Goro Shimura
Nagoya Math. J.
Vol. 43 (1971), 199–208

ON ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION AS FACTORS OF THE JACOBIANS OF MODULAR FUNCTION FIELDS

GORO SHIMURA

1. As Hecke showed, every L-function of an imaginary quadratic field K with a Grössen-character λ is the Mellin transform of a cusp form $f(z)$ belonging to a certain congruence subgroup Γ of $SL_2(\boldsymbol{Z})$. We can normalize λ so that

$$\lambda((\alpha)) = \alpha^{\nu} \quad \text{for} \quad \alpha \in K, \ \alpha \equiv 1 \ \mathrm{mod}^{\times} \mathfrak{c}$$

with a positive integer ν, where $\mathfrak{c}$ is the conductor of λ, and $\mathrm{mod}^{\times} \mathfrak{c}$ means the multiplicative congruence modulo $\mathfrak{c}$. Then $f(z)$ is of weight $\nu+1$, i.e.,

$$f((az+b)/(cz+d)) = f(z)(cz+d)^{\nu+1} \quad \text{for} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma,$$

and Γ is given by

$$\Gamma = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\boldsymbol{Z}) \middle| a \equiv d \equiv 1, \ c \equiv 0 \ \mathrm{mod} \ (D \cdot N(\mathfrak{c})) \right\},$$

where $-D$ is the discriminant of K. If $\nu = 1$, $f(z)dz$ is a differential form of the first kind on the compactification $(H/\Gamma)^*$ of the quotient H/Γ, where H denotes the upper half complex plane. Denote by $\mathrm{Jac}(H/\Gamma)$ the jacobian variety of $(H/\Gamma)^*$, and identify the tangent space of $\mathrm{Jac}(H/\Gamma)$ at the origin with the space of all differential forms of the first kind on $(H/\Gamma)^*$. Let A be the smallest abelian subvariety of $\mathrm{Jac}(H/\Gamma)$ that has $f(z)dz$ as a tangent at the origin. Then the first main result of this paper can be stated as follows:

The abelian variety A is a product of copies of an elliptic curve whose endomorphism algebra is isomorphic to K.

Hecke [3] proved this fact in the case where $K = \boldsymbol{Q}(\sqrt{-q})$ with a prime $q > 3$, $\equiv 3 \ \mathrm{mod} \ (4)$ and $\mathfrak{c} = (\sqrt{-q})$. In the general case, he showed only that

Received January 16, 1971.

the periods of $f(z)dz$ belong to a certain class field over K. His proof requires rather deep arithmetic results of complex multiplication. Ours is simpler, and based on the following

LEMMA 1. *Let X be an abelian variety of dimension n defined over $\boldsymbol{C}$, and h an injective homomorphism of K into $\mathrm{End}_{\boldsymbol{Q}}(X)$. Suppose that the representation of K, through h, on the tangent space of X at the origin is equivalent to n copies of the identity injection of K into $\boldsymbol{C}$. Then X is isogenous to a product of n copies of an elliptic curve E such that $\mathrm{End}_{\boldsymbol{Q}}(E)$ is isomorphic to K.*

Here and henceforth we denote by $\mathrm{End}(X)$ the ring of all endomorphisms of X over $\boldsymbol{C}$, and put $\mathrm{End}_{\boldsymbol{Q}}(X) = \mathrm{End}(X) \otimes \boldsymbol{Q}$.

Our next purpose is to show that every elliptic curve E defined over $\boldsymbol{Q}$ with complex multiplication is isogenous over $\boldsymbol{Q}$ to a factor of $\mathrm{Jac}(H/\Gamma')$ for some Γ' in the following way. By virtue of Deuring's result [1], if K is isomorphic to $\mathrm{End}_{\boldsymbol{Q}}(E)$, the zeta-function of E over $\boldsymbol{Q}$ is exactly the L-function of a certain Grössen-character λ of K. Then we obtain an abelian variety A by the procedure described above, i.e.,

elliptic curve $E \to$ zeta-function with a Grössen-character λ
$\to$ cusp form $f(z) \to$ abelian subvariety A of $\mathrm{Jac}(H/\Gamma')$.

In this situation, we shall prove:

A is an elliptic curve isogenous to E over $\boldsymbol{Q}$.

This is an easy consequence of the results in the previous articles [7], [8]. If $-D$ is the discriminant of K, and $\mathfrak{c}$ is the conductor of λ, the group Γ' is of the form

$$\Gamma' = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\boldsymbol{Z}) \,\middle|\, c \equiv 0 \mod (D \cdot N(\mathfrak{c})) \right\}.$$

2. Let us first prove the above lemma. Although it is a special case of [6, Prop. 14], we give here a direct proof for the reader's convenience.

Identify X with a complex torus $\boldsymbol{C}^n/L$ with a lattice L. Let $\boldsymbol{Q} \cdot L$ denote the $\boldsymbol{Q}$-linear span of L. Then K acts, through h, on $\boldsymbol{Q} \cdot L$, so that there exists a K-linear isomorphism p of K^n onto $\boldsymbol{Q} \cdot L$, where K^n is the submodule of $\boldsymbol{C}^n$ consisting of the vectors whose components belong to K. Since $\boldsymbol{C}^n = K^n \otimes_{\boldsymbol{Q}} \boldsymbol{R} = (\boldsymbol{Q} \cdot L) \otimes_{\boldsymbol{Q}} \boldsymbol{R}$, we can extend p to an $\boldsymbol{R}$-linear automorphism of $\boldsymbol{C}^n$, which we denote again by p. By our assumption, we may assume that the action of an element α of K on X is represented by the complex linear transformation $u \longrightarrow \alpha u$ ($u \in \boldsymbol{C}^n$) of $\boldsymbol{C}^n$. We can find a real number r and an element α of K so that $r \cdot \alpha = \sqrt{-1}$. Now p is K-linear and $\boldsymbol{R}$-linear, hence p commutes with the map $u \to \sqrt{-1} \cdot u$, i.e., p is $\boldsymbol{C}$-linear. Take any free $\boldsymbol{Z}$-submodule $\mathfrak{a}$ of rank 2 in K. Then p gives an isogeny of $\boldsymbol{C}^n/\mathfrak{a}^n = (\boldsymbol{C}/\mathfrak{a})^n$ onto $\boldsymbol{C}^n/L$. This proves the lemma, since $\boldsymbol{C}/\mathfrak{a}$ is an elliptic curve with K as its endomorphism algebra.

3. For a function $f(z)$ on H and $\xi = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\boldsymbol{R})$ with $\det(\xi) > 0$, we define a function $f|[\xi]_k$ on H by

$$(f|[\xi]_k)(z) = \det(\xi)^{k/2} \cdot (cz+d)^{-k} \cdot f((az+b)/(cz+d)).$$

For an arbitrary positive integer N, put

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\boldsymbol{Z}) \,\middle|\, c \equiv 0 \mod (N) \right\},$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \,\middle|\, a \equiv 1 \mod (N) \right\}.$$

Further, for a complex-valued character ε of $(\boldsymbol{Z}/N\boldsymbol{Z})^\times$,[1] we denote by $S_k(N, \varepsilon)$ the vector space of all the cusp forms $f(z)$ satisfying

$$f|[\gamma]_k = \varepsilon(d) \cdot f$$

for every $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$.

LEMMA 2. *Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ be an element of $S_k(N, \varepsilon)$, r a positive integer, M a common multiple of Nr and r^2, and let*

$$g(z) = \sum_{(n,r)=1} a_n e^{2\pi i n z}.$$

Then $g \in S_k(M, \varepsilon')$, where ε' is the restriction of ε to $(\boldsymbol{Z}/M\boldsymbol{Z})^\times$.

Proof. Put $\zeta = e^{2\pi i/r}$, $\eta_u = \begin{bmatrix} r & u \\ 0 & r \end{bmatrix}$ for $u \in \boldsymbol{Z}$, and $\Gamma = \Gamma_1(N)$. We see easily that $\Gamma\eta_u = \Gamma\eta_v$ if and only if $u \equiv v \mod (r)$. We can find numbers x_u of $\boldsymbol{Q}(\zeta)$ for $u \in \boldsymbol{Z}$ such that

$$x_u = x_v \quad \text{if} \quad u \equiv v \mod (r),$$

$$\sum_{u=0}^{r-1} x_u \zeta^{un} = \begin{cases} 1 & \text{if} \quad (n, r) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

[1] If S is an associative ring with the identity element, $S^\times$ denotes the group of all invertible elements in S.

We see easily that $g(z)=\sum_{u=0}^{r-1} x_u\cdot f|[\eta_u]_k$. Further, it can be seen that

$$x_u = x_{au} \qquad \text{if} \qquad (a, r)=1, \tag{1}$$

and x_u is invariant under $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$, hence $x_u\in\boldsymbol{Q}$. Now $g(z)$ is a cusp form of level Nr^2 (see for example [7, Prop. 2.4, Lemma 3.9]). Therefore, to prove our assertion, it is sufficient to check the behavior of g under an element $\gamma=\begin{bmatrix} a & b \\ Mc & d\end{bmatrix}$ of $\Gamma_0(M)$. We have

$$\begin{bmatrix} r & u \\ 0 & r\end{bmatrix}\begin{bmatrix} a & b \\ Mc & d\end{bmatrix}=\begin{bmatrix} a' & b' \\ Mc & d'\end{bmatrix}\begin{bmatrix} r & d^2u \\ 0 & r\end{bmatrix}$$

with $a'=a+cuM/r$, $b'=b+du(1-a'd)/r$, $d'=d-cd^2uM/r$. Note that $a'\equiv a$, $d'\equiv d \mod (N)\cap(r)$, and $a'd\equiv ad\equiv 1 \mod (r)$. Therefore, putting $v=d^2u$, we have $f|[\eta_u\gamma]_k=\varepsilon(d)\cdot f|[\eta_v]_k$. In view of (1), we obtain $g|[\gamma]_k=\varepsilon(d)\cdot g$, q.e.d.

4. For our purpose, it is necessary to consider Grössen-characters which are not necessarily "primitive". To define them, let $\mathfrak{m}$ be an integral ideal in K, and $I_{\mathfrak{m}}$ the group of all fractional ideals in K prime to $\mathfrak{m}$. Let $W_{\mathfrak{m}}$ denote the group of all elements α of $K^\times$ such that $\alpha\equiv 1 \mod^\times \mathfrak{m}$, i.e., $\alpha-1$ is $\mathfrak{p}$-integral and divisible by $\mathfrak{m}_{\mathfrak{p}}$ for all prime factors $\mathfrak{p}$ of $\mathfrak{m}$, where $\mathfrak{m}_{\mathfrak{p}}$ is the $\mathfrak{p}$-closure of $\mathfrak{m}$. Further let $P_{\mathfrak{m}}$ denote the subgroup of $I_{\mathfrak{m}}$ consisting of all principal ideals (α) with $\alpha\in W_{\mathfrak{m}}$. For a positive integer ν, let $\Lambda_{\mathfrak{m}}^{\nu}$ denote the set of all homomorphisms λ of $I_{\mathfrak{m}}$ into $\boldsymbol{C}^\times$ such that $\lambda((\alpha))=\alpha^\nu$ for every $\alpha\in W_{\mathfrak{m}}$. Such a λ is called a Grössen-character of K defined modulo $\mathfrak{m}$. Obviously, $\Lambda_{\mathfrak{m}}^{\nu}$ is not empty if and only if the following condition is satisfied:

(2) *If ζ is a root of unity in K and $\zeta\equiv 1 \mod \mathfrak{m}$, then $\zeta^\nu=1$.*

For each $\lambda\in\Lambda_{\mathfrak{m}}^{\nu}$, there is a unique divisor $\mathfrak{c}$ of $\mathfrak{m}$ such that: (i) λ is the restriction of an element of $\Lambda_{\mathfrak{c}}^{\nu}$; (ii) no proper divisor of $\mathfrak{c}$ has the property (i). Then $\mathfrak{c}$ is called the *conductor* of λ. We call λ *primitive* if $\mathfrak{m}$ is the conductor of λ.

We can associate with every $\lambda\in\Lambda_{\mathfrak{m}}^{\nu}$ an L-function $L(s,\lambda)$ and a function $f_\lambda(z)$ on H by

$$L(s,\lambda)=\sum_{\mathfrak{x}}\lambda(\mathfrak{x})N(\mathfrak{x})^{-s} \qquad (s\in\boldsymbol{C}),$$

$$f_\lambda(z)=\sum_{\mathfrak{x}}\lambda(\mathfrak{x})e^{2\pi i N(\mathfrak{x})z} \qquad (z\in H),$$

https://doi.org/10.1017/S0027763000014471 Published online by Cambridge University Press

where each sum is taken over all integral ideals $\mathfrak{x}$ in $I_{\mathfrak{m}}$. Under the assumption (2), let $V_{\mathfrak{m}}^{\nu}$ be the vector space spanned by the f_{λ} over $\boldsymbol{C}$ for all $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$. For λ, $\mu \in \Lambda_{\mathfrak{m}}^{\nu}$, we see easily that $f_{\lambda} = f_{\mu}$ if and only if $\lambda = \mu$. Moreover, we shall see later that the f_{λ} for $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$ are linearly independent over $\boldsymbol{C}$. Therefore $V_{\mathfrak{m}}^{\nu}$ is of dimension $[I_{\mathfrak{m}} : P_{\mathfrak{m}}]$.

Fix any set S of representatives for $I_{\mathfrak{m}}$ modulo $P_{\mathfrak{m}}$, whose members are prime to $\mathfrak{m}$, and put, for each $\mathfrak{a} \in S$,

$$g_{\mathfrak{a}}(z) = \sum_{(\alpha)} \alpha^{\nu} \cdot e^{2\pi i N(\alpha) z / N(\mathfrak{a})}, \tag{3}$$

where the sum is taken over all ideals (α) such that $\alpha \in W_{\mathfrak{m}} \cap \mathfrak{a}$. We have then

$$f_{\lambda} = \sum_{\mathfrak{a} \in S} \lambda(\mathfrak{a})^{-1} \cdot g_{\mathfrak{a}},$$

so that the functions $g_{\mathfrak{a}}$, for $\mathfrak{a} \in S$, form a basis of $V_{\mathfrak{m}}^{\nu}$ over $\boldsymbol{C}$. Hecke [2] proved that $g_{\mathfrak{a}}$ is a cusp form belonging to a certain congruence subgroup. We can state this fact in the following form.

LEMMA 3. *Let $-D$ be the discriminant of K, and let $\lambda \in \Lambda_{\mathfrak{m}}^{\nu}$, $M = D \cdot N(\mathfrak{m})$. Then f_{λ} is an element of $S_{\nu+1}(M, \varepsilon)$, where ε is the character of $(\boldsymbol{Z}/M\boldsymbol{Z})^{\times}$ defined by*

$$\varepsilon(a) = \left(\frac{-D}{a}\right) \cdot \frac{\lambda((a))}{a^{\nu}} \qquad (a \in \boldsymbol{Z},\ (a, M) = 1).$$

Proof. If λ is primitive, our assertion can be proved by examining the functional equations of $L(s, \lambda)$ and

$$L(s, \lambda, \chi) = \sum_{\mathfrak{x}} \lambda(\mathfrak{x}) \chi(N(\mathfrak{x})) N(\mathfrak{x})^{-s}$$

with primitive characters χ of $(\boldsymbol{Z}/p\boldsymbol{Z})^{\times}$ for all rational primes p not dividing M, and applying the principle of Weil [9]. Although [9, Satz 2] is concerned with $S_k(M, \varepsilon)$ for real characters ε, the result can easily be extended to the case of an arbitrary character ε. Let us now prove the general case by induction on $N(\mathfrak{c}^{-1}\mathfrak{m})$, where $\mathfrak{c}$ is the conductor of λ. Suppose that $\mathfrak{c}^{-1}\mathfrak{m}$ has a prime factor $\mathfrak{p}$, and put $\mathfrak{n} = \mathfrak{p}^{-1}\mathfrak{m}$. Let μ be the element of $\Lambda_{\mathfrak{n}}^{\nu}$ whose restriction to $\Lambda_{\mathfrak{m}}^{\nu}$ is λ. By the induction assumption, f_{μ} belongs to $S_{\nu+1}(D \cdot N(\mathfrak{n}), \varepsilon)$. Put $q = N(\mathfrak{p})$. Then

$$f_{\mu}(qz) = \sum_{(\mathfrak{x}, \mathfrak{n}) = 1} \mu(\mathfrak{x}) e^{2\pi i N(\mathfrak{p}\mathfrak{x}) z},$$

hence

(4) $$f_\mu(z) - \mu(\mathfrak{p}) f_\mu(qz) = \sum_{(\mathfrak{x}, \mathfrak{m})=1} \mu(\mathfrak{x}) e^{2\pi i N(\mathfrak{x}) z} = f_\lambda(z),$$

where we understand that $\mu(\mathfrak{p}) = 0$ if $\mathfrak{p}$ divides $\mathfrak{n}$. Since we have

$$\begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ qc & d \end{bmatrix} = \begin{bmatrix} a & qb \\ c & d \end{bmatrix} \begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix},$$

it can easily be verified that $f_\mu(qz) \in S_{\nu+1}(q \cdot D \cdot N(\mathfrak{n}), \varepsilon)$. Therefore the equality (4) implies that $f_\lambda \in S_{\nu+1}(q \cdot D \cdot N(\mathfrak{n}), \varepsilon)$, q.e.d.

The symbols λ, M, and ε being as above, put $f_\lambda(z) = \sum_n a_n e^{2\pi i n z}$. Then the L-function $L(s, \lambda)$ has an Euler product:

$$L(s, \lambda) = \Pi_p (1 - a_p p^{-s} + \varepsilon(p) p^{\nu - 2s})^{-1},$$

where the product is taken over all rational primes p ; $\varepsilon(p) = 0$ for every prime factor p of M. Therefore, by Hecke [4, II, Satz 42] (see also [7, Th. 3.43]), f_λ must be a common eigen-function of all Hecke operators. Thus the functions f_λ, for $\lambda \in \Lambda^\nu_\mathfrak{m}$, are distinct eigen-functions whose first Fourier coefficients are 1. Therefore they are linearly independent over $\boldsymbol{C}$.

5. Let us now consider a projective non-singular curve C_M biregularly isomorphic to the compactification of the quotient $H/\Gamma_1(M)$ for a positive integer M. There is a "standard" way to define C_M rational over $\boldsymbol{Q}$, up to biregular isomorphisms over $\boldsymbol{Q}$. (One can define, for instance, the function field of C_M to be the field of all $\Gamma_1(M)$-invariant modular functions whose Fourier expansions with respect to $e^{2\pi i z}$ have rational coefficients. See also [5], [7, §6.7, §6.3].) Then the jacobian variety $\mathrm{Jac}(C_M)$ of C_M can naturally be defined over $\boldsymbol{Q}$. We denote by τ_n the endomorphism of $\mathrm{Jac}(C_M)$ corresponding to the Hecke operator of degree n.

Let $\lambda \in \Lambda^1_\mathfrak{m}$, $M = D \cdot N(\mathfrak{m})$, and $f_\lambda(z) = \sum_n a_n e^{2\pi i n z}$. Further let k_λ denote the field generated over $\boldsymbol{Q}$ by the numbers a_n for all n. Since f_λ is a common eigen-function of all Hecke operators, we obtain, by virtue of [7, Th. 7.14], a couple $(A_\lambda, \theta_\lambda)$ satisfying the following three conditions:

(i) *A_λ is an abelian subvariety of $\mathrm{Jac}(C_M)$ of dimension $[k_\lambda : \boldsymbol{Q}]$.*

(ii) *θ_λ is an isomorphism of k_λ into $\mathrm{End}_{\boldsymbol{Q}}(A_\lambda)$ such that $\theta_\lambda(a_n)$ is the restriction of τ_n to A_λ for all n.*

(iii) *A_λ is rational over $\boldsymbol{Q}$.*

Moreover, $(A_\lambda, \theta_\lambda)$ is unique for f_λ under the conditions (i) and (ii).

For an automorphism σ of the algebraic closure of $\boldsymbol{Q}$, we define an element λ_σ of $\Lambda^1_{\mathfrak{m}^\sigma}$ by $\lambda_\sigma(\mathfrak{x}) = \lambda(\mathfrak{x}^\sigma)^\sigma$. If $f_\lambda(z) = \sum_n a_n e^{2\pi i n z}$, we see that $f_{\lambda_\sigma}(z) = \sum_n a_n^\sigma e^{2\pi i n z}$. Now identify the tangent space of $\mathrm{Jac}(C_M)$ at the origin with the space of all cusp forms of weight 2 with respect to $\Gamma_1(M)$. Then the proof of [7, Th. 7.14] shows that the tangent space of A_λ at the origin can be identified with the vector space spanned by all distinct f_{λ_σ}. Therefore our result mentioned at the beginning of this paper follows from the following

THEOREM 1. *The abelian variety A_λ is isogenous to a product of copies of an elliptic curve whose endomorphism algebra is isomorphic to K.*

Proof. (I) First let us assume that $\mathfrak{m}$ is divisible by $\sqrt{-D}$, and $\mathfrak{m}=\mathfrak{m}^\rho$, where ρ denotes the complex conjugation. Put

$$\Gamma = \Gamma_1(M), \quad \delta = \begin{bmatrix} 1 & 1/d \\ 0 & 1 \end{bmatrix}.$$

We can let $\Gamma\delta\Gamma$ act on the vector space of cusp forms with respect to Γ (see [7, §3.4]). Denote the action by $[\Gamma\delta\Gamma]_2$. Take a disjoint coset decomposition $\Gamma\delta\Gamma = \cup_{i=1}^{\kappa}\Gamma\delta\gamma_i$ with $\gamma_i \in \Gamma$. Let $g_\mathfrak{a}$ be as in (3). Then, by definition,

$$g_\mathfrak{a}|[\Gamma\delta\Gamma]_2 = \cup_{i=1}^{\kappa} g_\mathfrak{a}|[\delta\gamma_i]_2.$$

If $\alpha, \beta \in W_\mathfrak{m} \cap \mathfrak{a}$, we have

$$N(\alpha)/N(\mathfrak{a}) \equiv N(\beta)/N(\mathfrak{a}) \mod (D),$$

so that, if $\zeta_D = e^{2\pi i/D}$,

$$g_\mathfrak{a}|[\delta]_2 = \zeta_D^{N(\alpha)/N(\mathfrak{a})} \cdot g_\mathfrak{a}$$

with any fixed α contained in $W_\mathfrak{m} \cap \mathfrak{a}$. Therefore

$$g_\mathfrak{a}|[\Gamma\delta\Gamma]_2 = \kappa \cdot \zeta_D^{N(\alpha)/N(\mathfrak{a})} \cdot g_\mathfrak{a}. \tag{5}$$

Thus $[\Gamma\delta\Gamma]_2$ maps $V^1_\mathfrak{m}$ onto itself. Let A' be the abelian subvariety of $\mathrm{Jac}(C_M)$ generated by the A_λ for all $\lambda \in \Lambda^1_\mathfrak{m}$. Since $\mathfrak{m} = \mathfrak{m}^\rho$, $V^1_\mathfrak{m}$ can be identified with the tangent space of A' at the origin. Let ω denote the endomorphism of A' obtained from $[\Gamma\delta\Gamma]_2$. The relation (5) shows that the representation of ω on the tangent space has characteristic roots $\kappa \cdot \zeta_D^{N(\alpha)/N(\mathfrak{a})}$, where α must be fixed for each $\mathfrak{a} \in S$. Put $\chi(r) = \left(\frac{-D}{r}\right)$. Then we see that

$N(\alpha)/N(\mathfrak{a})$ is prime to D, and $\chi(N(\alpha)/N(\mathfrak{a}))=1$. We can define an embedding h of $\boldsymbol{Q}(\zeta_D)$ into $\mathrm{End}_{\boldsymbol{Q}}(A')$ by $h(\zeta_D)=\kappa^{-1}\omega$. If σ is an automorphism of $\boldsymbol{Q}(\zeta_D)$ such that $\zeta_D^\sigma=\zeta_D^r$ with $\chi(r)=1$, then the restriction of σ to K is the identity map. Therefore applying Lemma 1 to A', we see that A' is isogenous to a product of copies of an elliptic curve with K as its endomorphism algebra.

(II) Next assume that λ is primitive, and put $\mathfrak{m}'=\mathfrak{m}\mathfrak{m}^\rho\cdot(\sqrt{-D})$, $M'=N(\mathfrak{m}')\cdot D$, $\eta_u=\begin{bmatrix} M & u \\ 0 & M\end{bmatrix}$ for $u\in\boldsymbol{Z}$. Then $M'=M^2$ and $\mathfrak{m}'=\mathfrak{m}'^\rho$. Define, as in the proof of Lemma 2, rational numbers x_u so that

$$\textstyle\sum_{u=0}^{M-1} x_u\zeta_M^{un}=\begin{cases}1 & \text{if } (n,M)=1,\\ 0 & \text{otherwise,}\end{cases}$$

where $\zeta_M=e^{2\pi i/M}$. Take a positive integer t so that tx_u is an integer for every u. Put $\xi=\sum_{u=0}^{M-1} tx_u\cdot[\eta_u]_2$. For every

$$f(z)=\textstyle\sum_n a_n e^{2\pi i n z}\in S_2(M,\varepsilon),$$

we have, by Lemma 2 and its proof,

$$f|\xi=t\cdot\textstyle\sum_{(n,M)=1}a_n e^{2\pi i n z}\in S_2(M',\varepsilon).$$

Especially $f_\lambda|\xi=t\cdot f_\mu$ if μ is the restriction of λ to $I_{\mathfrak{m}'}$. Let V_λ be the subspace of $V_{\mathfrak{m}}^1+V_{\mathfrak{m}^\rho}^1$ spanned by all distinct f_{λ_σ} with automorphisms σ of the algebraic closure of $\boldsymbol{Q}$. Since λ is primitive, we see that ξ maps V_λ *injectively* into $V_{\mathfrak{m}'}^1$. (This is not necessarily true if λ is not primitive.) Since $\eta_u\cdot\Gamma_1(M')\eta_u^{-1}\subset\Gamma_1(M)$, the action $[\eta_u]_2$ defines a homomorphism of $\mathrm{Jac}(C_M)$ into $\mathrm{Jac}(C_{M'})$, hence ξ defines a homomorphism ξ^* of $\mathrm{Jac}(C_M)$ into $\mathrm{Jac}(C_{M'})$. Then the restriction of ξ^* to A_λ is an isogeny onto an abelian subvariety of A'', where A'' is the sum of A_μ for all $\mu\in\Lambda_{\mathfrak{m}'}^1$. By the result in the case (I), A'' is isogenous to a product of copies of an elliptic curve with K as its endomorphism algebra. Therefore A_λ has the same property.

(III) Finally let us consider the general case with no assumption on $\mathfrak{m}$. Let $\mathfrak{c}$ be the conductor of λ. To prove our assertion by induction on $N(\mathfrak{c}^{-1}\mathfrak{m})$, suppose that $\mathfrak{c}^{-1}\mathfrak{m}$ has a prime factor $\mathfrak{p}$, and put $\mathfrak{n}=\mathfrak{p}^{-1}\mathfrak{m}$, $q=N(\mathfrak{p})$, $L=q^{-1}M$, $\beta=\begin{bmatrix} q & 0 \\ 0 & 1\end{bmatrix}$. Since $\beta\Gamma_1(M)\beta^{-1}\subset\Gamma_1(L)$, $[\beta]_2$ defines an endomorphism ψ of $\mathrm{Jac}(C_L)$ into $\mathrm{Jac}(C_M)$. Let φ be the natural map of $\mathrm{Jac}(C_L)$ into $\mathrm{Jac}(C_M)$ corresponding to $[1]_2$. If μ is the element of $\Lambda_{\mathfrak{n}}^1$ whose restriction to $I_{\mathfrak{m}}$ is λ, we have $f_{\lambda_\sigma}=f_{\mu_\sigma}-s\cdot f_{\mu_\sigma}|[\beta]_2$ with a constant s, by virtue of (4),

https://doi.org/10.1017/S0027763000014471 Published online by Cambridge University Press

for every automorphism σ of the algebraic closure of $\boldsymbol{Q}$. This shows that $A_\lambda \subset \varphi(A_\mu) + \psi(A_\mu)$. Therefore our assertion about A_λ follows from that about A_μ, which is ensured by induction.

Remark. We have thus shown that the center $\mathfrak{Z}$ of $\mathrm{End}_{\boldsymbol{Q}}(A_\lambda)$ is isomorphic to K. It should be noted here that $\mathfrak{Z}$ *is not contained in* $\theta_\lambda(k_\lambda)$. This follows from either of the following two facts:

(i) The elements of $\theta_\lambda(k_\lambda) \cap \mathrm{End}(A_\lambda)$ are rational over $\boldsymbol{Q}$ (see [7, pp. 182–183]), while K is the smallest field of definition for any generator of $\mathfrak{Z}$ contained in $\mathrm{End}(A_\lambda)$.

(ii) The representation of k_λ, through θ_λ, on the tangent space of A_λ at the origin is equivalent to a regular representation over $\boldsymbol{Q}$.

6. Let E be an elliptic curve defined over $\boldsymbol{Q}$ such that $\mathrm{End}_{\boldsymbol{Q}}(E)$ is isomorphic to K. (This can happen if and only if the class number of K is one.) By the result of Deuring [1], the zeta-function of E over $\boldsymbol{Q}$ coincides exactly with $L(s, \lambda)$ with some primitive Grössen-character λ of K. Let $\mathfrak{c}$ be the conductor of λ, and $M = D \cdot N(\mathfrak{c})$. Then we obtain an element f_λ of $S_2(M, \varepsilon)$ as before. If $f_\lambda(z) = \sum_n a_n e^{2\pi i n z}$, we have

$$L(s, \lambda) = \Pi_p (1 - a_p p^{-s} + \varepsilon(p) p^{1-2s})^{-1}. \tag{6}$$

Since E is defined over $\boldsymbol{Q}$, we see that $a_n \in \boldsymbol{Q}$, and ε is the trivial character, so that f_λ is a cusp form invariant under $\Gamma_0(M)$. Therefore we can take $\mathrm{Jac}(H/\Gamma_0(M))$ (of course defined over $\boldsymbol{Q}$) instead of $\mathrm{Jac}(H/\Gamma_1(M))$ in the above discussion, and define A_λ as an abelian subvariety of $\mathrm{Jac}(H/\Gamma_0(M))$. Since $k_\lambda = \boldsymbol{Q}$, A_λ is an elliptic curve defined over $\boldsymbol{Q}$.

THEOREM 2. *The elliptic curve A_λ is isogenous to E over $\boldsymbol{Q}$.*

Proof. By [7, Th. 7.15], the zeta-function of A_λ over $\boldsymbol{Q}$ coincides, up to finitely many Euler factors, with (6). On the other hand, by Theorem 1, $\mathrm{End}_{\boldsymbol{Q}}(A_\lambda)$ is isomorphic to K, so that the zeta-function of A_λ over $\boldsymbol{Q}$ is $L(s, \mu)$ with a primitive Grössen-character μ of K. Thus $L(s, \lambda)$ coincides with $L(s, \mu)$ up to finitely many Euler factors. It follows that $\lambda(\mathfrak{p}) = \mu(\mathfrak{p})$ or $\lambda(\mathfrak{p}) = \mu(\mathfrak{p}^\rho)$ for almost all prime ideals $\mathfrak{p}$ in K. If $\mathfrak{m}$ is a common multiple of the conductors of λ and μ, we have $\lambda((\alpha)) = \alpha = \mu((\alpha))$ for $\alpha \in K$, $\alpha \equiv 1 \bmod^\times \mathfrak{m}$. Therefore we must have $\lambda(\mathfrak{p}) = \mu(\mathfrak{p})$, so that $\lambda = \mu$. Thus E and

A_λ determine the same Grössen-character of K. By [8, Th. 8], they must be isogenous over $\boldsymbol{Q}$.

It should be noted that E has good reduction modulo a rational prime p if and only if p does not divide $D \cdot N(\mathfrak{c})$. This is due to Deuring [1, IV] (see also [8] for a simpler proof).

References

[1] M. Deuring, Die Zetafunktion einer algebraischen Kurve vom Geschlecht Eins, I, II, III, IV, Nachr. Akad. Wiss. Göttingen, (1953) 85–94, (1955) 13–42, (1956) 37–76, (1957) 55–80.

[2] E. Hecke, Zur Theorie der elliptischen Modulfunktionen, Math. Ann., **97** (1926), 210–242 (=Math. Werke, 428–460).

[3] E. Hecke, Bestimmung der Perioden gewisser Integrale durch die Theorie der Klassenkörper, Math. Zeitschr., **28** (1928), 708–727 (=Math. Werke, 505–524).

[4] E. Hecke, Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung I, II, Math. Ann., **114** (1937), 1–28, 316–351 (=Math. Werke, 644–707).

[5] G. Shimura, Correspondances modulaires et les fonctions ζ de courbes algébriques, J. Math. Soc. Japan, **10** (1958), 1–28.

[6] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, Ann. of Math., **78** (1963), 149–192.

[7] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, No. 11, 1971.

[8] G. Shimura, On the zeta-function of an abelian variety with complex multiplication, to appear.

[9] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann., **168** (1967), 149–156.

Princeton University

https://doi.org/10.1017/S0027763000014471 Published online by Cambridge University Press