

ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

TREVOR ARNOLD

As a prelude to the general theory of complex multiplication of abelian varieties, we discuss the arithmetic of elliptic curves with complex multiplication (CM). The goal of these notes is to provide a cohesive summary of the classical theory. The material presented here comes from a variety of sources, notably Gross [3], Lang [5], Serre [6], Shimura [7], and Silverman [9, Ch. II]; we make no claims to originality. We assume a familiarity with elliptic curves (our reference for basic facts is Silverman's book [8]), algebraic geometry (on the level of Hartshorne's book), and algebraic number theory (through class field theory). In order to avoid duplication of effort, we also assume the Main Theorem of CM (stated in §3), as it will be the subject of a later set of notes, [2, Thm. 7.3].

CONTENTS

1. Elliptic curves over \mathbf{C} and rationality	1
2. Potentially good reduction and the integrality of j	5
3. The Main Theorem of CM and consequences	5
4. Ring class fields and abelian extensions	13
References	16

1. ELLIPTIC CURVES OVER \mathbf{C} AND RATIONALITY

Suppose that $L \subseteq \mathbf{C}$ is a subfield and that E/L is an elliptic curve. Recall that the (rational) endomorphism ring $\text{End}_L E$ of E is isomorphic either to \mathbf{Z} or to an order¹ \mathcal{O} in a quadratic imaginary field K/\mathbf{Q} . In the latter case, we say that E has CM by K (or by \mathcal{O}). If E has CM by K , then $\text{End}_L E = \text{End}_{\mathbf{C}} E$ and a choice of isomorphism $i : K \xrightarrow{\cong} (\text{End}_{\mathbf{C}} E) \otimes \mathbf{Q}$ determines an embedding $\tau = \tau(i) : K \hookrightarrow \mathbf{C}$ such that the diagram

$$\begin{array}{ccc}
 (\text{End}_{\mathbf{C}} E) \otimes \mathbf{Q} & \xleftarrow{\text{can.}} & \text{End}_{\mathbf{C}} \text{Tan}_0 E_{\mathbf{C}} \\
 \uparrow i & & \parallel \text{can.} \\
 K & \xleftarrow{\tau} & \mathbf{C}
 \end{array}$$

commutes, where $\text{Tan}_0 E_{\mathbf{C}}$ is the tangent space of $E_{\mathbf{C}}$ at the identity (it is a \mathbf{C} -vector space of dimension 1, whence the rightmost equality). The one-element set $\{\tau\}$ is the CM-type of the pair (E, i) . In what follows, we fix for every elliptic curve E/L with CM by K a choice of $i : K \xrightarrow{\cong} (\text{End}_{\mathbf{C}} E) \otimes \mathbf{Q}$ and set $K^* = \tau(K) \subseteq \mathbf{C}$.

¹Recall that an *order* in a number field K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ such that $\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Q} = K$.

Note that it may be the case that E/L does not have CM by K but that $E_{L'}$ does have CM by K for some extension L' of L in \mathbf{C} . In fact, we show later (Corollary 6) that if E/L is such that $E_{\mathbf{C}}$ has CM by K , then E has CM by K if and only if $L \supseteq K^*$. In what follows, we are (somewhat pedantically) careful to distinguish between the isomorphic fields K and $K^* = \tau(K) \subseteq \mathbf{C}$; in the terminology of the general theory of CM abelian varieties, the former is the CM field and the latter is the reflex field for the CM type $\Phi = \{\tau\}$. Also, we remark here that we make the assumption that $L \subseteq \mathbf{C}$ only for general convenience. The results presented here hold for elliptic curves defined over any field L of characteristic 0; this follows, for example, from ‘‘Lefschetz principle’’ arguments (cf. [8, Ch. VI §6]).

For an order \mathcal{O} , denote by $\text{Cl}(\mathcal{O})$ the set of isomorphism classes of projective \mathcal{O} -modules of generic rank 1. This set becomes a group under tensor product of modules: the inverse of a class $[\Lambda] \in \text{Cl}(\mathcal{O})$ is represented by $\text{Hom}_{\mathcal{O}}(\Lambda, \mathcal{O})$. The following lemma states a few basic properties of orders and their invertible modules, most of which are well-known; the proof of this lemma is only included for completeness and may safely be skipped.

Lemma 1. *Suppose \mathcal{O} is an order in the quadratic imaginary field K .*

- (1) *There is a (unique) positive integer c (called the conductor of \mathcal{O}) such that $\mathcal{O} = \mathbf{Z} + c\mathcal{O}_K$.*
- (2) *Every torsion-free finite \mathcal{O} -module of generic rank 1 is isomorphic to an ideal $\mathfrak{a} \subseteq \mathcal{O}$. In particular, every element of $\text{Cl}(\mathcal{O})$ is represented by an ideal of \mathcal{O} .*
- (3) *If $\Lambda, \Lambda' \subseteq K$ are two finite \mathcal{O} -modules of generic rank 1, then the natural map*

$$\Lambda \otimes_{\mathcal{O}} \Lambda' \longrightarrow \Lambda \cdot \Lambda' : \alpha \otimes \beta \longmapsto \alpha\beta$$

is an \mathcal{O} -module isomorphism. In particular, if $\Lambda \subseteq K$ is a projective \mathcal{O} -module, then

$$\Lambda^{-1} \cong \{\alpha \in K \mid \alpha\Lambda \subseteq \mathcal{O}\}.$$

- (4) *If Λ is a torsion-free finite \mathcal{O} -module of generic rank 1 such that $\text{End}_{\mathcal{O}}(\Lambda) = \mathcal{O}$, then Λ is a projective \mathcal{O} -module.*

Proof. To prove (1), set $c = [\mathcal{O}_K : \mathcal{O}]$. Then we have that $\mathbf{Z} + c\mathcal{O}_K \subseteq \mathcal{O}$. As \mathcal{O}_K admits a \mathbf{Z} -basis of the form $\{1, \alpha\}$, we see that $[\mathcal{O}_K : \mathbf{Z} + c\mathcal{O}_K] = c$, so $\mathbf{Z} + c\mathcal{O}_K = \mathcal{O}$.

For (2), note that the map $\Lambda \rightarrow \Lambda \otimes_{\mathcal{O}} K : \lambda \mapsto \lambda \otimes 1$ is injective, as Λ is a torsion-free \mathcal{O} -module. A choice of isomorphism $\Lambda \otimes_{\mathcal{O}} K \cong K$ therefore yields an \mathcal{O} -module map $\phi : \Lambda \hookrightarrow K$ identifying Λ with an \mathcal{O} -submodule of K . As $\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Q} = K$ and Λ is finitely generated (over \mathbf{Z}), some integer multiple of ϕ is an isomorphism of Λ onto an ideal of \mathcal{O} .

To prove (3), note that the given map $\Lambda \otimes_{\mathcal{O}} \Lambda' \rightarrow \Lambda\Lambda'$ is surjective and \mathcal{O} -linear, so we only need show that it is an injective map of abelian groups. This is clear, since both the domain and codomain are free abelian groups of rank 2.

Finally, we prove (4). For any finite \mathcal{O} -module $M \subseteq K$ of generic rank 1, we define the module M^* to be the dual of M with respect to the trace pairing:

$$M^* = \{k \in K \mid \text{tr}_{K/\mathbf{Q}}(kM) \subseteq \mathbf{Z}\}.$$

It is clear that M^* is an \mathcal{O} -module and one can see easily (for example, by choosing a \mathbf{Z} -basis for M) that M^* is a free \mathbf{Z} -module of rank 2 (and so of generic rank 1 over \mathcal{O}).

and that $(M^*)^* = M$. For such M , we have $\text{End}_{\mathcal{O}}(M) = \{k \in K \mid kM \subseteq M\}$. Using this, we see that

$$\text{End}_{\mathcal{O}}(M) \subseteq \text{End}_{\mathcal{O}}(M^*) \subseteq \text{End}_{\mathcal{O}}(M^{**}) = \text{End}_{\mathcal{O}}(M),$$

so the inclusions are equalities.

Choose as above a \mathbf{Z} -basis for \mathcal{O}_K of the form $\{1, \alpha\}$ for \mathcal{O}_K . Then $\{1, c\alpha\}$ is a \mathbf{Z} -basis for \mathcal{O} . Let $f(x) \in \mathbf{Z}[x]$ be the minimal polynomial for $c\alpha$ over \mathbf{Q} . A direct computation shows that $\mathcal{O}^* = f'(c\alpha)^{-1}\mathcal{O}$, so in particular $\mathcal{O}^* \cong \mathcal{O}$.

If Λ satisfies the hypotheses of (4), then (by (2), for example) we may assume that Λ is an \mathcal{O} -submodule of K . We therefore have that $\mathcal{O} = \text{End}_{\mathcal{O}}(\Lambda) = \text{End}_{\mathcal{O}}(\Lambda^*)$. We now show that $(\Lambda\Lambda^*)^* = \mathcal{O}$. If $\lambda \in (\Lambda\Lambda^*)^*$, then $\text{tr}_{K/\mathbf{Q}}(\lambda\Lambda\Lambda^*) \subseteq \mathbf{Z}$, so by definition of Λ^* we have $\lambda\Lambda^* \subseteq \Lambda^*$, whence $\lambda \in \text{End}_{\mathcal{O}}(\Lambda^*) = \mathcal{O}$. Conversely, suppose $\lambda \in \mathcal{O}$. Then $\lambda\Lambda^* \subseteq \Lambda^*$, so $\text{tr}_{K/\mathbf{Q}}(\lambda\Lambda\Lambda^*) \subseteq \mathbf{Z}$. In conclusion, we have that

$$\Lambda \otimes_{\mathcal{O}} \Lambda^* \cong \Lambda\Lambda^* = \mathcal{O}^* \cong \mathcal{O},$$

which shows that Λ is an invertible, hence projective, \mathcal{O} -module. \square

Let $\text{Ell}(\mathcal{O})$ be the set of \mathbf{C} -isomorphism classes of elliptic curves over \mathbf{C} with CM by \mathcal{O} . Abusing notation, we often describe representatives of classes in $\text{Ell}(\mathcal{O})$ in terms of the associated complex torus. This is justified by the fact that the functor $E \mapsto E(\mathbf{C})$ from the category of elliptic curves over \mathbf{C} to the category of complex tori of dimension 1 is an equivalence, [8, VI.5.1.1]. In particular, every class in $\text{Ell}(\mathcal{O})$ is represented by the elliptic curve associated to a complex torus of the form $(K \otimes \mathbf{R})/\Lambda$ for some lattice $\Lambda \subseteq K \otimes \mathbf{R}$. (Note that $\tau \otimes 1$ is an isomorphism $K \otimes \mathbf{R} \cong \mathbf{C}$.)

Theorem 2. *There is a simply transitive action of $\text{Cl}(\mathcal{O})$ on $\text{Ell}(\mathcal{O})$ such that $[\mathfrak{a}] \cdot [(K \otimes \mathbf{R})/\Lambda] = [(K \otimes \mathbf{R})/\mathfrak{a}^{-1}\Lambda]$ for any ideal $\mathfrak{a} \subseteq \mathcal{O}$ and any complex torus $(K \otimes \mathbf{R})/\Lambda$ with CM by \mathcal{O} .*

Proof. First note that $\mathfrak{a}^{-1}\Lambda$ is a lattice in $K \otimes \mathbf{R}$, as it is a discrete subgroup of $K \otimes \mathbf{R}$ of \mathbf{Z} -rank 2. If $(K \otimes \mathbf{R})/\Lambda \cong (K \otimes \mathbf{R})/\Lambda'$, then Λ and Λ' are homothetic by [8, VI.4.1.1], so $(K \otimes \mathbf{R})/\mathfrak{a}^{-1}\Lambda \cong (K \otimes \mathbf{R})/\mathfrak{a}^{-1}\Lambda'$. Thus, to show that the action described in the statement of the theorem is well-defined, we need to show that if $(K \otimes \mathbf{R})/\Lambda$ has CM by \mathcal{O} , then

- (1) $(K \otimes \mathbf{R})/\mathfrak{a}^{-1}\Lambda$ also has CM by \mathcal{O} and
- (2) $(K \otimes \mathbf{R})/\mathfrak{a}^{-1}\Lambda \cong (K \otimes \mathbf{R})/\mathfrak{b}^{-1}\Lambda$ if and only if $\mathfrak{a} \cong \mathfrak{b}$ as \mathcal{O} -modules.

To prove (1), we use the identification $\text{End}(K \otimes \mathbf{R})/\Lambda = \{\alpha \in (K \otimes \mathbf{R}) \mid \alpha\Lambda \subseteq \Lambda\}$ of [8, VI.5.3]. If we assume that $(K \otimes \mathbf{R})/\Lambda$ has CM by \mathcal{O} , then $\mathcal{O}\Lambda = \Lambda$, so

$$\{\alpha \in K \otimes \mathbf{R} \mid \alpha\Lambda \subseteq \Lambda\} = \{\alpha \in K \otimes \mathbf{R} \mid \alpha\mathfrak{a}^{-1}\Lambda \subseteq \mathfrak{a}^{-1}\Lambda\}.$$

Thus, $\text{End}(K \otimes \mathbf{R})/\Lambda = \text{End}(K \otimes \mathbf{R})/\mathfrak{a}^{-1}\Lambda$.

We now prove (2). By [8, VI.4.1.1], $(K \otimes \mathbf{R})/\mathfrak{a}^{-1}\Lambda \cong (K \otimes \mathbf{R})/\mathfrak{b}^{-1}\Lambda$ if and only if there exists $c \in (K \otimes \mathbf{R})^\times$ such that $c\mathfrak{a}^{-1}\Lambda = \mathfrak{b}^{-1}\Lambda$. This in turn holds if and only if there exists $d \in K$ such that $d\mathfrak{a} = \mathfrak{b}$, i.e., if and only if $\mathfrak{a} \cong \mathfrak{b}$ as \mathcal{O} -modules.

Note that (2) above shows that the given action is faithful, so it remains to check that it is transitive. If $(K \otimes \mathbf{R})/\Lambda$ has CM by \mathcal{O} , then we see that $\text{End}_{\mathcal{O}}(\Lambda) = \mathcal{O}$. Lemma 1(4) thus implies that Λ is a projective \mathcal{O} -module. Therefore, given complex tori $(K \otimes \mathbf{R})/\Lambda$ and $(K \otimes \mathbf{R})/\Lambda'$ with CM by \mathcal{O} , we have $(K \otimes \mathbf{R})/\Lambda' \cong (K \otimes \mathbf{R})/(\Lambda'\Lambda^{-1})\Lambda$, which shows that the action of $\text{Cl}(\mathcal{O})$ on $\text{Ell}(\mathcal{O})$ is transitive. \square

Corollary 3. *Every elliptic curve E with CM by K admits a model over a number field.*

Proof. Let $\sigma \in \text{Aut } \mathbf{C}$ and assume that E has CM by \mathcal{O} . Then E^σ likewise has CM by \mathcal{O} . By the theorem, $\text{Ell}(\mathcal{O})$ is finite, so $\{j(E^\sigma) \mid \sigma \in \text{Aut}(\mathbf{C})\}$ is finite. Thus, as $j(E^\sigma) = j(E)^\sigma$ for $\sigma \in \text{Aut}(\mathbf{C})$, we have $j(E) \in \overline{\mathbf{Q}}$. \square

Corollary 4. $[\mathbf{Q}(j(E)) : \mathbf{Q}] \leq \#\text{Cl}(\mathcal{O})$ for all $E \in \text{Ell}(\mathcal{O})$.

Proof. $\{j(E^\sigma)\} = \{j(E)^\sigma\} \hookrightarrow \text{Ell}(\mathcal{O})$ and $\text{Ell}(\mathcal{O})$ is a principal homogeneous space for $\text{Cl}(\mathcal{O})$. \square

In §4, Corollary 24(3), we show using the Main Theorem of CM that the inequality in Corollary 4 is an equality and identify $K^*(j(E))$ as the ring class field of K^* associated to the order $\tau(\mathcal{O})$. We thereby have complete information about the rationality of CM elliptic curves. The following results describe rationality properties of endomorphisms. Given an element $\sigma \in \text{Aut}(\mathbf{C})$, σ restricts to an automorphism of K^* and hence also acts on K via the isomorphism $\tau : K \rightarrow K^*$.

Proposition 5. *Let $E \in \text{Ell}(\mathcal{O})$, $\sigma \in \text{Aut}(\mathbf{C})$, and $\alpha \in \mathcal{O}$. Then the diagram*

$$\begin{array}{ccccc} & E(\mathbf{C}) & \xrightarrow{[\alpha]} & E(\mathbf{C}) & \\ x \downarrow & \downarrow & & \downarrow & x \downarrow \\ x^\sigma & E^\sigma(\mathbf{C}) & \xrightarrow{[\alpha^\sigma]} & E^\sigma(\mathbf{C}) & x^\sigma \end{array}$$

commutes, i.e., $[\alpha^\sigma] = [\alpha]^\sigma$.

Proof. It suffices to show that the diagram

$$\begin{array}{ccccc} [\alpha] & \text{End } E & \hookrightarrow & \text{End Tan}_0 E \cong \mathbf{C} & \\ \downarrow & \downarrow & & \downarrow & z \\ [\alpha]^\sigma & \text{End } E^\sigma & \hookrightarrow & \text{End Tan}_0 E^\sigma \cong \mathbf{C} & z^\sigma \end{array}$$

commutes. This can be checked on a basis element $\omega \in \text{End Tan}_0 E$ as follows:

$$([\alpha]^\sigma)^* \omega^\sigma = ([\alpha]^* \omega)^\sigma = (\tau(\alpha)\omega)^\sigma = \tau(\alpha^\sigma)\omega^\sigma = [\alpha^\sigma]^* \omega^\sigma. \quad \square$$

Corollary 6. *Let $L \subseteq \mathbf{C}$ be a number field. If E/L is such that $E_{\mathbf{C}}$ has CM by \mathcal{O} , then every element of $\text{End}_{\mathbf{C}} E$ is defined over LK^* , i.e., E_{LK^*} has CM by \mathcal{O} , and LK^* is the unique smallest extension of L for which this holds.*

Proof. Clear from the proposition. \square

We proved that $\text{Ell}(\mathcal{O})$ is a principal homogeneous space for $\text{Cl}(\mathcal{O})$. It is also a G_{K^*} -set, where $G_{K^*} = \text{Gal}(\overline{\mathbf{Q}}/K^*)$ ($\overline{\mathbf{Q}}$ denotes the algebraic closure of \mathbf{Q} in \mathbf{C}). Class field theory supplies (via the reciprocity map) a surjection $r : G_{K^*} \rightarrow \text{Cl}(\mathcal{O})$ satisfying $r(\text{Frob}_{\mathfrak{p}}) = \tau^{-1}(\mathfrak{p}) \cap \mathcal{O}$ for every prime \mathfrak{p} of K^* not dividing the conductor of \mathcal{O} (here $\text{Frob}_{\mathfrak{p}}$ is an arithmetic Frobenius element at \mathfrak{p}). One might ask whether the $\text{Cl}(\mathcal{O})$ - and G_{K^*} -actions on $\text{Ell}(\mathcal{O})$ are compatible with the homomorphism r .

Theorem 7. *For any $\sigma \in G_{K^*}$, we have $j(E)^\sigma = j(r(\sigma) \cdot [E])$.*

Proof. This is proved in §4, Corollary 24(2). \square

2. POTENTIALLY GOOD REDUCTION AND THE INTEGRALITY OF j

In this section, we prove that CM elliptic curves have everywhere potentially good reduction. The following proposition lies at the heart of this fact.

Proposition 8. *Let $L \subseteq \mathbf{C}$ be a number field and E/L be an elliptic curve with CM by K . The Tate module representations $\rho_\ell : G_L \rightarrow \text{Aut } T_\ell E$ have abelian image for every rational prime ℓ .*

Proof. It suffices to show that the representations $\rho_{\ell^n} : G_L \rightarrow \text{Aut } E[\ell^n](\overline{\mathbf{Q}})$ are abelian for all n . By Proposition 5, the G_L -action on $E[\ell^n](\overline{\mathbf{Q}})$ commutes with the \mathcal{O} -action, so the image of ρ_{ℓ^n} is contained in $\text{Aut}_{\mathcal{O}} E[\ell^n](\overline{\mathbf{Q}})$. We claim that $E[\ell^n](\overline{\mathbf{Q}})$ is a projective $\mathcal{O}/(\ell^n)$ -module of rank 1. Granting the claim, we have

$$\text{Aut}_{\mathcal{O}} E[\ell^n](\overline{\mathbf{Q}}) \cong \text{Aut}_{\mathcal{O}/(\ell^n)} E[\ell^n](\overline{\mathbf{Q}}) \cong (\mathcal{O}/(\ell^n))^\times,$$

which is abelian.

Write $E(\mathbf{C}) \cong \mathbf{C}/\Lambda$ for $\Lambda \subseteq K$ an \mathcal{O} -module. In fact, Λ is a projective \mathcal{O} -module of rank 1 (this was proved in the proof of Theorem 2). Thus, $\Lambda/\ell^n \Lambda \cong \ell^{-n} \Lambda/\Lambda \cong E[\ell^n](\overline{\mathbf{Q}})$ is a projective $\mathcal{O}/(\ell^n)$ -module of rank 1. \square

Proposition 8 also follows easily from the Main Theorem of CM.

Theorem 9. *Let $L \subseteq \mathbf{C}$ be a number field and E/L be an elliptic curve with CM by K . E has everywhere potentially good reduction.*

Proof. By Proposition 8, we may replace L by a finite extension and assume that $T_\ell E$ is an abelian G_L -module for all ℓ . Let \mathfrak{p} be a prime of L and choose a rational prime ℓ such that $\mathfrak{p} \nmid \ell$. To prove that E has potentially good reduction at \mathfrak{p} , it suffices (by the criterion of Néron-Ogg-Shafarevich [8, VII.7.1]) to show that the inertia group $I_{\mathfrak{p}}$ at \mathfrak{p} acts on $T_\ell E$ through a finite quotient.

Since $T_\ell E$ is an abelian G_L -module, $\rho_\ell|_{I_{\mathfrak{p}}}$ factors through a homomorphism $I_{\mathfrak{p}}^{\text{ab}} \rightarrow \text{Aut } T_\ell E$, where $I_{\mathfrak{p}}^{\text{ab}}$ denotes the image of $I_{\mathfrak{p}}$ in the abelianization G_L^{ab} . By class field theory, $I_{\mathfrak{p}}^{\text{ab}} \cong \mathcal{O}_{L_{\mathfrak{p}}}^\times$ is an extension of a finite group by a pro- p group (where p is the rational prime over which \mathfrak{p} lies). $\text{Aut } T_\ell E \cong \text{GL}_2(\mathbf{Z}_\ell)$ is an extension of a finite group by a pro- ℓ group. This is easily seen to imply that $\rho_\ell(I_{\mathfrak{p}})$ is finite. \square

Corollary 10. *If E has CM by \mathcal{O} , then $j(E)$ is an algebraic integer.*

Proof. By [8, VII.5.5], $j(E)$ is an algebraic integer if and only if E has everywhere potentially good reduction. \square

3. THE MAIN THEOREM OF CM AND CONSEQUENCES

We need a short discussion regarding lattices before we can state the Main Theorem of CM. Let $\Lambda \subseteq K$ be a lattice (i.e., free \mathbf{Z} -module of rank 2). For a rational prime p , set $\Lambda_p = \Lambda \otimes_{\mathbf{Z}} \mathbf{Z}_p \subseteq K_p$; then Λ_p is a \mathbf{Z}_p -lattice in $K \otimes_{\mathbf{Z}} \mathbf{Z}_p$.

Lemma 11. *Suppose given, for each rational prime p , a \mathbf{Z}_p -lattice $M_p \subseteq K_p$ such that $M_p = \mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}_p$ for almost all p . There is a unique lattice $\Lambda \subseteq K$ such that $\Lambda_p = M_p$ for all p .*

Proof. If such a Λ exists, then it is unique (equality of submodules is a local property). Given a collection $\{M_p\}$ satisfying the hypotheses of the lemma, set $\Lambda = \bigcap_p (M_p \cap K)$ (intersection inside of $K \otimes \widehat{\mathbf{Z}}$). One can check that Λ is a lattice in K satisfying $\Lambda_p = M_p$ for all p . \square

Given an idèle $s = (s_p) \in \mathbf{A}_K^\times$ with $s_p \in K_p$ and any lattice $\Lambda \subseteq K$, we can define (using Lemma 11) a lattice $s\Lambda$ by requiring that $(s\Lambda)_p = s_p\Lambda_p$ for all rational primes p . Moreover, we have $K/\Lambda \cong \bigoplus_p K_p/\Lambda_p$, so it makes sense to define the ‘‘multiplication by s ’’ map $\cdot s : K/\Lambda \rightarrow K/s\Lambda$ to be the sum of the maps $\cdot s_p : K_p/\Lambda_p \rightarrow K_p/s_p\Lambda_p$. For any number field L , we denote by $[-, L] : \mathbf{A}_L^\times \rightarrow \text{Gal}(L^{\text{ab}}/L)$ the Artin reciprocity map (normalized to take uniformizers to *arithmetic* Frobenius elements). Finally, we note that the isomorphism $\tau : K \rightarrow K^*$ induces (abusing notation slightly) isomorphisms $\tau : K_{\mathfrak{p}} \rightarrow K_{\tau(\mathfrak{p})}^*$ for every prime \mathfrak{p} of K , whence an isomorphism $\tau : \mathbf{A}_K^\times \rightarrow \mathbf{A}_{K^*}^\times$.

Theorem 12 (Main Theorem of CM). *Suppose that E/\mathbf{C} is an elliptic curve with CM by K . Choose $\Lambda \subseteq K$ for which there is an isomorphism $\xi : (K \otimes \mathbf{R})/\Lambda \rightarrow E(\mathbf{C})$. Choose $\sigma \in \text{Aut } \mathbf{C}$ and $s \in \mathbf{A}_K^\times$ such that $\sigma|_{(K^*)^{\text{ab}}} = [\tau(s), K^*]$. Then there is an isomorphism $\xi' : (K \otimes \mathbf{R})/s^{-1}\Lambda \rightarrow E^\sigma(\mathbf{C})$ such that the diagram*

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\xi} & E(\mathbf{C})_{\text{tors}} \\ \cdot s^{-1} \downarrow & & \downarrow \\ K/s^{-1}\Lambda & \xrightarrow{\xi'} & E^\sigma(\mathbf{C})_{\text{tors}} \end{array} \quad \begin{array}{c} x \\ \downarrow \\ x^\sigma \end{array}$$

commutes.

Proof. Brian Conrad’s notes [2], q.v., are devoted to the proof of this theorem. \square

As a first application of the Main Theorem of CM, we construct the Grössencharakter associated to a CM elliptic curve.

Theorem 13. *Let $L \subseteq \mathbf{C}$ be a number field and E/L an elliptic curve with CM by K , so $L \supseteq K^*$ by Corollary 6. There is a character $\alpha = \alpha_E : \mathbf{A}_L^\times \rightarrow K^\times$ such that if $x \in \mathbf{A}_L^\times$ and $s = (\tau^{-1} \circ \text{Nm}_{L/K^*})(x) \in \mathbf{A}_K^\times$, then $\alpha(x)$ is the unique element of K^\times such that*

- (1) $\alpha(x)\mathcal{O} = s\mathcal{O}$ and
- (2) if $\Lambda \subseteq K$ is an invertible \mathcal{O} -module and $\xi : (K \otimes \mathbf{R})/\Lambda \rightarrow E(\mathbf{C})$ is an analytic uniformization, then the diagram

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\cdot \alpha(x)s^{-1}} & K/\Lambda \\ \xi \downarrow & & \downarrow \xi \\ E(L^{\text{ab}}) & \xrightarrow{[x, L]} & E(L^{\text{ab}}) \end{array}$$

commutes.

Recall that we showed (Proposition 8) that $E(\mathbf{C})_{\text{tors}} \subseteq E(L^{\text{ab}})$, so the diagram in part (2) of the theorem makes sense. We also remark here that the role that τ^{-1} plays in the definition of s is that of the *reflex norm* $N_{\{\tau\}} : \mathbf{A}_{K^*}^\times \rightarrow \mathbf{A}_K^\times$ appearing in the general theory of CM abelian varieties (cf. [4]).

Proof. Let $\sigma \in \text{Aut } \mathbf{C}$ be such that $\sigma|_{L^{\text{ab}}} = [x, L]$, so $\sigma|_{(K^*)^{\text{ab}}} = [\tau(s), K^*]$. The Main Theorem of CM provides a uniformization $\xi' : (K \otimes \mathbf{R})/s^{-1}\Lambda \rightarrow E(\mathbf{C})$ such that the diagram

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\cdot s^{-1}} & K/s^{-1}\Lambda \\ \xi \downarrow & & \downarrow \xi' \\ E(\mathbf{C}) & \xrightarrow{\sigma} & E^\sigma(\mathbf{C}) = E(\mathbf{C}) \end{array}$$

commutes. Since $E^\sigma(\mathbf{C}) \cong E(\mathbf{C})$, the lattices $s^{-1}\Lambda$ and Λ are homothetic, so there exists $b = b(x) \in K^\times$ such that $bs^{-1}\Lambda = \Lambda$. Thus (again using the Main Theorem) the diagram

$$(*) \quad \begin{array}{ccc} K/\Lambda & \xrightarrow{\cdot bs^{-1}} & K/\Lambda \\ \xi \downarrow & & \downarrow \xi'' \\ E(\mathbf{C}) & \xrightarrow{\sigma} & E(\mathbf{C}) \end{array}$$

commutes for appropriate choice of uniformization $\xi'' : (K \otimes \mathbf{R})/\Lambda \rightarrow E(\mathbf{C})$.

Let $\alpha(x)$ be the element of K^\times satisfying $[\alpha(x)] = \xi'' \circ \xi^{-1} \circ [b] \in (\text{End}_{\mathbf{C}} E) \otimes \mathbf{Q}$. From (*) and the fact² that $\xi'' \circ (\cdot b) = \xi \circ (\cdot \alpha(x))$, we deduce the following commutative diagram:

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\cdot \alpha(x)s^{-1}} & K/\Lambda \\ \xi \downarrow & & \downarrow \xi \\ E(L^{\text{ab}}) & \xrightarrow{[x, L]} & E(L^{\text{ab}}) \end{array}$$

which shows (2). Because $\alpha(x)s^{-1}\Lambda = \Lambda$, we have $\alpha(x)\mathcal{O} = s\mathcal{O}$. Also, $\alpha(x)$ is the unique element of K^\times satisfying (2). It is straightforward to check that $\alpha(x)$ is independent of the choice of Λ and ξ . Finally, the fact that α is a homomorphism is clear from (2) and uniqueness. \square

The character α_E is not a Grössencharakter, as it is not trivial on $L^\times \subseteq \mathbf{A}_L^\times$. However, we have the following:

Theorem 14. *The character $\alpha = \alpha_E : \mathbf{A}_L^\times \rightarrow K^\times$ of Theorem 13 is the unique character such that*

- (1) $\ker \alpha$ is open,
- (2) $\alpha|_{L^\times} = \tau^{-1} \circ \text{Nm}_{L/K^*}$,
- (3) α is unramified at a prime \mathfrak{p} of L if and only if E has good reduction at \mathfrak{p} , and
- (4) if \mathfrak{p} is a prime of L at which E has good reduction and $\pi_{\mathfrak{p}}$ is a local uniformizer at \mathfrak{p} , then $[\alpha(\pi_{\mathfrak{p}})]$ is the unique element of $(\text{End}_L E) \otimes \mathbf{Q}$ whose reduction at \mathfrak{p} is the Frobenius endomorphism $\phi_{\mathfrak{p}}$ of the reduction $E_{\mathfrak{p}}$.

²For any element $k \in K$, one checks via a calculation on the tangent space at the identity that $[k] \circ \xi = \xi \circ (\cdot k)$ as elements of $\text{Hom}((K \otimes \mathbf{R})/\Lambda, E(\mathbf{C})) \otimes \mathbf{Q}$, so this fact follows from the definition of $\alpha(x)$.

Proof. (1), (2), and (3) determine α uniquely and (2) is immediate from the uniqueness of $\alpha(x)$ for $x \in L^\times$.

To prove (1), it suffices to show that $\ker \alpha$ contains an open subgroup. By Proposition 8, $L(E[m])/L$ is a finite abelian extension for any integer $m > 1$, so class field theory implies that there is an open subgroup $B_m \subseteq \mathbf{A}_L^\times$ such that the reciprocity map induces an isomorphism $L^\times \backslash \mathbf{A}_L^\times / B_m \cong \text{Gal}(L(E[m])/L)$. Set

$$U_m = \{x \in B_m \mid (\tau^{-1} \circ \text{Nm}_{L/K^*} x)_\ell \in (1 + m\mathcal{O}_\ell) \cap \mathcal{O}_\ell^\times, \text{ all } \ell \in \mathbf{Z} \text{ prime}\} \subseteq \mathbf{A}_L^\times.$$

Note that this is open, as $(1 + m\mathcal{O}_\ell) \cap \mathcal{O}_\ell^\times = \mathcal{O}_{K,\ell}^\times$ for almost all ℓ , and in general \mathcal{O}_ℓ^\times has finite index in $\mathcal{O}_{K,\ell}^\times$. We show that $\alpha|_{U_m} = 1$ for a suitable choice of m .

Choose an analytic uniformization $\xi : (K \otimes \mathbf{R})/\Lambda \rightarrow E(\mathbf{C})$, so $\xi(m^{-1}\Lambda/\Lambda) = E[m](\mathbf{C})$. Let $t \in m^{-1}\Lambda/\Lambda$ and $x \in U_m$ and set $s = (\tau^{-1} \circ \text{Nm}_{L/K^*})(x)$. Theorem 13 gives that

$$\xi(t) = \xi(t)^{[x,L]} = \xi(t \cdot \alpha(x)s^{-1}) = \xi(\alpha(x)t),$$

where the first equality holds because $x \in B_m$, so $[x, L]$ acts trivially on $E[m]$, and the second holds because $s_\ell \equiv 1 \pmod{m\mathcal{O}_\ell}$, so s_ℓ acts as 1 on $t_\ell \in m^{-1}\Lambda_\ell/\Lambda_\ell$. Therefore, $\alpha(x) \cdot (m^{-1}\Lambda/\Lambda) \subseteq m^{-1}\Lambda/\Lambda$, which implies that $(\alpha(x) - 1)m^{-1}\Lambda \subseteq \Lambda$, whence $(\alpha(x) - 1)\mathcal{O} \subseteq m\mathcal{O}$, i.e., $\alpha(x) \in \mathcal{O}$ and $\alpha(x) \equiv 1 \pmod{m\mathcal{O}}$. Theorem 13 implies that $\alpha(x)_\ell \mathcal{O}_\ell = s_\ell \mathcal{O}_\ell = \mathcal{O}_\ell$ for all ℓ , so $\alpha(x)\mathcal{O} = \mathcal{O}$, i.e., $\alpha(x) \in \mathcal{O}^\times$. Thus for appropriate choice of m , we see that $\alpha(x) = 1$ (as $\mathcal{O}^\times \subseteq \mathcal{O}_K^\times$ is finite).

We now prove (3). Let \mathfrak{p} be a prime of L lying over a rational prime p . Choose $m \in \mathbf{Z}_{>0}$ prime to p and an analytic uniformization $\xi : (K \otimes \mathbf{R})/\Lambda \rightarrow E(\mathbf{C})$. E has good reduction at \mathfrak{p} if and only if an inertia group $I_\mathfrak{p}$ at \mathfrak{p} acts trivially on $E[m^n]$ for all $n > 0$. Recall (Proposition 8) that $I_\mathfrak{p}$ acts through its quotient³ $I_\mathfrak{p}^{\text{ab}} \subseteq \text{Gal}(L^{\text{ab}}/L)$. Therefore, E has good reduction at \mathfrak{p} if and only if, for all n , $\xi(t)^\sigma = \xi(t)$ for all $\sigma \in I_\mathfrak{p}^{\text{ab}}$, $t \in m^{-n}\Lambda/\Lambda$. For such n , σ , and t , let $x \in \mathcal{O}_{L_\mathfrak{p}}^\times \subseteq \mathbf{A}_L^\times$ be such that $[x, L] = \sigma$ and set $s = (\tau^{-1} \circ \text{Nm}_{L/K^*})(x)$; then $s_\ell = 1$ unless $\ell = p$. By Theorem 13, we have $\xi(t)^\sigma = \xi(t)^{[x,L]} = \xi(t \cdot \alpha(x)s^{-1})$.

We claim

$$(\dagger) \quad s^{-1} \text{ acts trivially on } m^{-n}\Lambda/\Lambda \text{ for all } n.$$

As there are only finitely many primes ℓ for which $\mathcal{O}_\ell \neq \mathcal{O}_{K,\ell}$ and, for all ℓ , $\mathcal{O}_\ell^\times \subseteq \mathcal{O}_{K,\ell}^\times$ has finite index, there exists an integer k such that $m^{-kn} \in \mathcal{O}_\ell^\times$ for all n and all $\ell \nmid m$. For such k , we have $m^{-kn}\Lambda_\ell/\Lambda_\ell = m^{-n}\Lambda_\ell/\Lambda_\ell = 0$. Thus $m^{-n}\Lambda/\Lambda \cong \bigoplus_{\ell|m} m^{-n}\Lambda_\ell/\Lambda_\ell$. If $\ell \mid m$, then $s_\ell = 1$, which establishes our claim.

In conclusion, E has good reduction at \mathfrak{p} if and only if, for all n , $\xi(\alpha(x)t) = \xi(t)$ for all $x \in \mathcal{O}_{L_\mathfrak{p}}^\times \subseteq \mathbf{A}_L^\times$ and $t \in m^{-n}\Lambda/\Lambda$. This holds if and only if, for all n , $\alpha(x) \equiv 1 \pmod{m^n\mathcal{O}}$ for all $x \in \mathcal{O}_{L_\mathfrak{p}}^\times$, which is equivalent to the statement that $\alpha(x) = 1$ for all $x \in \mathcal{O}_{L_\mathfrak{p}}^\times$, i.e., that α is unramified at \mathfrak{p} .

Finally, we prove (4). Let \mathfrak{p} be a good prime for E/L and again choose $m > 0$ prime to \mathfrak{p} and a uniformization $\xi : (K \otimes \mathbf{R})/\Lambda \rightarrow E(\mathbf{C})$. By the claim (\dagger) above, we have that, for all n ,

$$\xi(t)^{\text{Frob}_\mathfrak{p}} = \xi(t)^{[\pi_\mathfrak{p}, L]} = \xi(\alpha(\pi_\mathfrak{p})t) = [\alpha(\pi_\mathfrak{p})]\xi(t)$$

³We defined there $I_\mathfrak{p}^{\text{ab}}$ to be the image of $I_\mathfrak{p}$ in $\text{Gal}(L^{\text{ab}}/L)$; this is a quotient the abelianization of $I_\mathfrak{p}$.

for all $t \in m^{-n}\Lambda/\Lambda$. Denote by $E_{\mathfrak{p}}/k(\mathfrak{p})$ the reduction of E at \mathfrak{p} , and denote by

$$E(L^{\text{ab}}) \longrightarrow E_{\mathfrak{p}}(\overline{k(\mathfrak{p})}) : x \mapsto \tilde{x}$$

the reduction map. We also denote the (injective⁴) map $\text{End}_L E \hookrightarrow \text{End}_{k(\mathfrak{p})} E_{\mathfrak{p}}$ by $\phi \mapsto \tilde{\phi}$. With this notation, we have $\xi(t)^{\widetilde{\text{Frob}_{\mathfrak{p}}}} = \phi_{\mathfrak{p}}(\xi(\tilde{t}))$ and $\tilde{\phi}(x) = \tilde{\phi}(\tilde{x})$. Hence $\phi_{\mathfrak{p}}(\xi(\tilde{t})) = [\alpha(\pi_{\mathfrak{p}})](\xi(\tilde{t}))$ for all $t \in m^{-n}\Lambda/\Lambda$, from which (4) follows (also cf. footnote 4). \square

We now discuss the Grössencharakter and L -function of an elliptic curve with CM. For any place (possibly infinite) ℓ of \mathbf{Q} and any number field L , set

$$L_{\ell} = L \otimes_{\mathbf{Q}} \mathbf{Q}_{\ell} = \prod_{\mathfrak{l}|\ell} L_{\mathfrak{l}}.$$

For an extension L/F of number fields, we define the local norm $\text{Nm}_{L_{\ell}/F_{\ell}} : L_{\ell} \rightarrow F_{\ell}$ to be $\text{Nm}_{L/F} \otimes \mathbf{Q}_{\ell}$.

Suppose E/L has CM by K and let $\alpha = \alpha_E$. Define

$$\chi_{\ell} = \chi_{E,\ell} : \mathbf{A}_L^{\times} \rightarrow K_{\ell}^{\times}$$

via $\chi_{\ell}(x) = \alpha(x)(\tau^{-1} \circ \text{Nm}_{L_{\ell}/K_{\ell}^*})(x_{\ell})^{-1}$. By Theorem 14(1), (2), $\ker \chi_{\ell} \supseteq L^{\times}$, i.e., χ_{ℓ} is an idèle class character. If ℓ is a finite prime, then K_{ℓ}^{\times} is totally disconnected, so χ_{ℓ} is trivial on the identity component $(L^{\times} \backslash \mathbf{A}_L^{\times})^{\circ}$ and by class field theory we can view χ_{ℓ} as a K_{ℓ}^{\times} -valued character of $\text{Gal}(L^{\text{ab}}/L)$. Recall that $\mathbf{T}_{\ell} E$ is an $\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_{\ell}$ -module of generic rank 1, so we can consider the associated ℓ -adic Galois representation ρ_{ℓ} as a character

$$\rho_{\ell} : \text{Gal}(L^{\text{ab}}/L) \longrightarrow \text{Aut}_{K_{\ell}}(\mathbf{T}_{\ell} E \otimes_{\mathbf{Z}_{\ell}} \mathbf{Q}_{\ell}) \cong K_{\ell}^{\times}.$$

Theorem 15. $\chi_{\ell} = \rho_{\ell}$ for all finite ℓ .

Proof. As both characters are continuous, we only need to check this on $\text{Frob}_{\mathfrak{p}}$ for $\mathfrak{p} \nmid \ell$ a good prime for E : such elements are dense in $\text{Gal}(L^{\text{ab}}/L)$. This is just Theorem 14(4) in light of the fact that $\alpha|_{L_{\mathfrak{p}}^{\times}} = \chi_{\ell}|_{L_{\mathfrak{p}}^{\times}}$. \square

For $p = \infty$, we get a character $\chi_{\infty} : L^{\times} \backslash \mathbf{A}_L^{\times} \rightarrow (K \otimes \mathbf{R})^{\times}$. Set $\Phi = \{\tau\} \subseteq \text{Hom}(K, \mathbf{C})$ and define

$$\Phi_{\tau}^* = \{\sigma \in \text{Hom}(K^*, \mathbf{C}) \mid \tilde{\sigma}^{-1}\tau \in \Phi\},$$

where $\tilde{\sigma}$ denotes any lift of σ to $\text{Aut}(\mathbf{C})$, so Φ_{τ}^* is the one-element set containing the inclusion map $K^* \hookrightarrow \mathbf{C}$. For any extension L/K^* , set $(\Phi_{\tau}^*)_L = \{\sigma \in \text{Hom}(L, \mathbf{C}) \mid \sigma|_{K^*} \in \Phi_{\tau}^*\}$, so $(\Phi_{\tau}^*)_L = \text{Hom}_{K^*}(L, \mathbf{C})$ (L is a totally complex field and $(\Phi_{\tau}^*)_L$ is a set of representatives for the quotient of $\text{Hom}(L, \mathbf{C})$ by the action of complex conjugation). If we set

$$\chi_E = (\tau \otimes 1) \circ \chi_{\infty} : L^{\times} \backslash \mathbf{A}_L^{\times} \rightarrow \mathbf{C}^{\times},$$

⁴The map arises from the Néron mapping property; it is injective because the diagram

$$\begin{array}{ccc} \text{End}_L E & \longrightarrow & \text{End}_L \mathbf{T}_{\ell} E \\ \downarrow & & \parallel \\ \text{End}_{k(\mathfrak{p})} \tilde{E} & \longrightarrow & \text{End}_{k(\mathfrak{p})} \mathbf{T}_{\ell} \tilde{E} \end{array}$$

commutes for all $\mathfrak{p} \nmid \ell$ and the horizontal arrows are injections.

then it is clear from Theorem 14 that χ_E is a Grössencharakter of L infinity type $\sum_{\sigma \in (\Phi_\tau^*)_L} \sigma$. The reason for our seemingly over-complicated notation is the following: in the language of the general theory of CM abelian varieties, Φ_τ^* is the *reflex type* associated to the CM type Φ of K and the embedding $\tau : K \hookrightarrow \mathbf{C}$. The statements we have made apply equally to the Grössencharaktere arising from CM abelian varieties of higher dimension.

Let L be a number field. Recall that attached to any Grössencharakter $\psi : \mathbf{A}_L^\times \rightarrow \mathbf{C}^\times$ is a complex L -function

$$L(\psi, s) = \prod_{\mathfrak{p} \in S} (1 - \psi(\pi_{\mathfrak{p}})q_{\mathfrak{p}}^{-1})^{-1},$$

where S is the set of finite places of L where ψ is unramified, $\pi_{\mathfrak{p}}$ is a uniformizer at \mathfrak{p} , and $q_{\mathfrak{p}} = \#k(\mathfrak{p})$ is the size of the residue field at \mathfrak{p} . Note that the Euler product for $L(\psi, s)$ only converges for $s \gg 0$. The following is a standard result.

Theorem 16. *Suppose the number field L has no real embeddings.⁵ If ψ is a Grössencharakter of L having infinity type $\sum_{\sigma \in \Sigma} n(\sigma)\sigma$, where $\Sigma = \{\sigma : L \hookrightarrow \mathbf{C}\}$, then $L(\psi, s)$ has meromorphic continuation to all of \mathbf{C} and satisfies the functional equation*

$$\Lambda(\psi, s) = w(\psi)\Lambda(\bar{\psi}, 1 - s),$$

where $\Lambda(\psi, s)$ is the “completed” L -function

$$\Lambda(\psi, s) = (\mathrm{Nm}_{L/\mathbf{Q}}(\mathrm{cond}_L \psi) d_{L/\mathbf{Q}})^{s/2} ((2\pi)^{-s} \Gamma(s))^{[L:\mathbf{Q}]/2}$$

and $w(\psi)$ is an explicit complex number of absolute value 1 defined by Gauss sums. If ψ is not a power of the norm character \mathbf{N} , then $L(\psi, s)$ is moreover an entire function.

We can also define an L -function attached to an elliptic curve E over L by the Euler product

$$L(E/L, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(E/L, q_{\mathfrak{p}}^{-s})^{-1},$$

where the product is over the finite places of L and

$$L_{\mathfrak{p}}(E/L, T) = \det(1 - \mathrm{Frob}_{\mathfrak{p}} T \mid T_{\ell} E^{I_{\mathfrak{p}}})$$

for any rational prime ℓ prime to \mathfrak{p} (this definition is independent of ℓ : [8, V.2.3]). The following table (cf. [9, II.10.1]) gives a formula for $L_{\mathfrak{p}}(E/L, T)$ in terms of the reduction type of E at \mathfrak{p} .

reduction type of E at \mathfrak{p}	$L_{\mathfrak{p}}(E/L, T)$
good	$(\det \phi_{\mathfrak{p}})T^2 - (\mathrm{tr} \phi_{\mathfrak{p}})T + 1$
split multiplicative	$1 - T$
non-split multiplicative	$1 + T$
additive	1

It is conjectured that $L(E/L, s)$ has analytic continuation to all of \mathbf{C} and enjoys a functional equation similar to that described in Theorem 16. When E is defined over \mathbf{Q} , this is a consequence of the famous work of Wiles, Wiles-Taylor, and Breuil-Conrad-Diamond-Taylor on the modularity conjecture, but the general case is very

⁵This assumption is only made to simplify the functional equation; a similar statement of course holds even when L admits real embeddings.

difficult. When E has complex multiplication, however, the situation is much more favorable as a result of the following theorem.

Theorem 17. *Suppose $L \subseteq \mathbf{C}$ and E/L is an elliptic curve such that $E_{\mathbf{C}}$ has CM by K .*

- (1) *If $L \supseteq K^*$, then $L(E/L, s) = L(\chi_E, s)L(\overline{\chi}_E, s)$.*
- (2) *If $L \not\supseteq K^*$, then $L(E/L, s) = L(\chi_E, s)$, where χ_E is the Grössencharakter of LK^* associated to E/LK^* .*

Proof. In fact, we prove the stronger theorem that the given equalities hold Euler factor by Euler factor. (In the case of (2), this means that we compare Euler factors at \mathfrak{p} to the product of the Euler factors at \mathfrak{P} for $\mathfrak{P} \mid \mathfrak{p}$.)

Suppose first that $L \supseteq K$. By Theorem 9, E has potentially good reduction at all places of L , so its reduction is everywhere good or additive. Theorem 14(3) implies that χ_E and $\overline{\chi}_E$ are unramified at \mathfrak{p} if and only if E has good reduction at \mathfrak{p} , so it suffices to only consider the Euler factors at places of good reduction. Hence, we must show that

- $\text{tr } \phi_{\mathfrak{p}} = \chi_E(\pi_{\mathfrak{p}}) + \overline{\chi_E(\pi_{\mathfrak{p}})}$ and
- $\det \phi_{\mathfrak{p}} = \chi_E(\pi_{\mathfrak{p}})\overline{\chi_E(\pi_{\mathfrak{p}})}$,

where we can compute $\text{tr } \phi_{\mathfrak{p}}$ and $\det \phi_{\mathfrak{p}}$ on $T_{\ell} E$ for any ℓ prime to \mathfrak{p} . The formula for the trace follows from the fact that (for ℓ split in K , e.g.) $\chi_{\ell} = \rho_{\ell}$. The formula for the determinant can be proved in the same way, or can be proved by combining the fact that χ_E has infinity type $\sum_{\sigma \in (\Phi_{\tau}^*)_L} \sigma$, so⁶ $\chi_E \overline{\chi}_E = \mathbf{N}$, with the fact $\det \phi_{\mathfrak{p}} = \deg \phi_{\mathfrak{p}} = q_{\mathfrak{p}} = \mathbf{N}(\pi_{\mathfrak{p}})$.

Proving (2) is somewhat more difficult, as we need to do more work to show that the reduction of E behaves as we expect. Let $F = LK^*$ and let σ be the nontrivial element of $\text{Gal}(F/L)$.

Lemma 18. *If a prime \mathfrak{p} of L is ramified in F/L , then E has bad reduction at the prime \mathfrak{P} of F lying over \mathfrak{p} .*

Proof. Let $\alpha \in \mathcal{O}$ be such that $\alpha^{\sigma} \neq \alpha$, so $[\alpha]^{\sigma} \neq [\alpha]$. If the reduction $E_{\mathfrak{P}}$ of E at \mathfrak{P} is good, then there is an injection (see footnote 4) $\text{End}_F E \hookrightarrow \text{End}_{k(\mathfrak{P})} E_{\mathfrak{P}}$. On the other hand, \mathfrak{p} is ramified in F/L , so $k(\mathfrak{P}) = k(\mathfrak{p})$ and σ fixes \mathfrak{P} , so it must be the case that $[\alpha]^{\sigma} = [\alpha]$, a contradiction. \square

By the lemma, if \mathfrak{p} is ramified in F/L and $\mathfrak{P} \mid \mathfrak{p}$, then E has additive reduction at \mathfrak{p} , so $L_{\mathfrak{p}}(E/L, T) = 1$. E_F will also have bad reduction at \mathfrak{P} , so χ_E is ramified at \mathfrak{P} by Theorem 14(3).

Therefore, it suffices to consider Euler factors at primes \mathfrak{p} unramified in F/L . Note that for such \mathfrak{p} , E has good reduction at \mathfrak{p} if and only if E_F has good reduction at all primes \mathfrak{P} of F lying over \mathfrak{p} . (This is because unramified base change does not change reduction type.) Thus, in fact, it suffices to consider Euler factors at primes of good reduction for E .

Lemma 19. *If \mathfrak{P} and \mathfrak{P}' are the primes of F lying over \mathfrak{p} (possibly $\mathfrak{P} = \mathfrak{P}'$), then*

$$\chi_E(\pi_{\mathfrak{P}}^{\sigma}) = \chi_E(\pi_{\mathfrak{P}'}) = \chi_E(\pi_{\mathfrak{P}})^{\sigma} = \overline{\chi_E(\pi_{\mathfrak{P}})}.$$

⁶Note that \mathbf{N} is the *inverse* of the adélic norm.

Note that this shows that $\overline{\chi}_E = \chi_E \circ \sigma$. Thus, we have $L(\overline{\chi}_E, s) = L(\chi_E \circ \sigma, s) = L(\chi_E, s)$ in case (2). (The last equality follows from the fact that the effect of composing with σ amounts rearranging the Euler factors.)

Proof. The first and last equalities are obvious. The middle equality follows from the fact that both $[\chi_E(\pi_{\mathfrak{P}'})]$ and $[\chi_E(\pi_{\mathfrak{P}})]^\sigma = [\chi_E(\pi_{\mathfrak{P}})]^\sigma$ are the unique endomorphism of E reducing to the Frobenius $\phi_{\mathfrak{P}'}$ at \mathfrak{P}' (Theorem 14(4)). \square

We consider primes split and inert in F/L separately. If \mathfrak{p} is split, we have that

$$\mathrm{tr} \phi_{\mathfrak{p}} = \mathrm{tr} \phi_{\mathfrak{P}} = \mathrm{tr} \phi_{\mathfrak{P}'} = \chi_E(\pi_{\mathfrak{P}'}) + \overline{\chi_E(\pi_{\mathfrak{P}'})} = \chi_E(\pi_{\mathfrak{P}}) + \chi(\pi_{\mathfrak{P}'})$$

and

$$\det \phi_{\mathfrak{p}} = q_{\mathfrak{p}} = q_{\mathfrak{P}} = q_{\mathfrak{P}'} = \chi_E(\pi_{\mathfrak{P}}) \overline{\chi_E(\pi_{\mathfrak{P}'})} = \chi_E(\pi_{\mathfrak{P}}) \chi_E(\pi_{\mathfrak{P}'}) .$$

Therefore, $L_{\mathfrak{p}}(E/L, T) = (1 - \chi_E(\pi_{\mathfrak{P}})T)(1 + \chi_E(\pi_{\mathfrak{P}'})T)$ if E has good reduction at \mathfrak{p} .

If \mathfrak{p} is inert and \mathfrak{P} is the prime of F lying over \mathfrak{p} , then we have $\chi_E(\pi_{\mathfrak{P}}) = \overline{\chi_E(\pi_{\mathfrak{P}'})}$, so $[\chi_E(\pi_{\mathfrak{P}})] \in \mathbf{Z} \subseteq \mathrm{End}_F E$. Consequently, we see by checking degrees (note that $\phi_{\mathfrak{p}}^2 = \phi_{\mathfrak{P}}$) that

$$[\widetilde{\chi(\pi_{\mathfrak{P}})}] = \phi_{\mathfrak{P}} = \pm q_{\mathfrak{p}} \in \mathbf{Z} \subseteq \mathrm{End}_{k(\mathfrak{P})} E_{\mathfrak{P}} .$$

Lemma 20. $\phi_{\mathfrak{P}} = -q_{\mathfrak{p}}$.

Proof. We first show that $\phi_{\mathfrak{p}} \notin \mathbf{Z} \subseteq \mathrm{End}_{k(\mathfrak{p})} E_{\mathfrak{P}}$. If we choose as above an endomorphism $[\alpha] \in \mathrm{End}_F E$ of E_F not defined over L , then we have $[\alpha] \neq [\alpha]^\sigma$, so $[\widetilde{\alpha}] \neq [\widetilde{\alpha}]^\sigma = [\widetilde{\alpha}]^{\mathrm{Frob}_{\mathfrak{p}}}$. As $\phi_{\mathfrak{p}}[\widetilde{\alpha}] = [\widetilde{\alpha}]^{\mathrm{Frob}_{\mathfrak{p}}} \phi_{\mathfrak{p}}$, we see that $\phi_{\mathfrak{p}}$ does not commute with $[\widetilde{\alpha}]$ and therefore cannot be an element of \mathbf{Z} , which is central in $\mathrm{End}_{k(\mathfrak{p})} E_{\mathfrak{P}}$.

Therefore, $\mathbf{Q}[\phi_{\mathfrak{p}}] = \mathbf{Q}[\sqrt{\phi_{\mathfrak{P}}}]$ is a quadratic extension of \mathbf{Q} with nontrivial automorphism given by $\phi_{\mathfrak{p}} \mapsto \widehat{\phi}_{\mathfrak{p}}$, where $\widehat{\phi}_{\mathfrak{p}}$ is the dual isogeny to $\phi_{\mathfrak{p}}$. This extension must be imaginary quadratic, because $\phi_{\mathfrak{p}} \widehat{\phi}_{\mathfrak{p}} = q_{\mathfrak{p}} > 0$. \square

Note that the characteristic polynomial of $\phi_{\mathfrak{p}}$ has conjugate roots:

$$\det \left(\frac{m}{n} - \phi_{\mathfrak{p}} \right) = \frac{1}{n^2} \deg(m - n\phi_{\mathfrak{p}}) \geq 0$$

for all $\frac{m}{n} \in \mathbf{Q}$. As $\phi_{\mathfrak{p}}$ is a root of $x^2 + q_{\mathfrak{p}}$ by the lemma, this must be its characteristic polynomial. In particular⁷, $\det \phi_{\mathfrak{p}} = q_{\mathfrak{p}} = -\chi_E(\pi_{\mathfrak{p}})$ and $\mathrm{tr} \phi_{\mathfrak{p}} = 0$.

In conclusion, we have shown that

$$L_v(E/L, T) = \begin{cases} (1 - \chi_E(\pi_w)T)(1 - \chi_E(\pi_{w'})T) & \text{good reduction, } v = ww' \text{ split} \\ 1 - \chi_E(\pi_w)T^2 & \text{good reduction, } v = w \text{ inert} \\ 1 & \text{bad reduction} \end{cases}$$

so

$$L(E/L, s) = \prod_v L_v(E/L, q_v^{-s}) = \prod_{v \nmid \mathrm{cond} \chi_E} (1 - \chi_E(\pi_w)q_w^{-s}) = L(\chi_E, s) .$$

(Note that $q_v^2 = q_w$ if v is inert in F/L .) \square

⁷Note that this shows that for a prime \mathfrak{p} of good reduction for E , E has good *supersingular* reduction at \mathfrak{p} if and only if \mathfrak{p} is split in F/L .

In case (2), we are essentially showing that $\rho_\ell = \text{Ind}_F^L \chi_\ell$ for all ℓ . A perhaps better way to proceed would be to show this and then deduce the given equality from general properties of L -functions. In our later notes [1], we prove the analogous theorem for abelian varieties by this method.

Corollary 21. *$L(E/L, s)$ has analytic continuation to all of \mathbf{C} and satisfies a functional equation of the form*

$$\Lambda(E/L, 2-s) = w(E)\Lambda(E/L, s), \quad w(E) = \pm 1,$$

where $\Lambda(E/L, s)$ is the “completed” L -function

$$\Lambda(E/L, s) = (\text{Nm}_{L/\mathbf{Q}}(\text{cond}_L E) d_{L/\mathbf{Q}}^2)^{s/2} ((2\pi)^{-s} \Gamma(s))^{[L:\mathbf{Q}]} L(E/L, s),$$

where $\text{cond}_L E$ is the conductor of E/L and $d_{L/\mathbf{Q}}$ is the discriminant of L .

Proof. This can be deduced from Theorems 16 and 17. \square

4. RING CLASS FIELDS AND ABELIAN EXTENSIONS

In the previous section, we showed how the Main Theorem of CM gives arithmetic information about an elliptic curve E/L with CM by K in terms of the arithmetic of K (in particular, its Grössencharaktere). In this section, we show how the Main Theorem of CM gives arithmetic information about K in terms of the arithmetic of elliptic curves E/L with CM by K .

If E is an elliptic curve over $L = K^*(j(E))$, define the *Weber function* of E to be the map

$$h = h_E : E \longrightarrow E/\text{Aut}_L E.$$

Note that both $E/\text{Aut}_L E$ and h are defined over L . If E and E' are isomorphic over \mathbf{C} , then there is a canonical L -isomorphism $E/\text{Aut}_L E \cong E'/\text{Aut}_L E'$, i.e., $h_E \eta = h_{E'}$ for every isomorphism $\eta : E_{\mathbf{C}} \xrightarrow{\cong} E'_{\mathbf{C}}$.

Proposition 22. *$E/\text{Aut}_L E \cong \mathbf{P}_L^1$ (non-canonically).*

Proof. Let R_h be the ramification divisor of h ; it is an effective divisor on E . The Hurwitz formula gives that

$$g(E/\text{Aut}_L E) = 1 - \frac{\deg R_h}{2 \deg h},$$

where $g(E/\text{Aut}_L E)$ denotes the genus of $E/\text{Aut}_L E$. To conclude the proposition, it therefore suffices to show that $\deg R_h > 0$ and that $(E/\text{Aut}_L E)(L) \neq \emptyset$. The first statement follows from the fact that $E[2] \subseteq E$ is contained in the support of R_h and the second from the fact that $h(0) \in (E/\text{Aut}_L E)(L)$. \square

If E has Weierstrass equation $y^2 = 4x^2 - g_2x - g_3$, the Weber function can be expressed (as a map to \mathbf{P}_L^1) by the formula

$$(\ddagger) \quad (x, y) \mapsto \begin{cases} \frac{g_2 g_3}{\Delta} x & j(E) \neq 0, 1728 \\ \frac{g_2^2}{\Delta} x^2 & j(E) = 1728 \\ \frac{g_3}{\Delta} x^3 & j(E) = 0, \end{cases}$$

though this depends both on the choice of Weierstrass equation and on a suitable choice of isomorphism $E/\text{Aut}_L E \cong \mathbf{P}_L^1$.

Theorem 23. *Suppose E/L has CM by $\mathcal{O} \subseteq K$ and that $L = K^*(j(E))$. Let $\xi : (K \otimes \mathbf{R})/\Lambda \rightarrow E(\mathbf{C})$ be an analytic uniformization of E for some $\Lambda \subseteq K$, fix $u \in K/\Lambda$, and set*

$$W = W(u) = \{\tau(s) \in \mathbf{A}_{K^*}^\times \mid s \in \mathbf{A}_K^\times \text{ satisfies } s\Lambda = \Lambda \text{ and } su = u\}.$$

Then W is open in $\mathbf{A}_{K^}^\times$ and does not depend on the choice of Λ . Moreover, $L(h(\xi(u)))$ is the subfield of $(K^*)^{\text{ab}}$ corresponding to $(K^*)^\times W \subseteq \mathbf{A}_{K^*}^\times$ by class field theory.*

By definition, the field $L(h(\xi(u))) = K^*(j(E), h(\xi(u)))$ is the residue field of the closed point in $(E/\text{Aut}_L E)$ corresponding to $h(\xi(u)) \in (E/\text{Aut}_L E)(\mathbf{C})$; that $\xi(u) \in E(L^{\text{ab}})$ guarantees that this is a finite extension of L . If we choose an L -isomorphism $(E/\text{Aut}_L E) \cong \mathbf{P}_L^1$, then we may view $h(\xi(u))$ as an element of $\mathbf{P}_L^1(\mathbf{C})$, and $K^*(j(E), h(\xi(u)))$ is equal to the subfield of \mathbf{C} generated over $K^*(j(E))$ by the coordinates of $h(\xi(u))$. In view of (\ddagger) , the theorem explicitly describes, in terms of class field theory, the abelian extensions of L generated by (powers of) the “ x -coordinates” of torsion points on E .

Proof. W is clearly open in $\mathbf{A}_{K^*}^\times$. Note that $W \supseteq (K_\infty^*)^\times$. Let $F \subseteq (K^*)^{\text{ab}}$ be the field corresponding to $(K^*)^\times W$ by class field theory, i.e., such that

$$[-, K^*] : (K^*)^\times \backslash \mathbf{A}_{K^*}^\times / W \xrightarrow{\cong} \text{Gal}(F/K^*).$$

Choose any $\sigma \in \text{Aut } \mathbf{C}$ fixing K^* and let $s \in \mathbf{A}_K^\times$ be such that $\sigma|_{L^{\text{ab}}} = [\tau(s), K^*]$. The Main Theorem of CM supplies a uniformization $\xi' : (K \otimes \mathbf{R})/s^{-1}\Lambda \rightarrow E^\sigma(\mathbf{C})$ such that the diagram

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{\cdot s^{-1}} & K/s^{-1}\Lambda \\ \xi \downarrow & & \downarrow \xi' \\ E(L^{\text{ab}}) & \xrightarrow{\sigma} & E^\sigma(L^{\text{ab}}) \end{array}$$

commutes.

We need to show that $\sigma|_F = 1$ if and only if $\sigma|_{L(h(\xi(u)))} = 1$. If $\sigma|_F = 1$, then $\tau(s) \in W$, so $s^{-1}\Lambda = \Lambda$ and hence $j(E) = j(E)^\sigma$. Let $\varepsilon = \xi(\xi')^{-1} : E^\sigma \xrightarrow{\cong} E$. Then

$$(\S) \quad h_E(\varepsilon(\xi(u)^\sigma)) = h_{E^\sigma}(\xi(u)^\sigma) = h_E(\xi(u))^\sigma,$$

where the first equality holds because $h_E \varepsilon$ is the Weber function of E^σ and the second holds because h_E^σ is also the Weber function of E^σ . On the other hand, we have

$$(\P) \quad \varepsilon(\xi(u)^\sigma) = \varepsilon(\xi'(s^{-1}u)) = \xi(u),$$

where the first equality follows from the definition of ξ' and the second follows from the definition of ε and the fact that $\tau(s) \in W$. Putting (\S) and (\P) together, we see that $h_E(\xi(u)) = h_E(\xi(u))^\sigma$, so $\sigma|_{L(h(\xi(u)))} = 1$.

Conversely, suppose that $\sigma|_{L(h(\xi(u)))} = 1$. In this case, $j(E) = j(E)^\sigma$, so again $(K \otimes \mathbf{R})/\Lambda \cong (K \otimes \mathbf{R})/s^{-1}\Lambda$. Thus, $s^{-1}\Lambda \cong \Lambda$ as \mathcal{O} -modules (Theorem 2) and so there is $\mu \in K^\times$ such that $\mu s^{-1}\Lambda = \Lambda$. Therefore, we can define an isomorphism

$\delta : E_{\mathbf{C}}^{\sigma} \xrightarrow{\cong} E_{\mathbf{C}}$ by requiring that the diagram

$$\begin{array}{ccc} (K \otimes \mathbf{R})/\Lambda & \xleftarrow{\cdot \mu} & (K \otimes \mathbf{R})/s^{-1}\Lambda \\ \xi \downarrow & & \downarrow \xi' \\ E(\mathbf{C}) & \xleftarrow{\delta} & E(\mathbf{C}) \end{array}$$

(all arrows of which are isomorphisms of complex tori) commutes. Again using properties of Weber functions, we get that $h_E(\delta(\xi(u)^\sigma)) = h_E(\xi(u))$, so $\delta(\xi(u)^\sigma)$ and $\xi(u)$ differ by an automorphism of E , say $\xi(u) = [\alpha]\delta(\xi(u)^\sigma)$. Now we note that

$$\delta(\xi(u)^\sigma) = \delta(\xi'(s^{-1}u)) = \xi(\mu s^{-1}u),$$

so $\xi(u) = \xi(\alpha \mu s^{-1}u)$. Thus, $(\alpha \mu s^{-1})\Lambda = \Lambda$ and $(\alpha \mu s^{-1})u = u$, i.e., $\tau(\alpha \mu s^{-1}) \in W$, so $\tau(s) \in (K^*)^\times W$, which shows that $\sigma|_F = 1$. \square

Recall (Theorem 2 and the discussion preceding Theorem 7) that $\text{Ell}(\mathcal{O})$ has a simply transitive action of $\text{Cl}(\mathcal{O})$ and an action of G_{K^*} and that there is a surjection $r : G_{K^*} \rightarrow \text{Cl}(\mathcal{O})$ defined by $r(\text{Frob}_{\mathfrak{p}}) = \tau^{-1}(\mathfrak{p}) \cap \mathcal{O}$ for $\mathfrak{p} \nmid \text{cond } \mathcal{O}$.

Corollary 24. *Suppose E/L has CM by $\mathcal{O} \subseteq K$ and that $L = K^*(j(E))$.*

- (1) $(K^*)^{\text{ab}} = K^*(j(E), h_E(E(\mathbf{C})_{\text{tors}}))$.
- (2) $j(E)^\sigma = j(r(\sigma)E)$ for all $\sigma \in G_{K^*}$. Also, $K^*(j(E))$ is the ring class field of K of conductor $c = \text{cond } \mathcal{O}$. (If $\mathcal{O} = \mathcal{O}_K$, this is the Hilbert class field.)
- (3) $[K^*(j(E)) : K^*] = [\mathbf{Q}(j(E)) : \mathbf{Q}] = \#\text{Cl}(\mathcal{O})$.
- (4) If $\{\Lambda_i\}_{i=1}^{\#\text{Cl}(\mathcal{O})}$ is a set of representatives for $\text{Cl}(\mathcal{O})$ with $\Lambda_i \subseteq K \otimes \mathbf{R}$, then $\{j((K \otimes \mathbf{R})/\Lambda_i)\}_{i=1}^{\#\text{Cl}(\mathcal{O})}$ is the complete set of conjugates of $j(E)$ over \mathbf{Q} (or K).

Proof. To prove (1), one checks that

$$\bigcap_u (K^*)^\times W(u) = (K^*)^\times (K_\infty^*)^\times.$$

From Proposition 4, we already know that $[K(j(E)) : K] \leq [\mathbf{Q}(j(E)) : \mathbf{Q}] \leq \#\text{Cl}(\mathcal{O})$, so (2) implies (3) and (4).

To prove (2), take $u = 0$ in Theorem 23. Then

$$W(u) = (K_\infty^*)^\times \times \prod_p \tau(\mathcal{O})_p^\times.$$

The theory of ring class fields implies that $(K^*)^\times W(0)$ is the kernel of the composite

$$\mathbf{A}_{K^*}^\times \xrightarrow{[-, K^*]} \text{Gal}((K^*)^{\text{ab}}/K^*) \xrightarrow{r} \text{Cl}(\mathcal{O});$$

by Theorem 23, $(K^*)^\times W(0)$ is also the kernel of

$$\mathbf{A}_{K^*}^\times \xrightarrow{[-, K^*]} \text{Gal}(K^*(j(E))/K^*).$$

Therefore, if we have $E(\mathbf{C}) \cong (K \otimes \mathbf{R})/\Lambda$, then the Main Theorem of CM implies that

$$\begin{aligned} j(E)^{\text{Frob}_{\mathfrak{p}}} &= j(E)^{[\pi_{\mathfrak{p}}, K^*]} = \\ &= j((K \otimes \mathbf{R})/\Lambda)^{[\pi_{\mathfrak{p}}, K^*]} = j((K \otimes \mathbf{R})/(\pi_{\tau^{-1}(\mathfrak{p})})^{-1}\Lambda) = \\ &= j((K \otimes \mathbf{R})/(\tau^{-1}(\mathfrak{p}) \cap \mathcal{O})^{-1}\Lambda) = j(r(\text{Frob}_{\mathfrak{p}}) \cdot [(K \otimes \mathbf{R})/\Lambda]) \end{aligned}$$

for all $\mathfrak{p} \nmid \text{cond } \mathcal{O}$. \square

Corollary 25. *If E has CM by \mathcal{O}_K and $\mathfrak{a} \subseteq \mathcal{O}_K$ is an ideal, then $K(j(E), h(E[\mathfrak{a}]))$ is the ray class field of K^* of conductor $\tau(\mathfrak{a})$.*

Here $E[\mathfrak{a}] = \{x \in E(\overline{\mathbf{Q}}) \mid [\alpha](x) = 0 \text{ for all } \alpha \in \mathfrak{a}\}$.

Proof. One checks that

$$\bigcap_{u \in \mathfrak{a}^{-1}\Lambda/\Lambda} (K^*)^{\times} W(u) = (K^*)^{\times} U(\tau(\mathfrak{a})),$$

where $U(\tau(\mathfrak{a})) \subseteq \mathbf{A}_{K^*}^{\times}$ is the subgroup defined by

$$\begin{aligned} U(\tau(\mathfrak{a})) &= \{\tau(s) \in \mathbf{A}_{K^*}^{\times} \mid s \in \mathbf{A}_K^{\times} \text{ satisfies } s_p \in \mathcal{O}_{K,p}^{\times} \text{ and} \\ &\quad s_p \equiv 1 \pmod{\mathfrak{a}\mathcal{O}_{K,p}} \text{ for all (finite) primes } p\}. \end{aligned}$$

The corollary then follows from the theory of ray class fields. \square

REFERENCES

1. T. Arnold, *L-functions for cm abelian varieties*, VIGRE CM seminar, 2005.
2. B. Conrad, *Main theorem of complex multiplication*, VIGRE CM seminar, 2005.
3. B. Gross, *Arithmetic on elliptic curves*, LNM, no. 776, Springer-Verlag, 1980.
4. K. Klosin, *On the reflex norm*, VIGRE CM seminar, 2005.
5. S. Lang, *Elliptic functions*, Springer-Verlag, 1987.
6. J-P. Serre, *Complex multiplication*, Algebraic number theory (J.W.S. Cassels and A. Fröhlich, eds.), Academic Press, 1967, pp. 292–296.
7. G. Shimura, *Introduction to the arithmetic theory of automorphic forms*, Princeton Univ. Press, 1971.
8. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.
9. ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, 1999.