \tag{2.6}$$

$$\begin{cases} X(u+v)=\lambda/X(u), \quad Y(u+v)=-\lambda Y(u)/X(u)^2; \\ X(u+w)=(X(u)-\lambda)/(X(u)-1), \quad Y(u+w)=(\lambda-1)Y(u)/(X(u)-1)^2; \\ X(u+v+w)=\lambda(X(u)-1)/(X(u)-\lambda), \quad Y(u+v+w)=-\lambda(\lambda-1)Y(u)/(X(u)-\lambda)^2. \end{cases} \tag{2.7}$$

We can prove these formulas simply by checking that both sides have the same divisor considered as functions of $u \in E$ and that they have the same value at a suitable point.

§ 3. Level 4 structures.

Now we consider a level 4 structure (E, r, s) defined over k. (We implicitly assume that k is a field of characteristic $\neq 2$, given with a fixed primitive 4-th root of unity $i=\sqrt{-1} \in k$ and that $e_4(r, s)=i$, cf. § 1.) The "underlying" level 2 structure $(E, 2r, 2s)$ of (E, r, s) determines a unique function X on E and some function Y, unique up to constants, satisfying (2.1), $\cdots$, (2.7) (with $v=2r$ and $w=2s$). We claim that Y can be uniquely normalized so that we have $c=1$ in (2.5). In fact, putting $u=r$ in (2.6) and $(2.7)_1$, we get $X(-r)=X(r)$, $X(r)^2=\lambda$. Hence, by (2.5), we have

$$cY(r)^2 = X(r)(X(r)-1)(X(r)-\lambda)$$
$$= \{iX(r)(X(r)-1)\}^2 .$$

Since, by assumption, $X(r)$ and $Y(r)$ are (non-zero) elements in k, it follows that c is a square in k. Therefore, replacing Y by $\sqrt{c}Y$, we can take $c=1$ in (2.5), i.e. we get the Legendre normal form of E:

$$Y^2 = X(X-1)(X-\lambda) . \tag{3.1}$$

The function Y on E is unique up to sign and we can uniquely normalize it by the condition:

$$Y(r) = iX(r)(X(r)-1) . \tag{3.2}$$

Summarizing, we have proved

PROPOSITION 1. *Let (E, r, s) be an elliptic curve with level 4 structure defined over a field k. Then there exists a unique pair of functions X, Y on E, defined over k, giving an isomorphism of E onto the non-singular cubic* (3.1) *and satisfying* (2.1), $\cdots$, (2.7) *and* (3.2) *with $v=2r$, $w=2s$ and $\lambda=X(2r+2s)$.*

We shall define the "level 4 invariant" or the "modulus" of a level 4 structure (E, r, s) by

$$\sigma = \sigma(E, r, s) = X(r)+i(X(s)-1) . \tag{3.3}$$

PROPOSITION 2. *Given a level 2 structure (E, v, w), there exist exactly four level 4 structures which have (E, v, w) as the underlying level 2 structure; if (E, r, s) is one of them, the other are given by*

$$(E, r, s+2r) , \qquad (E, r+2s, s) , \qquad (E, r+2s, s+2r) .$$

Moreover, if we put $\sigma=\sigma(E, r, s)$, then we have

$$\sigma(E, r, s+2r) = 1/\sigma , \qquad \sigma(E, r+2s, s) = -1/\sigma , \tag{3.4}$$
$$\sigma(E, r+2s, s+2r) = -\sigma .$$

PROOF. For a given (v, w), there are 16 pairs (r, s) of points of order 4 such that $2r=v$ and $2s=w$, and half of them satisfy the condition $e_4(r, s)=i$. Clearly, if (r, s) is a solution with $e_4(r, s)=i$, other solutions are given by $(r, s+2r)$; $(r+2s, s)$, $(r+2s, s+2r)$, and their "inverse" $(-r, -s)$, etc. Since (E, r, s) and $(E, -r, -s)$ are isomorphic level 4 structures, this proves the first assertion. To prove the second assertion, note that we can use the same function X on E to define σ. Putting $\alpha=X(r)$ and $\beta=X(s)$, we see from (2.7) (with $v=2r$, $w=2s$) that

$$\alpha^2=\lambda, \quad (\beta-1)^2=1-\lambda; \tag{3.5}$$
$$X(r+2s)=(\alpha-\lambda)/(\alpha-1)=-\alpha,$$
$$X(s+2r)-1=\lambda/\beta-1=-(\beta-1).$$

Now (3.4) follows from the definition (3.3), q. e. d.

PROPOSITION 3. *The invariants* $\sigma=\sigma(E, r, s)$ *and* $\lambda=\lambda(E, 2r, 2s)$ *are related by the formula:*

$$\lambda=\frac{1}{4}\left(\sigma+\frac{1}{\sigma}\right)^2. \tag{3.6}$$

In particular, σ *is different from* 0, ± 1, $\pm i$, ∞.

PROOF. With the notations in the above proof, we have $\lambda=\alpha^2$ and

$$\sigma=\alpha+i(\beta-1), \quad \frac{1}{\sigma}=\alpha-i(\beta-1), \tag{3.7}$$

hence the formula. The last assertion follows from $\lambda\neq 0, 1, \infty$, q. e. d.

PROPOSITION 4. *Let* (E, r, s) *be an elliptic curve with level* 4 *structure defined over* k, *and set* $\sigma=\sigma(E, r, s)$. *Then the coordinates of* r, s *are given by*

$$\begin{cases} r=((\sigma^2+1)/2\sigma,\ i(\sigma^2+1)(\sigma-1)^2/4\sigma^2), \\ s=((\sigma+i)^2/2i\sigma,\ \varepsilon(\sigma^2-1)(\sigma+i)^2/4\sigma^2), \end{cases} \tag{3.8}$$

the sign $\varepsilon=\pm 1$ *being determined by the condition* $e_4(r, s)=i$.

PROOF. Putting $\alpha=X(r)$ and $\beta=X(s)$ as before, we get

$$\alpha=\frac{1}{2}\left(\sigma+\frac{1}{\sigma}\right) \quad \text{and} \quad \beta-1=\frac{1}{2i}\left(\sigma-\frac{1}{\sigma}\right),$$

from (3.7). Then $Y(r)$ is given by (3.2), while we have from (3.1) and (3.5):

$$Y(s)^2=\beta(\beta-1)(\beta-\lambda)=\{\beta(\beta-1)\}^2,$$

hence $Y(s)=\pm\beta(\beta-1)$, in which the sign $\pm$ is determined by the condition $e_4(r, s)=i$, q. e. d.

Note that points of E of exact order 4 other than $\pm r$ and $\pm s$ are easily computed by the addition theorem on E (or by (2.6), (2.7)), and their coordinates are as follows:

$$(-(\sigma^2+1)/2\sigma,\ \pm i(\sigma^2+1)(\sigma+1)^2/4\sigma^2),$$
$$(-(\sigma-i)^2/2i\sigma,\ \pm(\sigma^2-1)(\sigma-i)^2/4\sigma^2), \tag{3.9}$$
$$((\sigma^2+1)/2,\ \pm(\sigma^4-1)/4\sigma),\ ((\sigma^2+1)/2\sigma^2,\ \pm(\sigma^4-1)/4\sigma^3).$$

Therefore we see that the smallest field of definition of an elliptic curve with level 4 structure (E, r, s) is given by $F(\sqrt{-1}, \sigma(E, r, s))$ where F is the prime field in a field of definition of E.

Following Igusa's treatment of the absolute invariant [4], we can state

PROPOSITION 5. *Let* (E, r, s) *and* (E', r', s') *be two elliptic curves with level 4 structure. Then*

i) (E, r, s) *and* (E', r', s') *are isomorphic if and only if* $\sigma(E, r, s)=\sigma(E', r', s')$.

ii) *If* (E', r', s') *is a specialization of* (E, r, s), $\sigma(E', r', s')$ *is the unique specialization of* $\sigma(E, r, s)$ *over this specialization.*[1]

PROOF. i) Since the only if part is clear, we prove the if part. Assume $\sigma(E, r, s)=\sigma(E', r', s')$. Then two structures have the same λ by (3.6); hence both E and E' are isomorphic to the same cubic (3.1) with the origin $(0, 1, 0)$. If we identify E, E' with the cubic, then Proposition 4 implies that

$$r=r' \quad \text{and} \quad s=\pm s' .$$

Since $e_4(r, s)=i=e_4(r', s')$, we must have $s=s'$, proving i).

ii) By the uniqueness of the function X on E, determined by a level 2 structure $(E, 2r, 2s)$, it follows that the similar function X' on E' is the unique specialization of X over the given specialization. Therefore

$$\sigma(E, r, s)=X(r)+i(X(s)-1)$$

is uniquely specialized to $\sigma(E', r', s')$, q. e. d.

COROLLARY. *The sign* ε *of* $Y(s)$ *in Proposition* 4 (3.8) *is independent of individual level* 4 *structure.*

Now we are ready to write down the universal family of elliptic curves with level 4 structure over k. We take a variable, $\tilde{\sigma}$, over k and consider the affine curve Δ':

$$\Delta'=\boldsymbol{P}^1-\{0, \pm 1, \pm i, \infty\} . \tag{3.10}$$

Let B' denote the subvariety of $\boldsymbol{P}^2\times\Delta'$ defined by the equation:

$$Y^2Z=X(X-Z)(X-\tilde{\lambda}Z), \tag{3.11}$$

where (X, Y, Z) is the homogeneous coordinates of $\boldsymbol{P}^2$ and $\tilde{\lambda}=(1/4)(\tilde{\sigma}+\tilde{\sigma}^{-1})^2$. Let Φ' denote the restriction to B' of the projection $\boldsymbol{P}^2\times\Delta'\rightarrow\Delta'$. Define the sections $\tilde{o}$, $\tilde{r}$, and $\tilde{s}$ of Φ': $B'\rightarrow\Delta'$ by $\tilde{o}=(0, 1, 0)$ and by the formulas (3.8) with σ replaced by $\tilde{\sigma}$. Summarizing the above arguments and noting that a level 4 structure admits no non-trivial automorphism, we have proved

THEOREM 1. *The fibre system* Φ': $B'\rightarrow\Delta'$, *together with sections* $\tilde{r}$, $\tilde{s}$ *of order* 4, *is the universal family of elliptic curves with level* 4 *structure.*

REMARK. 1) Note that B' is a non-singular quasi-projective surface and that both B' and Δ' can be defined over $F(i)$, the prime field F adjoined by

1) As in [4], we can allow unequal characteristic specialization in ii), provided that we fix $i=\sqrt{-1}$ in a compatible way in the fields under consideration.

$i=\sqrt{-1}$.

2) We also remark that the function field of the base curve Δ', $k(\tilde{\sigma})$, is the field of elliptic modular functions of level 4 as defined by Igusa [4], cf. p. 467-468.

3) Actually we can see that the fine moduli scheme of elliptic curves with level 4 structure exists and is given by the affine scheme:

$$M=\operatorname{Spec} \boldsymbol{Z}[\sqrt{-1}, \tilde{\sigma}, 1/2\tilde{\sigma}(\tilde{\sigma}^4-1)],$$

cf. Igusa [5], Deligne [1], Mumford [9] Ch. 7. For each field k with a primitive 4-th root of unity, our curve Δ' is obtained as $M \underset{\boldsymbol{Z}[i]}{\otimes} k$.

§ 4. Elliptic modular surface of level 4.

Let k be a field of characteristic $p \neq 2$ containing a primitive 4-th root of unity $i=\sqrt{-1}$, and let σ be a variable over k (instead of $\tilde{\sigma}$ of § 3). We put $K=k(\sigma)$. Consider the elliptic curve

(4.1) $$E: Y^2=X(X-1)(X-\lambda), \qquad \lambda=(1/4)(\sigma+1/\sigma)^2,$$

over K; E is nothing but the generic fibre of the universal family Φ': $B' \to \Delta'$ of elliptic curves with level 4 structure, discussed in § 3. We denote by $E(K)$ the group of K-rational points of E. Then it is clear that we have

(4.2) $$E(K) \supset E_4 = \text{the group of points of } E \text{ of order } 4,$$

cf. Proposition 4 of § 3.

We mention here another normal form of E known as Jacobi quartic (cf. [3]):

(4.3) $$C: y^2=(1-\sigma^2x^2)(1-x^2/\sigma^2).$$

Actually the curve C has a singular point at infinity and it is transformed to the non-singular cubic E by the birational transformation (over K):

(4.4) $$X=\frac{\sigma^2+1}{2\sigma^2} \cdot \frac{x-\sigma}{x-1/\sigma}, \qquad Y=\frac{\sigma^4-1}{4\sigma^3} \cdot \frac{y}{(x-1/\sigma)^2}.$$

On Jacobi quartic C, the points of order 4 have simple coordinates; their x-coordinates are just

$$\pm\sigma,\ \pm 1/\sigma,\ 0,\ \pm 1,\ \pm i,\ \infty, \qquad (\text{cf. } (3.8), (3.9)).$$

Sometimes it is easier to find K-rational points of C than that of E; in fact, this was how we first found K-rational points of infinite order in the case $p=3$ (cf. § 5).

Now we consider the Kodaira-Néron model of the elliptic curve E over the function field $K=k(\sigma)$, cf. [7], [**10**]. It is a non-singular projective surface, B, defined over k obtained as a compactification of the quasi-projective surface B'. Moreover B has a natural projection $\Phi: B\to \boldsymbol{P}^1$, which is an extension of $\Phi': B'\to \Delta'$. Putting $\Sigma=\boldsymbol{P}^1-\Delta'=\{0, \pm 1, \pm i, \infty\}$ (cf. (3.10)), we consider the singular fibre $C_v=\Phi^{-1}(v)$ over $v\in\Sigma$:

$$B=B'\cup(\bigcup_{v\in\Sigma}C_v). \tag{4.5}$$

PROPOSITION 6. *Each singular fibre C_v $(v\in\Sigma)$ is composed of* 4 *non-singular rational curves $\Theta_{v,i}$ $(i=0, 1, 2, 3)$ intersecting like* ♯, *i.e. it is of type I_4 in Kodaira's notation* [**7**] p. 604 (*or of type b_4 in Néron's notation* [**10**] p. 124). *Moreover each curve $\Theta_{v,i}$ in B is defined over K.*

PROOF. The absolute invariant j of our elliptic curve E is given as follows (cf. [4] p. 455):

$$j=2^8(\lambda^2-\lambda+1)^3/\lambda^2(\lambda-1)^2=2^4(1+14\sigma^4+\sigma^8)^3/\sigma^4(\sigma^4-1)^4. \tag{4.6}$$

Therefore each point v of Σ is a pole of order 4 of j, and the singular fibre C_v is either of type I_4 or I_4^* $(=c5_4$ in [**10**]). On the other hand, the torsion subgroup of $E(K)$ contains the group E_4 of points of order 4 (4.2), which excludes the possibility of I_4^* (cf. [EMS], Remark 1.10). Of course, we could prove this directly without using (4.2), but our proof applies also for general level N case ([EMS] Appendix). The last assertion follows from the explicit construction of C_v (cf. [**10**], III-10), q.e.d.

COROLLARY. *The torsion subgroup of $E(K)$ is equal to E_4.*

THEOREM 2. *Assume $k=\boldsymbol{C}$. Then the algebraic surface B is a $K3$ surface, biholomorphic* (*over $\boldsymbol{P}^1$*) *to the elliptic modular surface of level* 4, $B(4)$, *in the sense of* [*EMS*] (*see* p. 38 *and* p. 50). *In particular, the first and second Betti numbers of B are given by*

$$b_1=0, \qquad b_2=22. \tag{4.7}$$

PROOF. We denote by c_2, p_g and q respectively the Euler number, the geometric genus and the irregularity of B. Then, applying theorems of Kodaira [7] § 12, we have

$$c_2=12(p_g-q+1)=24 \qquad \text{and} \qquad q=0.$$

This implies $p_g=1$, $b_1=2q=0$, $b_2=c_2+2b_1-2=22$ and also the triviality of the canonical bundle of B. Therefore B is a $K3$ surface. On the other hand, let E' denote the generic fibre of $B(4)$ over $\boldsymbol{P}^1$. E' is an elliptic curve defined over the field, K', of elliptic modular functions of level 4 and we have $E'(K')=E_4'$ by [EMS] Theorem 5.5. Then there is an isomorphism of $K=\boldsymbol{C}(\sigma)$ onto K' (over $\boldsymbol{C}$), sending the element $j\in K$ of (4.6) to 12^3-times ordinary elliptic modular function (of level 1) $j(z)$. When we identify K with K', both

E and E' have the same absolute invariant j, and hence they are isomorphic over some extension of K. Since we know that both $E(K)$ and $E'(K)$ contain all points of order 4, the isomorphism of E onto E' is unique and defined over K, cf. § 3. By the uniqueness of Kodaira-Néron model, the elliptic surfaces B and $B(4)$ are biholomorphic over $\boldsymbol{P}^1$, q. e. d.

COROLLARY. *If k is a field of characteristic* 0, *then*

$$E(K)=E_4 .$$

Going back to general case, we shall call the surface B in characteristic $p\neq 2$ *the elliptic modular surface of level* 4 *in characteristic* p (defined over k), and write $B=B_p$ if necessary. Now, for a non-singular algebraic surface V in an arbitrary characteristic, Igusa [**6**] defined its Betti numbers $b_\nu(V)$ and proved the inequality:

$$\rho(V)\leqq b_2(V)\,, \tag{4.8}$$

$\rho(V)$ being the Picard number of V. In our case, by a similar argument to the proof of Theorem 2, we have (cf. [**11**] p. 20)

$$b_1(B_p)=0\,,\qquad b_2(B_p)=22\,. \tag{4.9}$$

Another way to prove (4.9) is to reduce it to (4.7) by observing first that the surface B_p is obtained as reduction mod p of the corresponding surface B_0 in characteristic 0 and that Igusa's Betti numbers are the same as those defined by means of l-adic cohomology (cf. [**2**] 3.8).

On the other hand, the Picard number of B_p is given by the formula (cf. [EMS] Corollary 1.5):

$$\rho(B_p)=\text{rank}\,E(K)+20\,, \tag{4.10}$$

since there are 6 singular fibres of type I_4. Combining (4.10) with (4.8) and (4.9), we get

PROPOSITION 7. *The rank of $E(K)$ is at most* 2.

We note that, if $p=0$, we can use the stronger inequality $\rho\leqq b_2-2p_g$ instead of (4.8), implying the finiteness of the group $E(K)$. Note also that the above argument can be applied to the case of any level $N\geqq 3$, giving the upper bound of the rank of $E(K)$ stated in the introduction.

§ 5. The group $E(K)$ in the case $p>0$.

We use the same notations as in § 4, except that we now assume k is the finite field $\boldsymbol{F}_q$, where

$$q=p \qquad \text{or} \qquad p^2 \tag{5.1}$$

according as $p\equiv 1 \bmod 4$ (case a) or $p\equiv 3 \bmod 4$ (case b). In this case, $B=B_p$

is a non-singular projective surface defined over $\boldsymbol{F}_q$ and its zeta function is given by

$$\zeta(B, T) = 1/(1-T)\cdot(1-qT)^{20} H_{3,q}(T)\cdot(1-q^2T), \tag{5.2}$$

where $H_{3,q}(T)$ is the polynomial

$$H_{3,q}(T) = \begin{cases} (1-\pi^2 T)(1-\pi'^2 T) & \text{(case a)}, \\ (1-qT)^2 & \text{(case b)}, \end{cases} \tag{5.3}$$

associated with the Hecke polynomial of level 4 and of weight 3. (Here π, π' are integers of $\boldsymbol{Z}[i]$ such that $p=\pi\pi'$, $\pi\equiv 1 \bmod 2i$.) We proved this result in [EMS], Appendix (esp. p. 56-57), where we made use of some results explained in the previous section. We note that the zeta function $Z_E(s)$ of the elliptic curve E defined over the function field $K=\boldsymbol{F}_q(\sigma)$, as defined in [**15**], p. 142, is equal to the main part of the zeta function of B:

$$Z_E(s) = H_{3,q}(q^{-s}). \tag{5.4}$$

We recall here the conjecture of Birch and Swinnerton-Dyer on the rank of the group of rational points of an elliptic curve defined over a global field, and the conjecture of Tate on the Picard number of a surface defined over a finite field, cf. [**13**]. In our notations, their conjectures are:

(5.5)*[2] $\quad \operatorname{rank} E(K) = \text{order of zero of } Z_E(s) \text{ at } s=1,$

(5.6)* $\quad \rho(B) = \text{order of pole of } \zeta(B, T) \text{ at } T=q^{-1}.$

Hence, in our case, these two conjectures are equivalent by (4.10), (5.2) and (5.4) and they claim:

(5.7)* $\quad \operatorname{rank} E(K) = \begin{cases} 0, \\ 2, \end{cases} \quad \rho(B) = \begin{cases} 20 & \text{(case a)}, \\ 22 & \text{(case b)}. \end{cases}$

Moreover, the formula (4.10) implies the validity of these conjectures in (case a). In view of Corollary to Proposition 6, we have

THEOREM 3. *Assume* $p\equiv 1 \bmod 4$. *Then*

i) *The group* $E(K)$ *of* K*-rational points of the generic elliptic curve* E *with level* 4 *structure in characteristic* p *consists exactly of points of order* 4 *of* E.

ii) *The Picard number of the elliptic modular surface of level* 4 *in characteristic* p *is equal to* 20.

(Note that in the above theorem we may replace the constant field $\boldsymbol{F}_p$ by an arbitrary field k of the same characteristic, as we can see by a standard argument.)

For the remaining (case b), we restate (5.7):

2) * marked to indicate that these are conjectures!

CONJECTURE. If $p\equiv 3 \bmod 4$, then

$$\text{rank } E(K)=2 \quad \text{and} \quad \rho(B)=22\,. \tag{5.8}$$

The rest of this section is devoted to the proof of this conjecture in the special case $p=3$. First the quotient group $E(K)/2E(K)$ is a finite group of type $(2, \cdots, 2)$, i.e. a vector space over $\boldsymbol{F}_2=\boldsymbol{Z}/2\boldsymbol{Z}$, whose dimension is $2+\text{rank } E(K)$, because $E(K)$ contains the group E_2 of points of order 2. Therefore (5.8) is equivalent to

$$\dim_{\boldsymbol{F}_2} E(K)/2E(K)=4\,, \tag{5.9}$$

the inequality $\leqq$ being true by Proposition 7. Next, for any element α of the multiplicative group $K^\times$ of the field K, we denote by $\text{cl}(\alpha)$ the class of α modulo the subgroup $(K^\times)^2$ of squares in $K^\times$. The following lemma is a crucial point in the proof of the so-called weak Mordell-Weil theorem (cf. [8] Chapter 16):

LEMMA. *Let φ denote the map of $E(K)$ into the group $K^\times/(K^\times)^2 \oplus K^\times/(K^\times)^2$ defined by*

$$\varphi(u)=(\text{cl}(X(u)),\ \text{cl}(X(u)-1))\,, \qquad u=(X(u),\ Y(u))\in E(K)\,.$$ [3]

Then the map φ induces an injective homomorphism:

$$E(K)/2E(K) \hookrightarrow K^\times/(K^\times)^2 \oplus K^\times/(K^\times)^2\,. \tag{5.10}$$

PROPOSITION 8. *Assume $p=3$. Then the following points u and v are K-rational points of E:*

$$\begin{aligned} u&=(\sigma^2,\ \sigma^2-1)\,,\\ v&=((1-i)(\sigma-i)\,,\ (1+i)(\sigma+1)(\sigma-i)(\sigma-1+i)/\sigma)\,. \end{aligned} \tag{5.11}$$

Letting r, s denote the points of order 4 of E given by (3.8), *the four points u, v, r and s induce a basis of $E(K)/2E(K)$ over $\boldsymbol{F}_2=\boldsymbol{Z}/2\boldsymbol{Z}$.*

PROOF. The first assertion can be verified by computation. To prove the second assertion, we form the table:

	$X(u)$	$X(u)-1$
u	σ^2	σ^2-1
v	$(1-i)(\sigma-i)$	$(1-i)(\sigma+1)$
r	$(\sigma^2+1)/2\sigma$	$(\sigma-1)^2/2\sigma$
s	$(\sigma+i)^2/2i\sigma$	$(\sigma^2-1)/2i\sigma$

Suppose there is a relation:

3) When $X(u)=0$, 1 or ∞, the definition of $\varphi(u)$ must be suitably modified.

$$n_1u+n_2v+n_3r+n_4s\equiv 0 \mod 2E(K).$$

By the above lemma (5.10), this is equivalent to

$$(5.12)\qquad \begin{cases} (\sigma^2)^{n_1}\{(1-i)(\sigma-i)\}^{n_2}\{(\sigma^2+1)/2\sigma\}^{n_3}\{(\sigma+i)^2/2i\sigma\}^{n_4}\in (K^\times)^2, \\ (\sigma^2-1)^{n_1}\{(1-i)(\sigma+1)\}^{n_2}\{(\sigma-1)^2/2\sigma\}^{n_3}\{(\sigma^2-1)/2i\sigma\}^{n_4}\in (K^\times)^2. \end{cases}$$

Since $K=k(\sigma)$ is the quotient field of the polynomial ring $k[\sigma]$ (a UFD), it follows from (5.12) that

$$n_1\equiv n_2\equiv n_3\equiv n_4\equiv 0 \qquad \mod 2.$$

This completes the proof (cf. (5.9)), q. e. d.

Actually the hardest part was to find K-rational points u, v. It is likely that these u, v, r and s generate the whole group $E(K)$. At any rate, we obtain

THEOREM 4. *Assume $p=3$. Then the group $E(K)$ of K-rational points of the generic elliptic curve E with level 4 structure in characteristic 3 is an infinite group of rank 2, whose torsion subgroup consists of points of order 4, i.e.*

$$E(K)\cong \boldsymbol{Z}\oplus\boldsymbol{Z}\oplus\boldsymbol{Z}/4\boldsymbol{Z}\oplus\boldsymbol{Z}/4\boldsymbol{Z}.$$

REMARK. Let N be a natural number divisible by 4 and let K_N denote the field of elliptic modular functions of level N in characteristic p ($p\nmid N$), cf. [4]. We have

$$K_N\supset K_4=K=k(\sigma)\supset K_2=k(\lambda).$$

It follows from the results of § 3 that the generic elliptic curve with level N structure is again given by the Legendre cubic

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

considered now over the field K_N. We have

$$E(K_N)\supset E(K_4)\supset E(K_2)=E_2,$$

the last equality being a result of Igusa [4] p. 463. (It can also be proved by the method used in § 4.) Therefore Theorem 4 implies the following partial result for higher level case:

COROLLARY. *Let N be a natural number divisible by 4 and not divisible by 3. Then the group of K_N-rational points of the generic elliptic curve with level N structure in characteristic 3 is an infinite group of rank $\geqq 2$.*

We close this paper by raising a question. What is the true meaning of rational points of infinite order on the generic elliptic curve with level N structure in certain characteristic p?

Department of Mathematics
University of Tokyo
Hongo, Bunkyo-ku
Tokyo, Japan

References

[1] P. Deligne, Formes modulaires et représentations l-adiques, Sém. Bourbaki, 1968/69, exp. 355, 1–33.

[2] A. Grothendieck, Le groupe de Brauer II, Sém. Bourbaki, 1965/66, exp. 297, 1–21.

[3] J. Igusa, On the transformation theory of elliptic modular functions, Amer. J. Math., **81** (1959), 436–452.

[4] J. Igusa, Fibre systems of Jacobian varieties (III. Fibre systems of elliptic curves), Amer. J. Math., **81** (1959), 453–476.

[5] J. Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math., **81** (1959), 561–577.

[6] J. Igusa, Betti and Picard numbers of abstract algebraic surfaces, Proc. Nat. Acad. Sci., **46** (1960), 724–726.

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

[8] L. J. Mordell, Diophantine equations, Academic Press, London and New York, 1969.

[9] D. Mumford, Geometric invariant theory, Springer-Verlag, Berlin-Heidelberg-New York, 1965.

[10] A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. I. H. E. S., No. 21, 1964.

[11] A. P. Ogg, Elliptic curves and wild ramification, Amer. J. Math., **89** (1967), 1–21.

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

[13] J. Tate, On the conjecture of Birch and Swinnerton-Dyer and a geometric analog, Sém. Bourbaki, 1966, exp. 306, 1–26.

[14] A. Weil, Variétés abéliennes et courbes algébriques, Hermann, Paris, 1948.

[15] A. Weil, Dirichlet series and automorphic forms, Lecture notes No. 189, Springer, 1970.

Added in proof. Recently we have proved the conjecture in § 5 (5.8) for all prime number p such that $p \equiv 3 \bmod 4$. The method of the proof is different from that of § 5, and depends on the fact that our surface B (elliptic modular surface of level 4) is a Kummer surface. This result will be published in "Algebraic cycles on certain $K3$ surfaces in characteristic p" (in preparation).