Doi, K.
Osaka Math. J.
15 (1963), 249-256.

ON THE JACOBIAN VARIETIES OF THE FIELDS OF ELLIPTIC MODULAR FUNCTIONS

BY

KOJI DOI

In his essay [9, §16, p. 75], G. Shimura proposed to push further the problem studied by Hecke [3, p. 731-772] on the decomposition of the jacobian variety corresponding to a modular function field into simple factors (in the sense of isogeny). He asked especially to investigate the property of these simple factors. For instance, do there appear abelian varieties of dimension greater than 1 among them? As we shall describe in the following, there do appear such abelian varities; in fact, there are examples of elliptic modular function fields (of genus 2) for which we can prove that the corresponding jacobian varieties are simple. The result is achieved by calculating the ring of endomorphisms of these jacobian varieties. (It is well-known that an abelian variety is simple if and only if the ring of endomorphisms is a division algebra.) Our result is that the rings of endomorphisms of the jacobian varieties of the elliptic modular function fields corresponding to the groups $\Gamma_0(22)$, $\Gamma_0(23)$, $\Gamma_0(29)$ and $\Gamma_0(31)$ are $M_2(\boldsymbol{Q})$, $\boldsymbol{Q}(\sqrt{5})$, $\boldsymbol{Q}(\sqrt{2})$ and $\boldsymbol{Q}(\sqrt{5})$ respectively, where the modular group $\Gamma_0(N)$ is defined by

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \boldsymbol{Z})\,;\ c \equiv 0 \mod N\right\}.$$

This result shows that the corresponding jacobian varieties $J_{\Gamma_0(q)}$ are simple for $q=23, 29, 31$. We note that the method employed in the following is applicable to other cases of higher genus and various modular groups (other than $\Gamma_0(N)$).

To carry out our calculation of rings of endomorphisms, we have to make use of *the congruence relation* due to M. Eichler and G. Shimura:

$$T_p = \Pi_p + \Pi_p' \circ R_p \mod p$$

for the modular correspondences, and *the trace formula* due to M. Eichler and A. Selberg, for the Hecke operators T_p. Namely, we can calculate from these results the characteristic polynomial of the l-adic representation $M_l(\pi_p)$ of π_p, where π_p is the p-th power endomorphism of $\tilde{J}_{\Gamma_0(N)}$ (the reduction of $J_{\Gamma_0(N)}$ mod p), as indicated in [7, p. 328].

Notation and Convention. We denote by $\boldsymbol{Z}$ and $\boldsymbol{Q}$ respectively, the ring of rational integers and the rational number field. $\mathcal{A}(A)$ and $\mathcal{A}_0(A)$ denote the ring of endomorphisms of an abelian variety A and the algebra $\mathcal{A}(A)\otimes\boldsymbol{Q}$, respectively, According to Hecke, we denote by $\Gamma^*(N)$ the group generated by $\Gamma_0(N)$ and $\begin{pmatrix}0 & -1\\ N & 0\end{pmatrix}$. The genera of the groups $\Gamma_0(N)$ and $\Gamma^*(N)$, which we denote by $p_0(N)$ and $p^*(N)$, are calculated in [3]. In particular, we have (Fricke [2, p. 366]):

$$p^*(N) = \frac{1}{2}p_0(N)+\frac{1}{2}-\frac{1}{4}\cdot\delta_N\cdot h(4N)\,,$$

where

$$\delta_N = \begin{cases} 2 & \text{for } N\equiv 7 \mod 8 \\ \dfrac{4}{3} & \text{for } N\equiv 3 \mod 8 \quad (N\geqq 5) \\ 1 & \text{otherwise}\,, \end{cases}$$

and $h(4N)$ is the class number of primitive positive quadratic forms with the discriminant $-4N$. For the sake of convenience, we recall here Fricke's table of $p_0(N)$ and $p^*(N)$ [2, p. 357 and p. 367].

$p_0(N)=0$	:	$N=$	2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25.
$p_0(N)=1$	:	$N=$	11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49.
$p_0(N)=2$	:	$N=$	22, 23, 26, 28, 29, 31, 37, 50.
$p_0(N)=3$	:	$N=$	30, 33, 34, 35, 39, 40, 41, 43, 45, 48, 64.
$p_0(N)=4$	:	$N=$	38, 44, 47, 53, 54, 61.
$p_0(N)=5$	:	$N=$	42, 46, 51, 52, 55, 56, 57, 59, 63, 65, 67, 72.
$p_0(N)=6$	:	$N=$	58, 71.
$p_0(N)=7$	:	$N=$	60, 62, 68, 69.
$p_0(N)=9$	:	$N=$	66, 70.
$p^*(N)=0$	for	$N=$	2, 3, $\cdots$, 21, 23, 24, 25, 26, 27, 29, 31, 32, 35, 36, 39, 41, 47, 49, 50, 71.

The author wishes to express his sincere thanks to Prof. G. Shimura, and also to Prof. M. Sato who encouraged him with many suggestions.

§ 1. **Preliminaries.** We deal with the group $\Gamma_0(N)$ and restrict ourselves to the case $p_0(N)=2$. We remark that in the case of our $\Gamma_0(N)$

the congruence relation takes the simpler form:

(1) $$T_p = \Pi_p + \Pi_p' \mod p,$$

or equivalently,

(2) $$\tilde{\xi}_p = \pi_p + \pi_p' ,$$

where ξ_p is the element of $\mathcal{A}_0(J_{\Gamma_0(N)})$ corresponding to T_p and $\tilde{\xi}_p$ is the reduction of ξ_p mod p. We assume (throughout this note) that p is not one of those exceptional primes (in finite number) for which either $p|N$ holds or the validity of the equivalence between (1) and (2) is destroyed, i.e. exceptional primes are, by the precise result of Igusa [4], and also by [5], $p|2\cdot 3\cdot N$.

Lemma 1. *Tne eigenvalues $\tau_{p,i}$ $(i=1,2)$ of a Hecke operator T_p acting on the space of cusp-forms of degree 2 with respect to $\Gamma_0(N)$ satisfies the quadratic equation*:

$$X^2-(Tr(T_p))X+\frac{(Tr(T_p))^2-Tr(T_{p^2})-2p}{2}=0,$$

where $Tr(T_p)$ is the trace of the operator T_p.

Proof. We have a fundamental relation for operators T_p acting on the space of modular forms of degree k (cf. [3, p. 676]):

$$T_{p^r}\circ T_p = T_{p^{r+1}}+p^{k-1}R_p\circ T_{p^{r-1}} \qquad (r\geqq 1)$$

in which we can put $R_p=1$ in the present case. Setting $r=1$ and $k=2$ and taking the trace, we obtain

$$Tr(T_p^2) = Tr(T_{p^2})+2p.$$

Our assertion is an immediate consequeuce of this identity.

We can calculate eigenvalues of T_p in the case of higher genus by the same arguments using elementary relations between symmetric polynomials.

Lemma 2. *Notations and assumptions being as in Lemma 1, let π_p be the p–th power endomorphism of the jacobian variety $\tilde{J}_{\Gamma_0(N)}$. Denoting with $\pi_{p,j}$ $(j=1,2,3,4)$ the eigenvalues of an l–adic representation $M_l(\pi_p)$, they are the solutions of*

$$X^2-\tau_{p,i}X+p=0, \qquad i=1,2$$

in pairs.

Proof. Let M^d be a representation of $\mathcal{A}(J_{\Gamma_0(N)})$ by the differential forms of the first kind. Then M_l is equivalent to $M^d \oplus \bar{M}^d$ where $\bar{M}^d$ denotes the complex conjugate representation of M^d. For a prime $l \neq p$, we can choose an l-adic representation M_l so that $M_l(\mu) = M_l(\tilde{\mu})$ for every $\mu \in \mathcal{A}(J_{\Gamma_0(N)})$ and its reduction $\tilde{\mu}$ mod p. Our assertion follows from the fact that $M^d(\xi_p)$ can be considered as a representation of T_p for the cusp-forms of degree 2 with respect to $\Gamma_0(N)$ and from the relations

$$\tilde{\xi}_p = \pi_p + \pi_p{}',$$
$$\pi_p \circ \pi_p{}' = p \cdot \delta_{\tilde{J}_{\Gamma_0(N)}}.$$

§2. Criterion for $J_{\Gamma_0(N)}$ to be simple. The idea of this section is applicable to the case of higher genus by a slight modification.

Notations and assumptions being as §1, let p be a prime number satisfying the conditions of §1 and let $\tau_{p,i}$ be eigenvalues of T_p. Then, for a given $\Gamma_0(N)$, each $\tau_{p,i}$ is either a rational integer or a real quadratic integer (cf. [6, the remarks to the corollary of Th. 3, p. 308]).

Now we shall state the key theorem for the criterion for $J_{\Gamma_0(N)}$ to be simple.

Shimura's criterion:

(i) *$J_{\Gamma_0(N)}$ is simple if there exists a prime p (which is not exceptional in the sense of* §1) *such that*

(Pi) $[\boldsymbol{Q}(\tau_{p,i}) : \boldsymbol{Q}] = 2, \quad i = 1, 2;$

(Pii) $[\boldsymbol{Q}(\pi_{p,j}) : \boldsymbol{Q}] = 4, \quad j = 1, 2, 3, 4;$

(Piii) $\boldsymbol{Q}(\pi_{p,j})/\boldsymbol{Q}$ *is not a normal extension*;

(Piv) *For any positive rational integer m, $\pi_{p,j}^m \notin \boldsymbol{Q}(\tau_{p,i})$.*

(ii) *If there are two primes p_1, p_2 for which* (i) *is true and such that* $\boldsymbol{Q}(\pi_{p_1,j}) \neq \boldsymbol{Q}(\pi_{p_2,j})$ *then* $\mathcal{A}_0(J_{\Gamma_0(N)}) \cong \boldsymbol{Q}(\pi_{p_1,i})$ $(= \boldsymbol{Q}(\tau_{p_2,i}))$.

Here we shall add one more lemma which is convenient to know whether $\pi_{p,j}$ satisfies the condition (Piv) or not.

Lemma 3. *Let p be a prime number which satisfies* (Pi) *and remains prime in $\boldsymbol{Q}(\tau_{p,i})$. If $\pi_{p,j}^m \in \boldsymbol{Q}(\tau_{p,i})$ for some positive integer m, then $\pi_{p,j} = \sqrt{p} \cdot \zeta$ where ζ is a root of unity.*

Proof. Let $\bar{\pi}_{p,i}$ be the conjugate of $\pi_{p,i}$ over $\boldsymbol{Q}(\tau_{p,i})$ i.e. $\bar{\pi}_{p,i} = \pi_{p,j}$ for some j $(1 \leq j \leq 4)$. Then $\bar{\pi}_{p,i}$ is the complex conjugate of $\pi_{p,i}$. If we put $\pi_{p,i}^m = \gamma \in \boldsymbol{Q}(\tau_{p,i})$, we have

$$\pi_{p,i}^m \cdot \bar{\pi}_{p,i}^m = (\pi_{p,i} \cdot \bar{\pi}_{p,i})^m = \gamma^2$$

because $\boldsymbol{Q}(\tau_{p,i})$ is real. On the other hand, by Lemma 2, $\pi_{p,i}\cdot\bar{\pi}_{p,i}=p$, so that $p^m=\gamma^2$. From this and by the assumption that p remains prime in $\boldsymbol{Q}(\tau_{p,i})$, $\gamma=\varepsilon\cdot p^k$, where ε is a unit in $\boldsymbol{Q}(\tau_{p,i})$ and $\varepsilon^2=1$, $2k=m$. Hence we have $\pi_{p,i}^{2k}=\pm p^k$, so that $\pi_{p,i}=\zeta\cdot\sqrt{p}$.

For the proof of the above criterion, we need

Proposition [8, Prop. 30, p. 40]). *Let A be an abelian variety of dimension n. If $\mathcal{A}_0(A)$ contains a field F of degree $2n$ over $\boldsymbol{Q}$, then A is isogenous to a product $B\times\cdots\times B$ with a simple abelian variety B; the commutator of F in $\mathcal{A}_0(A)$ coincides with F.*

Proof of the criterion. By (Piii), $\boldsymbol{Q}(\pi_{p,j})/\boldsymbol{Q}$ is not a normal extension of degree 4 over $\boldsymbol{Q}$, so that $\boldsymbol{Q}(\pi_{p,j}^m)$ must coincide with $\boldsymbol{Q}(\pi_{p,j})$ or $\boldsymbol{Q}(\pi_{p,i})$ (cf. [8, p. 74, (c)]. The latter case does not occur by (Piv). Hence

$$\boldsymbol{Q}(\pi_{p,j}) = \boldsymbol{Q}(\pi_{p,j}^m),\ [\boldsymbol{Q}(\pi_{p,j}^m):\boldsymbol{Q}] = 4\,.$$

For any element $\alpha\in\mathcal{A}_0(\tilde{J}_{\Gamma_0(N)})$, we can choose a positive integer m such that α is defined over the finite field $GF(p^m)$ and hence $\alpha\circ\pi_p^m=\pi_p^m\circ\alpha$. By the above proposition, we have $\alpha\in\boldsymbol{Q}(\pi_{p,j}^m)$. This shows that

$$\mathcal{A}_0(\tilde{J}_{\Gamma_0(N)}) = \boldsymbol{Q}(\pi_{p,j})\,.$$

Therefore $\tilde{J}_{\Gamma_0(N)}$, and hence $J_{\Gamma_0(N)}$, is simple. The second part of the criterion is obvious by the theory of reduction mod p for the endomorphism-algebra of abelian variety.

§ 3. **Numerical examples.** Now we shall apply our results to the cases where $N=22, 23, 29, 31, 37$, the genera of corresponding $\Gamma_0(N)$ being equal to 2. We shall denote, as usual, by $\Delta(z)$ the cusp-form of degree 12 with respect to $\Gamma(1)=SL(2,\boldsymbol{Z})$:

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}\,,\qquad q = e^{2\pi i z}\,.$$

The case $N=22$ ($p^*(22)=1$). In this case $J_{\Gamma_0(22)}$ is isogenous to a product of two elliptic curves; this is easily seen by the relations

$$\Gamma^*(N)\supset\Gamma_0(N)\,,\ p_0(22) = 2 \quad\text{and}\quad p^*(22) = 1\,,$$

and by the general theory for algebraic curves and their jacobian varieties. Moreover, we can infer more detailed fact as follows. The space of cusp-forms of degree 2 with respect to $\Gamma_0(22)$ is spanned by $f(z)$, $f(2z)$, where

$$f(z) = \sqrt[12]{\Delta(z)\Delta(11z)}$$
$$= q-2q^2-q^3+2q^4+q^5+2q^6-2q^7+0\cdot q^8+\cdots .$$

This shows $J_{\Gamma_0(22)}$ is isogenous to a product $E\times E$ with the elliptic curve E corresponding to $\Gamma_0(11)$ which has no complex multiplication (Remark; the eigenvalues of T_p are multiple and contained in $\boldsymbol{Q}$).

The case $N=23$ ($p^*(23)=0$). Eigenvalues of T_p are contained in $\boldsymbol{Q}(\sqrt{5})$ (cf. [3, p. 903]). For $p=7$, 17 we have $\left(\frac{5}{p}\right)=-1$, i.e. they remain prime in $\boldsymbol{Q}(\sqrt{5})$. By the trace formula (cf. for the case $\Gamma_0(N)$, [1, (30), (30a) and (31), p. 165]) and lemma 1, 2, we have

$$\tau_{7,i} = 1\pm\sqrt{5}\ (i=1,2), \qquad \pi_{7,j} = \frac{\tau_{7,i}\pm\sqrt{\tau_{7,i}^2-28}}{2} \quad (j=1,2,3,4),$$

$$\tau_{17,i} = 3\pm\sqrt{5}\ (i=1,2), \qquad \pi_{17,j} = \frac{\tau_{17,i}\pm\sqrt{\tau_{17,i}^2-68}}{2} \quad (j=1,2,3,4).$$

By simple calculation, we can see that they satisfy the whole conditions of the criterion, hence $J_{\Gamma_0(23)}$ is a simple jacobian variety of dimension 2, whose endomorphism algebra $\mathcal{A}_0(J_{\Gamma_0(23)})$ is equal to $\boldsymbol{Q}(\sqrt{5})$.

Remark. By a suggestion of M. Sato, the author calculated values $\tau_{p,i}$ in a different way as follows.

Put

$$f(z) = \sqrt[12]{\Delta(z)\Delta(23z)} = \sum_{n=0}^{\infty} c_n q^n$$
$$g(z) = f(z)\,|\,T_2,$$

where $|\,T_p$ denotes the application of T_p. Then the eigenvalues $\tau_{p,i}$ are obtained from

$$\varphi_i(z) = g(z)+\alpha_i f(z) = \sum_{n=0}^{\infty}\tau_{n,i}q^n \qquad (i=1,2)$$

in which the constant α_i is to be chosen so that the corresponding Dirichlet series $\sum_n \tau_{n,i}n^{-s}$ should admit an Euler product. It is easy to derive that α_i satisfies

$$\alpha_i^2-\alpha_i-1=0, \quad \text{whence} \quad \alpha_1, \alpha_2 = \frac{1\pm\sqrt{5}}{2}.$$

From $\varphi_i(z)$ we have

$$\tau_{p,i} = c_{2p}+\alpha_i\cdot c_p, \qquad (p\neq 2).$$

The result is as follows:

p	$\tau_{p,i}$ $(i=1, 2)$	p	$\tau_{p,i}$ $(i=1, 2)$
3	$1-2a=\pm\sqrt{5}$	17	$4-2a=3\mp\sqrt{5}$
5	$-2+2a=-1\pm\sqrt{5}$	19	-2
7	$2a=1\pm\sqrt{5}$	23	$+1$
11	$-2-2a=-3\mp\sqrt{5}$	29	-3
13	$+3$	31	$-3+6a=\pm 3\sqrt{5}$

The case $N=29$ ($p^*(29)=0$) (cf. [3, p. 904]). The eigenvalues of T_p are in $\boldsymbol{Q}(\sqrt{2})$; $p=11, 13$ remain prime in $\boldsymbol{Q}(\sqrt{2})$. By the same procedure as above, we have

$$\tau_{11,i} = 1 \pm \sqrt{2}\,, \qquad \pi_{11,j} = \frac{\pi_{11,i} \pm \sqrt{\tau_{11,i}^2 - 44}}{2}\,,$$

$$\tau_{13,i} = -1 \pm 2\sqrt{2}\,, \qquad \pi_{13,j} = \frac{\tau_{13,i} \pm \sqrt{\tau_{13,i}^2 - 52}}{2}\,.$$

Hence $J_{\Gamma_0(29)}$ is simple, $\mathcal{A}_0(J_{\Gamma_0(29)})=\boldsymbol{Q}(\sqrt{2})$.

The case $N=31$ ($p^*(31)=0$). The eigenvalues of T_p are in $\boldsymbol{Q}(\sqrt{5})$ (an exact form of corresponding Dirichlet series is given in [3, p. 641–643]. $p=7, 13$ remain prime in $\boldsymbol{Q}(\sqrt{5})$. We have

$$\tau_{7,i} = -2 \pm \sqrt{5}\,, \qquad \pi_{7,j} = \frac{\tau_{7,i} \pm \sqrt{\tau_{7,i}^2 - 28}}{2}\,,$$

$$\tau_{13,i} = -1 \pm \sqrt{5}\,, \qquad \pi_{13,j} = \frac{\tau_{13,i} \pm \sqrt{\tau_{13,i}^2 - 52}}{2}\,.$$

Hence $J_{\Gamma_0(31)}$ is simple, $\mathcal{A}_0(J_{\Gamma_0(31)})=\boldsymbol{Q}(\sqrt{5})$.

The case $N=37$ ($p^*(37)=1$). The author calculated the eigenvalues $\tau_{p,i}$ for smaller values of p and found that they are all contained in $\boldsymbol{Q}$ and that they are not multiple for several p. Anyway, by the same reason as in the case $N=22$, $J_{\Gamma_0(37)}$ is isogenous to a product of two elliptic curves.

OSAKA UNIVERSITY

(Received August 23, 1963)

References

[1] M. Eichler: *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1956), 156–171.

[2] R. Fricke: Die elliptischen Funktionen und ihre Anwendungen II, Berlin, Leipzig, B. G. Teubner, 1922.

[3] E. Hecke: Mathematische Werke, Göttingen, Vandenhoeck & Ruprecht, 1959.

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

[5] G. Shimura: *Correspondences modulaires et les fonctions ζ de courbes algébriques*, J. Math. Soc. Japan **10** (1958),

[6] G. Shimura: *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. Japan **11** (1959), 291–311.

[7] G. Shimura: *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), 275–331.

[8] G. Shimura and Y. Taniyama: Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, **No. 6**, 1961.

[9] G. Shimura: *Automorphic functions and Arithmetic II*, (Japanese) Sūgaku, **13** (1961), 65–80.