Chin. Ann. Math.
37B(6), 2016, 821–832
DOI: 10.1007/s11401-016-1009-x

Chinese Annals of Mathematics, Series B

Rational Structure of $X(N)$ over $\mathbb{Q}$ and Explicit Galois Action on CM Points[*]

Tonghai YANG[1]

Abstract This paper reviews a less known rational structure on the Siegel modular variety $X(N) = \Gamma(N)\backslash\mathbb{H}_g$ over $\mathbb{Q}$ for integers $g, N \geq 1$. The author then describes explicitly how Galois groups act on CM points on this variety. Finally, another proof of the Shimura reciprocity law by using the result and the q-expansion principle is given.

Keywords Siegel modular variety, Galois action, Explicit reciprocity law
2000 MR Subject Classification 11G18, 14G40, 11F67

1 Introduction

Let $g \geq 1$ and $N \geq 1$ be positive integers, and let $\mathbb{H}_g$ be the Siegel upper half plane of genus g, i.e., the set of symmetric complex matrices τ of order g such that $\Im(\tau) > 0$. Let

$$\Gamma(N) = \{\gamma \in \mathrm{Sp}_g(\mathbb{Z}) : \gamma \equiv 1 \pmod N\}$$

be the main congruence subgroup and let $X(N) = \Gamma(N)\backslash\mathbb{H}_g$ be the complex manifold which turns out to be an algebraic variety. To construct a cryptosystem by using genus g $(g = 1, 2)$ CM curves, it is important to compute a CM point in $X(N)$ and its Galois conjugates in $X(N)$ explicitly so that one can compute $f(\tau)$ explicitly for some explicit modular functions (invariants) f on $X(N)$. For this, one needs to interpret $X(N)$ in terms of moduli. There are two well-known moduli schemes: $\mathcal{X}_0$ over $\mathbb{Q}(\mu_N)$ whose $\mathbb{C}$-points give $X(N)$, and $\mathcal{X}$ over $\mathbb{Q}$ whose $\mathbb{C}$-points give $(\mathbb{Z}/N)^\times$-copies of $X(N)$ (see Section 2 for a review), which are thus not connected. Here μ_N is the group of N-th root of unity. Neither one is handy for our purpose as the first one is only defined over $\mathbb{Q}(\mu_N)$ and the second one has extra $(\mathbb{Z}/N)^\times$ in addition to $X(N)$. There turns out to be a third non-standard moduli scheme $\mathcal{X}^*$ over $\mathbb{Q}$, whose $\mathbb{C}$-points also give $X(N)$, which is natural and good for our purpose. This is constructed as a quotient of $\mathcal{X}$ in Section 2. This moduli interpretation is a special case of the general Shimura variety construction, though not explicitly presented in the literature and it should be of interest to publicize it. Using this interpretation, we give an explicit Galois action on a CM point in $X(N)$ in Section 3. As a byproduct, we give in Section 4 a direct proof of the well-known Shimura

Manuscript received February 1, 2015.
[1] Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA.
E-mail: thyang@math.wisc.edu
[*] This work was supported by the National Science Foundation Grants (No. DMS-1200380, DMS-1500743) and the Chinese Qian Ren Plan of Tsinghua (No. 543100001).

reciprocity law, which Shimura developed in the 1970s (see for example [6]), and its explicit version given by Streng recently (see [10]).

This work was inspired by my joint work with Castello, Deines-Shartz, and Lauter [1] on genus two curues.

2 Open Modular Variety $X(N)$ over $\mathbb{Q}$

Let $G = \mathrm{GSp}_g$ be the generalized symplectic group (matrices of order $2g$) with a similitude character μ, and let $G_0 = \mathrm{Sp}_g$ be the usual symplectic group, i.e., the kernel of μ:

$$1 \to \mathrm{Sp}_g \to \mathrm{GSp}_g \to \mathbb{G}_m \to 1.$$

There are two well-known moduli spaces associated with $X(N)$ which we now briefly review, and refer to [2] for a thorough review. Let μ_N be the group of the N-th roots of unity in $\mathbb{C}$, fix an isomorphism $\mu_N \cong \mathbb{Z}/N$ and identify them in this paper. Then for any principally polarized abelian variety A over a field F (of a character prime to N), the Weil pairing on the N-torsion $A[N]$ becomes a symplectic pairing

$$\langle\, ,\, \rangle_{\mathrm{we}} : A[N](F) \times A[N](F) \to \mathbb{Z}/N,$$

which is perfect if $A[N](F) = A[N]$.

Let $\mathcal{X}$ be the moduli space over $\mathbb{Z}[\frac{1}{N}]$ as follows: For a $\mathbb{Z}[\frac{1}{N}]$-scheme S, $\mathcal{X}(S)$ consists of isomorphism classes of the triplets (A, λ, ϕ), where

(1) A is an abelian scheme over S,

(2) $\lambda : A \to A^\vee$ is a principal polarization of A, and

(3) $\phi : (\mathbb{Z}/N)^{2g} \to A[N](S)$ is locally a similitude symplectic isomorphism, i.e., $\langle\phi(x), \phi(y)\rangle_{\mathrm{we}} = d\langle x, y\rangle$ for some $d \in (\mathbb{Z}/N)^\times$ (both ϕ and d may vary, depending on local connected components of S). Here we use the standard sympletic form on $(\mathbb{Z}/N)^{2g}$:

$$\langle x, y\rangle = \sum_{i=1}^{g} x_i y_{g+i} - \sum_{i=1}^{g} x_{g+i} y_i.$$

Notice that due to the freedom on $d \in (\mathbb{Z}/N)^\times$, the moduli problem does not depend on the choice of our identification $\mu_N \cong \mathbb{Z}/N$. It is well-known that this moduli space is represented by a smooth Deligne-Mumford stack, still denoted by $\mathcal{X}$, over $\mathbb{Z}[\frac{1}{N}]$. It is actually a smooth scheme when $N \geq 3$.

Let $\mathcal{X}_0$ be the moduli space over $\mathbb{Z}[\frac{1}{N}, \mu_N]$ as follows: For a $\mathbb{Z}[\frac{1}{N}, \zeta_N]$-scheme S, $\mathcal{X}(S)$ consists of isomorphism classes of the triplets (A, λ, ϕ), where

(1) A is an abelian scheme over S,

(2) $\lambda : A \to A^\vee$ is a principal polarization of A, and

(3) $\phi : (\mathbb{Z}/N)^{2g} \to A[N](S)$ is a symplectic isomorphism, i.e., $\langle\phi(x), \phi(y)\rangle_{\mathrm{we}} = \langle x, y\rangle$.

It is also well-known that this moduli space is represented by a smooth Deligne-Mumford stack, still denoted by $\mathcal{X}_0$, over $\mathbb{Z}[\frac{1}{N}, \mu_N]$. It is again a smooth scheme when $N \geq 3$.

In terms of the Shimura datum, one has the following: Let

$$K(N) = \{g \in G(\widehat{\mathbb{Z}}) : g \equiv 1 \pmod N\}, \quad K_0(N) = K(N) \cap G_0(\widehat{\mathbb{Z}}).$$

Then $\mathcal{X}$ is the Shimura variety associated with K, i.e.,

$$\mathcal{X}(\mathbb{C}) = G(\mathbb{Q})\backslash(\mathbb{H}_g^{\pm} \times G(\mathbb{A}_f)/K(N)) = (\Gamma(N)\backslash\mathbb{H}_g) \times (\mathbb{Z}/N)^{\times}.$$

Moreover,

$$\mathcal{X}_0(\mathbb{C}) = X(N) = \mathbb{G}_0(\mathbb{Q})\backslash(\mathbb{H}_g \times G_0(\mathbb{A}_f)/K_0(N))$$

is the connected component of $\mathcal{X}(\mathbb{C})$.

It turns out that there is a (less known) third Shimura variety $\mathcal{X}^*$ over $\mathbb{Z}[\frac{1}{N}]$ directly related to $X(N)$. It is associated with the compact open subgroup of G

$$K^*(N) = \{g \in G(\widehat{\mathbb{Z}}) : \ g \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right) \pmod N\}.$$

By the strong approximation theorem, one has

$$\begin{aligned} &\mathcal{X}^*(\mathbb{C}) = G(\mathbb{Q})\backslash(\mathbb{H}_g^{\pm} \times G(\mathbb{A}_f)/K^*(N)) = X(N), \\ &\mathcal{X}_0(\mathbb{C}) \hookrightarrow \mathcal{X}(\mathbb{C}) \twoheadrightarrow (\mathbb{Z}/N)^{\times} \end{aligned}$$

and

$$(\mathbb{Z}/N)^{\times} \circlearrowright \mathcal{X}(\mathbb{C}) \twoheadrightarrow \mathcal{X}^*(\mathbb{C}).$$

Here the action is given by $d \circ [z, g] = [z, gv(d)]$, and the natural project from $\mathcal{X}(\mathbb{C})$ to $\mathcal{X}^*(\mathbb{C})$ has fiber $(\mathbb{Z}/N)^{\times}$. Here $v(d) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ with respect to the standard symplectic basis of $(\mathbb{Z}/N)^{2g}$.

To give the moduli problem for this variety, let $(\mathbb{Z}/N)^{\times}$ act on $\mathcal{X}$ as follows:

$$d \circ (A, \lambda, \phi) = (A, \lambda, \phi \circ v(d)).$$

The action is free, so there is a quotient stack (a scheme for $N \geq 3$) $\mathcal{X}^* = \mathcal{X}/(\mathbb{Z}/N)^{\times}$ which represents the following quotient moduli problem over $\mathbb{Z}[\frac{1}{N}]$. For a $\mathbb{Z}[\frac{1}{N}]$-scheme S, $\mathcal{X}^*(S)$ consists of the equivalence classes of the triples (A, λ, ϕ) as in $\mathcal{X}(S)$, but with the following equivalence relation: $(A_1, \lambda_1, \phi_1) \sim (A_2, \lambda_2, \phi_2)$ if and only if there is an S-isomorphism $f : A_1 \to A_2$ commuting with the polarizations λ_i and $\phi_2 = \phi_1 \circ v(d)$ for some $d \in (\mathbb{Z}/N)^{\times}$. Alternatively, $\mathcal{X}^*(S)$ are the equivalence classes of the triples $(A, \lambda, \vec{e})$ where (A, λ) is a principally polarized abelian scheme over S, and $\vec{e} = (e_1, \cdots, e_{2g})$ is locally an ordered similitude symplectic basis of $A[N](S)$ with respect to the Weil pairing, i.e., for $i \leq j$,

$$\langle e_i, e_j \rangle_{\mathrm{we}} = \begin{cases} d, & \text{if } 1 \leq i \leq g, \ j = g + i, \\ 0, & \text{otherwise} \end{cases}$$

for some $d \in (\mathbb{Z}/N)^{\times}$. A similitude symplectic basis is called a symplectic basis if $d = 1$. Two such triples $(A, \lambda, \vec{e}) \sim (A', B', \vec{e}')$ if and only if there is an S-isomorphism $f : (A, \lambda) \to (A', \lambda')$ such that $f(e_i) = e_i'$ for $1 \leq i \leq g$ and $f(e_i) = de_i'$ for all $g + 1 \leq i \leq 2g$ and some $d \in (\mathbb{Z}/N)^{\times}$ locally.

Proposition 2.1 *One has, over* $\mathbb{Z}[\frac{1}{N}, \mu_N]$,

$$\mathcal{X}^* = \mathcal{X}_0.$$

Proof Let $\vec{e} = (e_1, e_2, \cdots, e_{2g})$ be the standard symplectic basis of $(\mathbb{Z}/N)^{2g}$. Given two triples (A, λ, ϕ) and (A', λ', ϕ') in $\mathcal{X}_0(S)$ for a $\mathbb{Z}[\frac{1}{N}, \mu_N]$-scheme S, if they are equal in $\mathcal{X}^*(S)$, i.e., there is an S-isomorphism $f : (A, \lambda) \to (A', \lambda')$ and $d \in (\mathbb{Z}/N)^\times$ such that $\phi' = f \circ \phi \circ v(d)$, one has

$$1 = \langle \phi'(e_i), \phi'(e_{i+g}) \rangle_{\mathrm{we}} = \langle \phi(v(d)e_i), \phi(v(d)e_{g+i}) \rangle_{\mathrm{we}} = \langle e_i, de_{g+i} \rangle = d \in (\mathbb{Z}/N)^\times.$$

So $(A, \lambda, \phi) = (A', \lambda', \phi')$ in $\mathcal{X}_0(S)$. This gives an injection $\mathcal{X}_0 \to \mathcal{X}^*$ over $\mathbb{Z}[\frac{1}{N}, \mu_N]$. To verify the surjectivity, let $(A, \lambda, \phi) \in \mathcal{X}^*(S)$. Let $P_i = \phi(e_i)$, and then there is $d \in (\mathbb{Z}/N)^\times$ such that

$$\langle P_i, P_j \rangle_{\mathrm{we}} = d \langle e_i, e_j \rangle.$$

Take $\phi' = \phi \circ v(d^{-1})$, and then one sees that ϕ' is a symplectic isomorphism. So $(A, \lambda, \phi) = (A, \lambda, \phi') \in \mathcal{X}^*(S)$ is the image of $(A, \lambda, \phi') \in \mathcal{X}_0(S)$.

Remark 2.1 There is another moduli interpretation for $X(N)$ over $\mathbb{Q}$ as follows: Let $\mathcal{X}'$ be the moduli space of the equivalence classes of the triples (A, λ, ϕ), where (A, λ) are principally polarized abelian schemes as above, and $\phi : (\mathbb{Z}/N)^g \times (\mu_N)^g \to A[N]$ is a Galois equivariant map which respects the pairings. The equivalence is the usual one as in the moduli interpretation of $\mathcal{X}$. Here the pairing at the right-hand side is the Weil pairing while the one at the left-hand side is the obvious one

$$\langle (n, \xi), (\widetilde{n}, \widetilde{\xi}) \rangle = \sum_{i=1}^{g} \widetilde{\xi}_i^{n_i} - \sum_{i=1}^{g} \xi_i^{\widetilde{n}_i}.$$

The natural maps

$$\mathcal{X}' \to \mathcal{X}_0 \to \mathcal{X} \to \mathcal{X}^*$$

are defined over $\mathbb{Q}(\mu_N)$. One can prove that the composition $\mathcal{X}' \to \mathcal{X}^*$ is actually an isomorphism defined over $\mathbb{Q}$. This remark belongs to the anonymous referee.

Remark 2.2 The moduli variety $\mathcal{X}^*$ is quite natural both in terms of the Shimura datum and in terms of moduli interpretation. It is curious and a bit strange that it has not appeared in any literature to my best knowledge. For example, it could have naturally been in [3, Table (7.4.3)], as its analogues for $\Gamma_1(N)$ and $\Gamma_0(N)$ are both there.

Remark 2.3 If we let N change, temporarily write $\mathcal{X}(N)$ for $\mathcal{X}$ and take the inverse limit, then the pro-Shimura variety $\mathcal{X} = \varprojlim \mathcal{X}(N)$ is a right $G(\mathbb{A}_f)$-module, but far from connected. On the other hand, $\mathcal{X}^* = \varprojlim \mathcal{X}^*(N) = \mathcal{X}/v(\widehat{\mathbb{Z}}^\times)$ is a connected quotient of $\mathcal{X}$. However, only the normalizer of $v(\widehat{\mathbb{Z}}^\times)$ in $G(\mathbb{A}_f)$, not the whole $G(\mathbb{A}_f)$, can act on $\mathcal{X}^*$.

3 Complex Multiplication and Galois Orbit of a CM Point

Let (E, Φ) be a CM number field with the CM type Φ, and let $(\widetilde{E}, \widetilde{\Phi})$ be the reflex CM field with the reflex CM type. Let M be a Galois extension of $\mathbb{Q}$ containing both E and $\widetilde{E}$. Recall the type-norm on elements

$$\mathrm{N}_\Phi : E^\times \to \widetilde{E}^\times, \quad x \mapsto \prod_{\sigma \in \Phi} \sigma(x),$$

and on ideals

$$\mathrm{N}_\Phi(\mathfrak{a}) = \Big(\prod_{\sigma\in\Phi} \sigma(\mathfrak{a})\mathcal{O}_M\Big) \cap \mathcal{O}_{\widetilde{E}}.$$

Here M is a (any) Galois extension of $\mathbb{Q}$ containing both E and $\widetilde{E}$. For the convenience of the reader, we first recall the well-known main theorem of Shimura and Taniyama on complex multiplication (see [7–8]). A CM abelian variety over a field $L \hookrightarrow \mathbb{C}$ of the CM type (E, Φ) is in this paper a pair (A, ι), where A is an abelian variety over L of dimension $\frac{1}{2}[E:\mathbb{Q}]$, $\iota : \mathcal{O}_E \to \mathrm{End}_L(A)$ is an isomorphism, and there is a $\mathbb{C}$ basis $\{\omega_\sigma, \sigma\in\Phi\}$ on $\Omega_{A/\mathbb{C}}$ such that $i(z)^*\omega_\sigma = \sigma(z)\omega_\sigma$. For a number field E, we denote by E_f the finite adeles of E, and by $\widehat{\mathcal{O}}_E$ the ring of integers of E_f.

Theorem 3.1 (Shimura-Taniyama) *Let* $\mathbf{b} \in \widetilde{E}_f^\times$ *and* $\sigma \in \mathrm{Aut}(\mathbb{C}/\widetilde{E})$ *such that* $\sigma|_{\widetilde{E}^{ab}} = \sigma_{\mathbf{b}^{-1}}$ *via the class field theory* (*the Artin map*). *Here* $\widetilde{E}^{ab}$ *is the maximal abelian extension of* $\widetilde{E}$. *Let* (A, ι) *be a CM abelian variety over* $\mathbb{C}$ *of CM type* (E, Φ). *Then there is an isomorphism* $f : \mathbb{C}^g/\Phi(\mathfrak{a}) \cong A$ *for some fractional ideal* $\mathfrak{a}$ *of* E *over* $\mathbb{C}$. *Fix such an isomorphism* f (*and* $\mathfrak{a}$), *and there is a unique isomorphism* $f' : \mathbb{C}^g/\Phi(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}\,\mathbf{b}) \to A^\sigma$ *over* $\mathbb{C}$ *such that the following diagram commutes:*

$$\begin{tikzcd}
E/\mathfrak{a} \arrow[r, "f\circ\Phi"] \arrow[d, "\cdot\,\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b})"] & A_{tor}\,. \arrow[d, "\sigma"] \\
E/\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b}) \arrow[r, "\Phi\circ f'"] & A^\sigma_{tor}
\end{tikzcd}$$

Here the multiplication by the idele in the column makes sense via the canonical isomorphism $E/\mathfrak{a} = \oplus_{\mathfrak{p}} E_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$. *Here* $E_{\mathfrak{p}}$ (*resp.* $\mathfrak{a}_{\mathfrak{p}}$) *is the completion of* E (*resp.* $\mathfrak{a}$) *with respect to the prime ideal* $\mathfrak{p}$.

A CM point of the CM type (E, Φ) in $\mathcal{X}^*(L)$, for a field $L \subset \mathbb{C}$, is a tuple $(A, \iota, \lambda, \phi)$ where (A, ι) is a CM abelian variety of the CM type (E, Φ) and $(A, \lambda, \phi) \in \mathcal{X}^*(L)$ such that the Rosati involution associated to λ induces the complex conjugation on E. Let $\mathrm{CM}(E, \Phi)$ be the set of CM points in $\mathcal{X}^*(\mathbb{C}) = X(N)$ of the CM type (E, Φ).

Let R be a (communicative) ring, and let V be a free R-module of rank $2g$ with the non-degenerate symplectic form $\langle\,,\,\rangle$. A basis $\vec{a} = (a_1, \cdots, a_{2g})$ is called a similitude symplectic basis if the associated matrix

$$(\langle a_i, a_j\rangle) = \begin{pmatrix} 0 & dI_g \\ -I_g & 0 \end{pmatrix}$$

for some $d \in R^\times$. When $d = 1$, we call it a symplectic basis.

Proposition 3.1 *There are bijections among the following sets:*

(1) *The set* $\mathrm{CM}(E, \Phi) \subset X(N)$ *of CM points of the CM type* (E, Φ).

(2) *The set of points* $[\tau] \in X(N)$ *such that* $\Lambda_\tau = \tau\mathbb{Z}^g + \mathbb{Z}^g \subset \mathbb{C}^g$ *is a* (*projective*) $\mathcal{O}_E$*-module via* $\Phi = \{\sigma_1, \cdots, \sigma_g\}$, *where* E *acts on* $\mathbb{C}^g$ *via* $\iota(z)x = \mathrm{diag}(\sigma_1(z), \cdots, \sigma_g(z))x$ *for* $z \in E$ *and* $x \in \mathbb{C}^g$.

(3) *The set of equivalence classes of* $(\mathfrak{a}, \xi, \vec{a})$, *where* $\mathfrak{a}$ *is a fractional ideal of* E, *and* $\xi \in E^\times$ *such that* $\overline{\xi} = -\xi$ *and* $\mathfrak{a}$ *is integral and self-dual with respect to the symplectic pairing* (*the*

Riemann form)

$$E_\xi : E \times E \to \mathbb{Q}, \quad E_\xi(x,y) = \mathrm{tr}_{E/\mathbb{Q}}\, \xi x\overline{y}, \tag{3.1}$$

i.e., $\xi \partial_E \mathfrak{a}\overline{\mathfrak{a}} = \mathcal{O}_E$, *where* ∂_E *is different from* E. $\vec{a} = (a_1, \cdots, a_{2g})$ *is an ordered symplectic basis of* $\mathfrak{a}$ *with respect to* E_ξ. *Two triples* $(\mathfrak{a}, \xi, \vec{a})$ *and* $(\mathfrak{b}, \eta, \vec{b})$ *are equivalent if there is an* $r \in E^\times$ *and a* $\gamma \in \Gamma(N)$ *such that* $r\overline{r} \in \mathbb{Q}^\times$, $\mathfrak{a} = r\mathfrak{b}$, $\xi = (r\overline{r})^{-1}\eta$, *and* $\vec{a} = r\gamma\vec{b}$.

$(3')$ *The set of equivalence classes of* $(\mathfrak{a}, \xi, \frac{1}{N}\vec{a})$, *where* $\mathfrak{a}$ *is a fractional ideal of* E, $\xi \in E^\times$ *such that* $\overline{\xi} = -\xi$ *and* $\frac{1}{N}\vec{a}$ *is a symplectic basis for* $\frac{1}{N}\mathfrak{a}/\mathfrak{a}$ *with respect to the Weil pairing*

$$\left\langle \frac{x}{N}, \frac{y}{N} \right\rangle_{\mathrm{we}} = E_\xi(x,y) \pmod{N}.$$

Two triples $(\mathfrak{a}, \xi, \frac{1}{N}\vec{a})$ *and* $(\mathfrak{b}, \eta, \frac{1}{N}\vec{b})$ *are equivalent if there is an* $r \in E^\times$ *such that* $r\overline{r} \in \mathbb{Q}^\times$, $\mathfrak{a} = r\mathfrak{b}$, $\xi = (r\overline{r})^{-1}\eta$, *and* $\frac{1}{N}\vec{a} = \frac{1}{N}r\vec{b}$ *(i.e.,* $\vec{a} \equiv r\vec{b} (\mathrm{mod}\ N)$*).*

(4) *The set of equivalence classes of triples* $(A_\mathfrak{a}, E_\xi, \frac{1}{N}\vec{a})$ *where* $A_\mathfrak{a} = \mathbb{C}^g/\Phi(\mathfrak{a})$ *is a CM abelian variety of the CM type* (E, Φ) *over* $\mathbb{C}$, E_ξ, *as defined in* (3.1), *is a Riemann form on* $A_\mathfrak{a}$, *which gives a principally polarization on* $A_\mathfrak{a}$, *and* $\frac{1}{N}\vec{a}$ *is a similitude symplectic basis of* $A_\mathfrak{a}[N] = \frac{1}{N}\mathfrak{a}/\mathfrak{a}$ *with respect to the Weil pairing:*

$$\left\langle \frac{x}{N}, \frac{y}{N} \right\rangle_{\mathrm{we}} = E_\xi(x,y) \pmod{N}.$$

Two triples $(A_\mathfrak{a}, E_\xi, \vec{a})$ *and* $(A_\mathfrak{b}, E_\eta, \vec{b})$ *are equivalent if there is an* $r \in E$ *such that* $r\overline{r} \in \mathbb{Q}^\times$, $\mathfrak{a} = r\mathfrak{b}$, $\xi = (r\overline{r})^{-1}\eta$, *and* $\frac{1}{N}\vec{a} = v(d)(r\vec{b})$ *in* $\frac{1}{N}\mathfrak{a}/\mathfrak{a}$ *for some* $d \in (\mathbb{Z}/N)^\times$.

Proof (Sketch) The bijection between (1) and (3) follows from $X(N) = \mathcal{X}_0(\mathbb{C})$ and Theorem 3.1. The bijection between (1) and (4) follows from $X(N) = \mathcal{X}^*(\mathbb{C})$ and Theorem 3.1. The bijection between (3) and $(3')$ is due to the fact that $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N)$ is surjective. Now we describe the bijection between (2) and (3). Recall that $\tau \in X(N) = \mathcal{X}_0(\mathbb{C})$ gives the triple $(A_\tau, E_\tau, \frac{1}{N}\vec{e}_\tau)$, where $A_\tau = \mathbb{C}^g/\Lambda_\tau$ with $\Lambda_\tau = \tau\mathbb{Z}^g + \mathbb{Z}^g$ and the principal polarization $E_\tau = \Im H_\tau$, where

$$H_\tau(x,y) = x^t \Im(\tau)^{-1}\overline{y}$$

is the associated positive definite Hermitian form on $\mathbb{C}^g$, and $\vec{e}_\tau = (e_i)_{1 \le i \le 2g}$ with

$$(e_1, e_2, \cdots, e_g) = \tau, \quad (e_{g+1}, \cdots, e_{2g}) = I_g.$$

Notice that $\vec{e}_\tau$ is a symplectic basis of Λ_τ with respect to E_τ, and that $H_\tau(x,y) = E_\tau(ix,y) + iE_\tau(x,y)$ (see for example [2, 7]).

Given a triple $(\mathfrak{a}, \xi, \vec{a})$ in (3), let $\tau = (\Phi(a_{g+1}), \cdots, \Phi(a_{2g}))^{-1}(\Phi(a_1), \cdots, \Phi(a_g))$, also denoted by $\tau(\mathfrak{a}, \xi, \vec{a})$. Then

$$f : A_\tau \cong A_\mathfrak{a}, \quad f(z) = (\Phi(a_{g+1}), \cdots, \Phi(a_{2g}))z,$$

which sends $\vec{e}_\tau$ to $\vec{a}$. So $(A_\tau, E_\tau, \frac{1}{N}\vec{e}_\tau) = (A_\mathfrak{a}, E_\xi, \frac{1}{N}\vec{a}) \in \mathcal{X}_0(\mathbb{C}) = X(N)$. Via the map f, $\Lambda_\tau \cong \Phi(\mathfrak{a})$ becomes an $\mathcal{O}_E$-module.

Conversely, if Λ_τ is an $\mathcal{O}_E$-module via Φ, then it is finitely generated, torsion-free and thus projective of rank 1 (comparing with the $\mathbb{Z}$-rank). So there is a fractional ideal $\mathfrak{a}$ of E and an

$\mathcal{O}_E$-module isomorphism $f : \Phi(\mathfrak{a}) \cong \Lambda_\tau$, which extends to an isomorphism $f : A_{\mathfrak{a}} \cong A_\tau$. The Riemann form E_τ on Λ_τ gives a self-dual sympletic form on $\mathfrak{a}$. So there is ξ such that $\mathfrak{a}$ is E_ξ-self-dual, and that $\vec{a} = \Phi^{-1}f^{-1}(\vec{e_\tau})$ is a symplectic basis of $\mathfrak{a}$. That is $\tau = \tau(\mathfrak{a}, \xi, \vec{a})$. This gives the bijection between (2) and (3).

We will identify each set in Proposition 3.1 with $\mathrm{CM}(E, \Phi)$. Given $(\mathfrak{a}, \xi, \vec{a}) \in \mathrm{CM}(E, \Phi)$, we write the associated τ in $X(N)$ as $\tau = \tau(\mathfrak{a}, \xi, \vec{a})$. It is given by

$$\tau = (\Phi(a_{g+1}), \cdots, \Phi(a_{2g}))^{-1}(\Phi(a_1), \cdots, \Phi(a_g)). \tag{3.2}$$

Viewing $\vec{a}$ as a $\mathbb{Q}$-basis of E, one obtains an embedding

$$\epsilon : E^\times \to \mathrm{GL}_{2g}(\mathbb{Q}), \quad \epsilon(z)a_i = za_i, \tag{3.3}$$

and a map

$$g = g(\mathfrak{a}, \xi, \vec{a}) : \widetilde{E}^\times \to \mathrm{GSp}_g(\mathbb{Q})^+, \quad g(z) = \epsilon(\mathrm{N}_{\widetilde{\Phi}}(z)). \tag{3.4}$$

The map is well-defined as

$$E_\xi(g(z)(a_i), g(z)(a_j)) = E_\xi(\mathrm{N}_{\widetilde{\Phi}}(z)a_i, \mathrm{N}_{\widetilde{\Phi}}(z)a_j) = \mathrm{N}_{\widetilde{\Phi}}(z)\overline{\mathrm{N}_{\widetilde{\Phi}}(z)}E_\xi(a_i, a_j) = \mathrm{N}(z)E_\xi(a_i, a_j).$$

One has further $\mu(g(z)) = \mathrm{N}(z)$. The maps g and ϵ depend on the point τ.

Let $\mathrm{Cl}(\widetilde{\Phi}, N)$ be the type-class group of modulus N, defined as the quotient of all fractional ideals of $\widetilde{E}$ prime to N by the subgroup

$$P(\widetilde{\Phi}, N) = \{\mathfrak{a} \subset \widetilde{E} : \mathrm{N}_{\widetilde{\Phi}}(\mathfrak{a}) = \mu\mathcal{O}_E, \text{ for some } \mu \equiv 1 \pmod{N}, \ \mu\overline{\mu} = \mathrm{N}(\mathfrak{a})\}.$$

Let $H(\widetilde{\Phi}, N)$ be the associated type-class field of $\widetilde{E}$. For a number field E, we write E_f as its finite adeles and $\widehat{\mathcal{O}}_E$ as the ring of integers of E_f. The following isomorphism is well-known:

$$\mathrm{Cl}(\widetilde{\Phi}, N) \cong \widetilde{E}_f^\times / U(\widetilde{\Phi}, N), \quad [\mathfrak{b}] \mapsto [\mathbf{b}], \tag{3.5}$$

where $\mathbf{b} \in \widetilde{E}_f^\times$ satisfies $(\mathbf{b}) = \mathbf{b}\widehat{\mathcal{O}}_{\widetilde{E}} \cap \widetilde{E} = \mathfrak{b}$ and $\mathbf{b}_{\mathfrak{p}} \equiv 1 \pmod{N}$ for all $\mathfrak{p}|N$. Here

$$U(\widetilde{\Phi}, N) = \{x \in \widetilde{E}_f^\times : \mathrm{N}_{\widetilde{\Phi}}(x) \in E^\times((1 + N\widehat{\mathcal{O}}_E) \cap \widehat{\mathcal{O}}_E^\times)\}.$$

Proposition 3.2 (1) *For every CM point $\tau = \tau(\mathfrak{a}, \xi, \vec{a}) \in \mathcal{X}_0(\mathbb{C})$, its field of definition is the class field $H(\widetilde{\Phi}, N)$.*

(2) *For a CM point $\tau = \tau(\mathfrak{a}, \xi, \vec{a}) \in \mathcal{X}^*(\mathbb{C})$, its field of definition is the class field $H^*(\widetilde{\Phi}, N)$ associated to the class group $\mathrm{Cl}^*(\widetilde{\Phi}, N) = \widetilde{E}_f^\times / U^*(\widetilde{\Phi}, N)$, where*

$$U^*(\widetilde{\Phi}, N) = \{\mathbf{b} \in \widetilde{E}_f^\times : \mathrm{N}_{\widetilde{\Phi}}(\mathbf{b}) = \alpha u : \alpha \in E^\times, \alpha\overline{\alpha} = \mathrm{N}(\mathfrak{b}), \epsilon(u) \in K^*(N)\}.$$

Proof This proposition is a direct consequence of Theorem 3.1 and we give a sketch of (2) for convenience. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ with $\sigma|_{H^*(\widetilde{\Phi}, N)} = \sigma_{\mathbf{b}^{-1}}$ via the class field theory. Here we use the normalization in [7] for the Artin map, i.e., $\sigma_{\mathfrak{p}}(x) \equiv x^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{p}}$. Let $\mathfrak{b} = (\mathbf{b})$ be the ideal of $\mathbf{b}$. Assume $\tau^\sigma = \tau$, and then $A_{\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})} \cong A_{\mathfrak{a}}$. So $\mathrm{N}_{\widetilde{\Phi}}\, \mathfrak{b} = \alpha \mathcal{O}_E$ for some $\alpha \in E^\times$. Write $\mathrm{N}_{\widetilde{\Phi}}\, \mathbf{b} = \alpha u$ with $u \in \widehat{\mathcal{O}}_E^\times$. So we have

$$\tau^\sigma = \tau\Big(\mathfrak{a}, \xi \frac{\alpha\overline{\alpha}}{\mathrm{N}(\mathfrak{b})}, \frac{1}{N} u\vec{a}\Big) = \tau\Big(\mathfrak{a}, \xi, \frac{1}{N}\vec{a}\Big).$$

This implies that we can change α properly to make $\alpha\overline{\alpha} = \mathrm{N}(\mathfrak{b})$. Since the two symplectic similitude bases $\frac{1}{N} u\vec{a}$ and $\frac{1}{N}\vec{a}$ of $\frac{1}{N}\mathfrak{a}/\mathfrak{a}$ with respect to the Weil pairing have to be equivalent, i.e., differing only by $v(d)$ for some $d \in (\mathbb{Z}/N)^\times$, one has $\epsilon(u) \in K^*(N)$. The other way is the same.

Noticing that $\mu_N \subset H(\widetilde{\Phi}, N)$ and $\mathcal{X}_0 = \mathcal{X}^*_{\mathbb{Q}(\mu_N)}$, one has that $H(\widetilde{\Phi}, N) = H^*(\widetilde{\Phi}, N)(\mu_N)$. We remark that the class field $H^*(\widetilde{\Phi}, N)$ might depend on the map ϵ in (3.3), and thus the CM point τ. It is an interesting question whether and how $H^*(\widetilde{\Phi}, N)$ really depends on τ. For example, do different Galois orbits in $\mathrm{CM}(E, \Phi)$ have the same cardinality? (or does the index $[H^*(\widetilde{\Phi}, N) : \widetilde{E}]$ depend on τ?)

Theorem 3.2 *Let $\tau = \tau(\mathfrak{a}, \xi, \vec{a}) \in \mathrm{CM}(E, \Phi) \in X(N)(\mathbb{C})$. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/\widetilde{E})$ and $[\mathfrak{b}] \in \mathrm{Cl}(\widetilde{\Phi}, N)$ such that $\sigma|_{H(\widetilde{\Phi},N)} = \sigma_{\mathfrak{b}^{-1}}$ via the class field theory. Choose an (ordered) symplectic basis $\vec{c}$ of $\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})$ with respect to the symplectic form $E_{\xi\,\mathrm{N}(\mathfrak{b})^{-1}}$ such that*

$$c_i \equiv a_i \pmod N, \quad 1 \le i \le g, \quad c_i \equiv a_i\,\mathrm{N}(\mathfrak{b}) \pmod N, \quad g+1 \le i \le 2g.$$

Then

$$\tau(\mathfrak{a}, \xi, \vec{a})^\sigma = \tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}), \xi\,\mathrm{N}(\mathfrak{b})^{-1}, \vec{c}).$$

Proof Choose $\mathbf{b} \in \widetilde{E}_f^\times$ such that $(\mathbf{b}) = \mathfrak{b}$ and $\mathbf{b}_{\mathfrak{p}} = 1$ for all primes of $\widetilde{E}$ above N, as in (3.5). We may assume that $\mathfrak{b}$ is integral. Then Theorem 3.1 implies

$$\Big(A_{\mathfrak{a}}, E_\xi, \frac{1}{N}\vec{a}\Big)^\sigma = \Big(A_{\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})}, E_{\xi\,\mathrm{N}(\mathfrak{b})^{-1}}, \frac{1}{N}\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b})\vec{a}\Big).$$

Notice

$$\begin{aligned}\Big\langle \frac{1}{N}\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b})a_i, \frac{1}{N}\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b})a_j\Big\rangle_{\mathrm{we}} &\equiv \frac{\mathrm{N}(\mathbf{b})}{\mathrm{N}(\mathfrak{b})} E_\xi(a_i, a_j) \pmod N \\ &\equiv \frac{1}{\mathrm{N}(\mathfrak{b})} E_\xi(a_i, a_j) \pmod N.\end{aligned}$$

So one has in $(\frac{1}{N}\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}))/\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})$,

$$\frac{1}{N}c_i = \frac{1}{N}\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b})a_i, \quad 1 \le i \le g$$

and

$$\frac{1}{N}c_i = \frac{1}{N}\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b})\,\mathrm{N}(\mathfrak{b})a_i, \quad g+1 \le i \le 2g.$$

So $\frac{1}{N}\vec{c} = v(\mathrm{N}(\mathfrak{b}))\big(\frac{1}{N}\mathrm{N}_{\widetilde{\Phi}}(\mathbf{b})\vec{a}\big)$. Indeed, for a prime $\mathfrak{p}$ of E above N, it is true by our choice of $\vec{c}$ and by the fact $\mathrm{N}_{\widetilde{\Phi}}\,\mathbf{b}_{\mathfrak{p}} = 1$. For $\mathfrak{p} \nmid N$, both sides are zero. Therefore,

$$\Big(A_{\mathfrak{a}}, E_\xi, \frac{1}{N}\vec{a}\Big)^\sigma = (A_{\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})}, E_{\xi\,\mathrm{N}(\mathfrak{b})^{-1}}, \vec{c}),$$

i.e.,

$$\tau(\mathfrak{a},\xi,\vec{a})^{\sigma}=\tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}),\xi\,\mathrm{N}(\mathfrak{b})^{-1},\vec{c}).$$

Let $f(\tau)$ be a memormorphic modular function on $\mathbb{H}_g$ for $\Gamma(N)$, viewed also as a rational function on $\mathcal{X}^*(\mathbb{C})$, and let

$$f(\tau)=\sum_{T\in\mathrm{Sym}_g(\mathbb{Z})^*}c(T)q_N^{\mathrm{T}}$$

be the Fourier expansion of $f(\tau)$ with $c(n)\in\mathbb{C}$ and $q_N^{\mathrm{T}}=e(\frac{1}{N}\operatorname{tr}T\tau)$. For $\sigma\in\mathrm{Aut}(\mathbb{C})$, f^{σ}, as a rational function on $\mathcal{X}^*(\mathbb{C})$, is defined to satisfy the following condition: For every $P\in\mathcal{X}^*(\mathbb{C})$, one has

$$f(P)^{\sigma}=f^{\sigma}(P^{\sigma}).$$

By the q-expansion principle, f^{σ} has the following Fourier expansion:

$$f^{\sigma}(\tau)=\sum_{T}c(T)^{\sigma}q_N^{\mathrm{T}}.$$

Now the following explicit Galois action formula on CM values follows directly from Theorems 3.1–3.2.

Corollary 3.1 *Let $f(\tau)$ be a memomorphic modular function on $\mathbb{H}_g$ for $\Gamma(N)$ (also momomorphic at cusps). Let $\tau=\tau(\mathfrak{a},\xi,\vec{a})\in\mathrm{CM}(E,\Phi)$ be a CM point on $X(N)$. Let $\sigma\in\mathrm{Aut}(\mathbb{C}/\widetilde{E})$, and let $[\mathfrak{b}]\in\mathrm{Cl}(\widetilde{\Phi},N)$ such that $\sigma|_{\widetilde{E}^{ab}}=\sigma_{\mathfrak{b}^{-1}}$. Then*

$$f(\tau)^{\sigma}=f^{\sigma}(\tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}\,\mathfrak{b},\xi\,\mathrm{N}(\mathfrak{b})^{-1},\vec{c})),$$

where $\tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}\,\mathfrak{b},\xi\,\mathrm{N}(\mathfrak{b})^{-1},\vec{c})=\tau^{\sigma}$ is given as in Theorem 3.2.

Proof Let X be a toriodal compactification of $\mathcal{X}^*/\mathbb{Q}$ which is a projective algebraic variety. By our assumption, f is a rational function on X. So $f(\tau)^{\sigma}=f^{\sigma}(\tau^{\sigma})$, and the first claim follows directly from Theorem 3.1.

The case $N=2$ and $g=2$ was used in [1] and is the initial motivation for this work.

Remark 3.1 It should be very interesting to work out the whole Galois orbit of a CM point under $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. It should be doable by using Deligne and Langlands' generalization of Theorem 3.1 (see [4]).

Remark 3.2 There is another group acting on $\mathrm{CM}(E,\Phi)$. Let

$$C_0(E,N)=\frac{\{(\mathfrak{b},\alpha\in\mathbb{Q}_{>0},b\in\mathfrak{b}/N\mathfrak{b}):\mathrm{N}_{E/F}\,\mathfrak{b}=\alpha\mathcal{O}_F,b\bar{b}\alpha^{-1}\equiv1\ (\mathrm{mod}\ N)\}}{\{(\xi\mathcal{O}_E,\xi\bar{\xi},\xi):\xi\in E^{\times},\xi\equiv1\ (\mathrm{mod}\ N)\}}.$$

The action is given as follows:

$$(\mathfrak{b},\alpha,b)\Big(\mathfrak{a},\xi,\frac{1}{N}\vec{a}\Big)=\Big(\mathfrak{a}\mathfrak{b},\alpha^{-1}\xi,\frac{b}{N}\vec{a}\Big).$$

4 Reciprocity Law

In this section, we will use Corollary 3.1 to give another proof of Streng's explicit Shimura reciprocity law and the original Shimura reciprocity law. We need some notations before stating their theorems (see [5–6, 10]). We will mainly follow [10] in the review and refer to it for more details. Let $\mathcal{F}_N$ be the field of meromorphic Siegel modular functions $\frac{g_1}{g_2}$, where g_i $(i = 1, 2)$ are holomorphic Siegel modular forms of level N and of the equal weight with Fourier coefficients in $\mathbb{Q}(\mu_N)$, and $g_2 \neq 0$. By the q-expansion principle, one has $\mathcal{F}_N = \mathbb{Q}(\mu_N)(\mathcal{X}_0) = \mathbb{Q}(\mu_N)(\mathcal{X}^*)$. Let $\mathcal{F}_\infty = \cup \mathcal{F}_N$. The following proposition is due to Shimura (see [10, Propositions 2.1 and 3.1]). Let $G(\mathbb{R})^+$ be the subgroup of $G(\mathbb{R})$ with $\mu(g) > 0$, $G(\mathbb{A})^+ = G(\mathbb{A}_f) \times G(\mathbb{R})^+$ and $G(\mathbb{Q})^+ = G(\mathbb{R})^+ \cap G(\mathbb{Q})$. Recall $G = \mathrm{GSp}_g$ (GSp_{2g} in Streng's notation).

Proposition 4.1 (a) *There is a unique action of $G(\mathbb{A})^+$ on $\mathcal{F}_\infty$ satisfying the following conditions:*

(1) *For $\gamma \in G(\mathbb{Q})^+$, one has $f^\gamma(\tau) = f(\gamma\tau)$.*

(2) *For $x \in \mathbb{A}^\times$, one has $f^{v(x)} = f^{\sigma_x}$. Here $\sigma_x \in \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}$ is the Artin map image of x via the class field theory, $v(x) = \mathrm{diag}(I_g, xI_g)$, and $f^\sigma(\tau)$ is the new modular function with σ acting on the Fourier coefficients of f.*

(3) *For any $N \geq 1$, the group $K(N) \times G(\mathbb{R})^\times$ acts on $\mathcal{F}_N$ trivially. Here we recall that $K(N)$ is the compact open subgroup of $G(\mathbb{A}_f)$ defining $\mathcal{X}$.*

(b) *There is a unique action of $G(\mathbb{Z}/N)$ on $\mathcal{F}_N$ as follows:*

(1) *The action of $\mathrm{Sp}_g(\mathbb{Z}/N)$ on $\mathcal{F}_N$ is given by $f^{\gamma (\mathrm{mod}\ N)} = f^\gamma$ for $\gamma \in \mathrm{Sp}_g(\mathbb{Z})$, where f^γ is given by* (a)(1) *above.*

(2) *For any $x \in (\mathbb{Z}/N)^\times$, $f^{v(x)} = f^{\sigma_x}$.*

Now we are ready to give a direct proof of Streng's explicit reciprocity law (without using Shimura's reciprocity law). Please note that we only deal with the case of the maximal order of E while Shimura and Streng dealt with the general case, though our method works in general too.

Theorem 4.1 (see [10, Theorem 2.4]) *Let $\tau = \tau(\mathfrak{a}, \xi, \vec{a}) \in X(N)$ be a CM point of the CM type (E, Φ) as before. Let $\sigma = \sigma_{\mathfrak{b}^{-1}} \in \mathrm{Gal}(H(\widetilde{\Phi}, N)/\widetilde{E})$. Let $\vec{b}$ be a symplectic basis of $\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})$ with respect to $E_{\xi\,\mathrm{N}(\mathfrak{b})^{-1}}$. Let $M \in \mathrm{GSp}_g(\mathbb{Q})^+$ such that $M(\vec{a}) = \vec{b}$. Then M is N-integral and invertiable modulo N. Let $U = M^{-1} (\mathrm{mod}\ N) \in \mathrm{GSp}_g(\mathbb{Z}/N)$. Then for any $f \in \mathcal{F}_N$, one has*

$$f(\tau)^\sigma = f^U(M\tau).$$

Proof By Corollary 3.1, one has

$$f(\tau)^\sigma = f^\sigma(\tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}), \xi d, \vec{c})),$$

where $d = \mathrm{N}(\mathfrak{b})^{-1}$ and $\vec{c}$ is the symplectic basis of $\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})$ with respect to $E_{d\xi}$ given in Theorem 3.2. Let $\mathrm{Cl}(\mathbb{Z}, N)$ be the ray class group of $\mathbb{Q}$ with modulus N, and its associated class field is $\mathbb{Q}(\mu_N)$. Notice that the norm map from $\mathrm{Cl}(\widetilde{\Phi}, N)$ to $\mathrm{Cl}(\mathbb{Z}, N)$ is surjective which also explains $\mathbb{Q}(\mu_N) \subset H(\widetilde{\Phi}, N)$. So by the class field theory, one has $\mathbb{Q}(\mu_N) \subset H(\widetilde{\Phi}, N)$, and

$$\sigma_{\mathfrak{b}^{-1}}|_{\mathbb{Q}(\mu_N)} = \sigma_{\mathrm{N}(\mathfrak{b})^{-1}}|_{\mathbb{Q}(\mu_N)}.$$

So $f^\sigma = f^{\sigma_d} = f^{v(d)}$, and

$$f(\tau)^\sigma = f^{v(d)}(\tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}), \xi d, \vec{c})).$$

Let $\gamma \in \mathrm{Sp}_g(\mathbb{Z})$ such that $\gamma(\vec{b}) = \vec{c}$. Then $\gamma M(\tau) = \tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}), \xi d, \vec{c})$. On the other hand, $M\vec{a} = \vec{b}$ implies $\mu(M) = d^{-1}$ and thus $\mu(U) = d \pmod N$, and $U(\vec{b}) = \vec{a} \pmod N$. So

$$U = v(d)\gamma \pmod N.$$

Therefore

$$f^U(M\tau) = f^{v(d)}(\gamma M\tau) = f^{v(d)}(\tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}), \xi d, \vec{c})) = f(\tau)^\sigma$$

as claimed.

Finally, we derive Shimura's reciprocity law in its original adelic form (see [6, P. 57]). Let $\tau = \tau(\mathfrak{a}, \xi, \vec{a}) \in \mathrm{CM}(E, \Phi) \in X(N)$ as before. Recall the maps ϵ and g in (3.3)–(3.4). The following is the Shimura's reciprocity law (see [6, P. 57], see also [10, Theorem 3.4]).

Theorem 4.2 (Shimura) *Let $\tau = \tau(\mathfrak{a}, \xi, \vec{a}) \in \mathrm{CM}(E, \Phi) \in X(N)$ be a CM point of the CM type (E, Φ), and let $g : \widetilde{E}_{\mathbb{A}}^\times \to \mathrm{GSp}_g(\mathbb{A})^+$ be the adelization of the map g defined in* (3.4). *Then for any $f \in \mathcal{F}_\infty$ such that $f(\tau)$ is finite, and for any $\mathbf{b} \in \widetilde{E}_{\mathbb{A}}^\times$, we have*

$$f(\tau) \in \widetilde{E}^{ab}, \quad f(\tau)^{\sigma_{\mathbf{b}^{-1}}} = f^{g(\mathbf{b})}(\tau).$$

Proof We can choose N big enough so that $f \in \mathcal{F}_N$, and then view τ as a CM point on $X(N)$. So $f(\tau) \in H(\widetilde{\Phi}, N)$, and both sides of the identity depend only on the idele class $[\mathbf{b}] \in \widetilde{E}^\times \backslash \widetilde{E}_f^\times / U(\widetilde{\Phi}, N)$. Therefore we may assume that $\mathbf{b}_{\mathfrak{p}} = 1$ for all primes of $\widetilde{E}$ above N, and let $\mathfrak{b} = (\mathbf{b})$ be the fractional ideal of $\widetilde{E}$ associated to $\mathbf{b}$. Let $\tau^\sigma = (\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}), \xi\,\mathrm{N}(\mathfrak{b})^{-1}, \vec{c})$ as in Theorem 3.2. We write $\widehat{\mathfrak{a}} = \mathfrak{a} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, and $g = g(\mathbf{b})$. Then $\widehat{\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b})}$ has two similitude symplectic $\widehat{\mathbb{Z}}$-bases $g(\vec{a}) = \mathrm{N}_{\widetilde{\Phi}}\,\mathbf{b}\vec{a}$ and $\vec{c}$ (with respect to E_ξ). So there is $\gamma \in \mathrm{GSp}_g(\widehat{\mathbb{Z}})$ such that $\gamma^{-1} g(\vec{a}) = \vec{c}$ and $\mu(\gamma^{-1}) = \frac{\mathrm{N}(\mathfrak{b})}{\mathrm{N}(\mathbf{b})} \in \widehat{\mathbb{Z}}^\times$. Let $M = \gamma^{-1} g \in \mathrm{GSp}_g(\mathbb{A}_f)$ with $\mu(M) = \mathrm{N}(\mathfrak{b})$. Since $\vec{a}$ and $\vec{c} = M(\vec{a})$ are both similitude symplectic $\mathbb{Q}$-bases of E (with respect to E_ξ), one has $M \in \mathrm{GSp}_g(\mathbb{Q})^+$. Write $\gamma = \gamma_1 v(\frac{\mathrm{N}(\mathbf{b})}{\mathrm{N}(\mathfrak{b})})$ with $\gamma_1 \in \mathrm{Sp}_g(\widehat{\mathbb{Z}})$. Recalling the condition on $\vec{c}$ in Theorem 3.1 and that $\mathbf{b}_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \mid N$, one sees that γ_1 maps $\vec{a}$ to $\vec{a}$ modulo N. So $\gamma_1 \equiv 1 \pmod N$. Now $g = \gamma_1 v(\frac{\mathrm{N}(\mathbf{b})}{\mathrm{N}(\mathfrak{b})}) M$ (since we write elements in G as maps in the proof, this order of decomposition is correct), and one has by Proposition 4.1 that

$$f^g(\tau) = f^{v(\frac{\mathrm{N}(\mathbf{b})}{\mathrm{N}(\mathfrak{b})})}(M\tau) = f^{\sigma_{\mathrm{N}(\mathfrak{b})^{-1}}}(\tau(\mathfrak{a}\,\mathrm{N}_{\widetilde{\Phi}}(\mathfrak{b}), \xi\,\mathrm{N}(\mathfrak{b})^{-1}, \vec{c})) = f(\tau)^\sigma$$

as claimed.

Acknowledgements This work was motivated while I was working with Castello, Deines-Shartz, and Lauter during my Microsoft visit in Fall 2013. I thank them for the inspiration and the joint work. During that time, I did not realize the existence of Streng's excellent work on explicit Shimura reciprocity law in [10] (otherwise, this note would not have existed). My approach is very different from his. The last section of this work is inspired by his work. I thank Conrad, B., Howard, B., Nicole, M. H., Rapoport, M., and Yuan Xinyi for the helpful discussions. This work was done during my visit to Microsoft in Fall 2013 and to the MPIM-Bonn in Spring 2014. I thank both institutes for providing me with the excellent working conditions. Finally, I thank the anonymous referee for his/her careful reading and suggestions/comments on the earlier versions of this paper.

References

[1] Costello, C., Deines-Schartz, A., Lauter, K. and Yang, T. H., Constructing abelian surfaces for cryptography via Rosenhain invariants, *LMS J. Comput. Math. Ser. A*, **17**, 2014, 157–180.

[2] Genestier, A. and Ngo, B. C., Lectures on Shimura varieties, Asian-French Summer School on Algebraic Geometry and Number Theory, Volume I, 187–236, Panor. Synth., 29, Soc. Math. France, Paris, 2009.

[3] Katz, N. and Mazur, B., Arithmetic moduli of elliptic curves, Ann. Math. Studies, **108**, Princeton University Press, 1985.

[4] Lang, S., Complex Multiplication, GTM, 255, Springer-Verlag, New York, 1983.

[5] Shimura, G., On canonical models of bounded symmetric domains I, *Ann. Math.*, **91**, 1970, 144–222, II, **92**, 1970, 528–549.

[6] Shimura, G., On certain reciprocity laws for theta functions and modular functions, *Acta Math.*, **141**, 1978, 35–71.

[7] Shimura, G., Abelian Vareities with Complex Multiplication and Modular Forms, Princeton University Press, princeton, 1998.

[8] Shimura, G. and Taniyama, Y., Complext Multiplication of Abelian Varieties and Its Applications to Number Theory, Publ. Math. Soc. Japan, **6**, The Mathematical Society of Japan, Tokyo, 1961.

[9] Silverman, J. H., Advanced Topics in the Arithmetic of Elliptic Curves, GTM 151, Springer-Verlag, New York, 1994.

[10] Streng, M., An explicit version of Shimura's reciprocity law for the Siegel modular functions, preprint, 2012.