The Main Theorem of Complex Multiplication [1]

Dipendra Prasad

These are the notes of a few lectures given on the main theorem of Complex Multiplication for elliptic curves. As the name suggests, the theorem plays a central role in many questions about elliptic curves with Complex Multiplication (also called CM elliptic curves for short). The theorem gives precise information about the field obtained by attaching the (co-ordinates of) torsion points of Complex Multiplication elliptic curves.

An Elliptic curve E over $\mathbb{C}$ is said to have Complex Multiplication if there exists an endomorphism ϕ of E which is not multiplication by n, for any integer n. In such a situation, the ring $End(E)$ is an order in a quadratic imaginary field K, i.e., $End(E)$ is a subring of the ring of integers of K, to be denoted by $\mathcal{O}_K$. This and many other theorems about elliptic curves with Complex Multiplication have been exposed in the notes of E. Ghate [Gh], so we will not go into these matters here.

We begin by introducing certain functions on $E(\mathbb{C})$, called the Weber functions. For this assume that the elliptic curve E is written as

$$y^2 = 4x^3 - g_2x - g_3.$$

Define,

$$\begin{aligned} h_E^1(x,y) &= \frac{g_2g_3}{\Delta} \cdot x \\ h_E^2(x,y) &= \frac{g_2^2}{\Delta} \cdot x^2 \\ h_E^3(x,y) &= \frac{g_3}{\Delta} \cdot x^3, \end{aligned}$$

[1] Elliptic Curves, Modular Forms and Cryptography, *Proceedings of the Advanced Instructional Workshop on Algebraic Number Theory, HRI, Allahabad, November 2000* (A. K. Bhandari, D. S. Nagaraj, B. Ramakrishnan, T. N. Venkataramana, Eds.), Hindustan Book Agency (2003), **–**.

2000 *Mathematics subject classification.* Primary:10D25

where $\Delta = g_2^3 - 27g_3^2$. The following proposition, although simple to prove, is crucial.

Proposition 1

1. *If E_1 and E_2 are elliptic curves, and ϕ is an isomorphism from E_1 onto E_2, then*

$$h^i_{E_1}(t) = h^i_{E_2}(\phi(t)),$$

for any $i \in \{1, 2, 3\}$, and any $t \in E_1(\mathbb{C})$.

2. *Let $i = 1, 2,$ or 3 be the integer such that the automorphism group of $E(\mathbb{C})$ has order $2i$. Then $h^i_E(t_1) = h^i_E(t_2)$ for points $t_1, t_2 \in E(\mathbb{C})$ if and only if there exists an automorphism ϕ of E taking t_1 to t_2.*

Proof : Suppose that the elliptic curve E_1 is given by the equation,

$$y^2 = 4x^3 - g_2x - g_3,$$

and that the elliptic curve E_2 is given by the equation,

$$y^2 = 4x^3 - h_2x - h_3.$$

Then it is known that any isomorphism ϕ of E_1 onto E_2 is given by

$$(x, y) \to (\alpha^2 x, \alpha^3 y),$$

for some $\alpha \in \mathbb{C}^*$, and if such an isomorphism exists, then

$$\begin{aligned} h_2 &= g_2\alpha^4 \\ h_3 &= g_3\alpha^6. \end{aligned}$$

This clearly proves both the parts of the proposition.

For definiteness, we will be using the first Weber function $h_E(t) = h^1_E(t)$ in the rest of this exposition, thus leaving the case of elliptic curves with $g_2g_3 = 0$ (corresponding to curves $y^2 = 4x^3 - ax$, and $y^2 = 4x^3 - b$) to be treated separately using other Weber functions.

The crucial reason why Weber functions are used instead of just the (co-ordinates) of a point on $E(\mathbb{C})$ is that there might be elliptic

curves E_1 and E_2 over a number field L such that $j(E_1) = j(E_2)$, i.e., E_1 and E_2 are isomorphic over $\mathbb{C}$, but they may not be isomorphic over L. In this case the field extensions L_1 and L_2 of L obtained by attaching n-torsion points of E_1 and E_2 may not be the same. However, the fields M_1 and M_2 obtained by attaching $h_{E_1}(p)$ and $h_{E_2}(q)$ where p and q are all the n-torsion points on E_1 and E_2 respectively, are the same. This allows for great flexibility in using elliptic curves as $\mathbb{C}/\Lambda$ even when dealing with number theoretic questions.

1. Classical context for Weber functions

We will digress in this section to introduce the classical context in which Weber functions have been studied.

For τ in the upper-half plane $\mathbb{H} = \{z \in \mathbb{C} \,|\, \mathrm{Im}(z) > 0\}$, let E_τ be the elliptic curve $\mathbb{C}/\mathcal{L}_\tau$ where $\mathcal{L}_\tau$ is the lattice $\mathbb{Z} \oplus \mathbb{Z}\tau$. Let $\wp(z;\tau)$ be the Weierstrass $\wp$-function defined for the lattice $\mathcal{L}_\tau$ as follows

$$\wp(z;\tau) = \frac{1}{z^2} + \sum_{\omega \in \mathcal{L}_\tau - \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

Then $z \to (\wp(z,\tau), \wp'(z;\tau))$ gives an isomorphism of $\mathbb{C}/\mathcal{L}_\tau$ with the algebraic curve

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

where g_2 and g_3 have the well-known formula in terms of τ

$$g_2 = 60 \sum_{\omega \in \mathcal{L}_\tau - \{0\}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in \mathcal{L}_\tau - \{0\}} \frac{1}{\omega^6}.$$

For any triple of integers (m, n, N), $\frac{m+n\tau}{N}$ is an N-torsion point on E_τ. We will assume in the rest of the discussion that N does not divide both m, n. The value of the (first) Weber function at such a torsion point is

$$h_{m,n;N}(\tau) = \frac{g_2(\tau)g_3(\tau)}{\Delta} \wp(\frac{m+n\tau}{N};\tau).$$

These (Weber) functions $h_{m,n;N}(\tau)$ are entire functions on the upper-half plane, and satisfy

$$h_{m,n;N}(\tau) = h_{m,n;N}(\frac{a\tau+b}{c\tau+d})$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$, the principal congruence subgroup of $SL_2(\mathbb{Z})$ of level N. These are in fact modular functions of level N, i.e., they are meromorphic functions at the cusps.

We summarise the main properties of these Weber functions in the following theorem, referring to Shimura's book [Sh] for the proofs.

Theorem 1

1. *The Fourier expansion of $h_{m,n;N}(\tau)$ is of the form*

$$h_{m,n;N}(\tau) = \sum_{j \geq 0} a_j e^{\frac{2\pi i j \tau}{N}},$$

with $a_j \in \mathbb{Q}(\zeta_N)$ where $\zeta_N = e^{\frac{2\pi i}{N}}$.

2. *The functions $h_{m,n;N}(\tau)$ satisfy algebraic equations over $\mathbb{Q}(j)$, hence the field generated by $h_{m,n;N}(\tau)$ and the j-function, for a given N, is an algebraic extension F_N of $F_1 = \mathbb{Q}(j)$.*

3. *The field F_N is exactly the field of modular functions of level N with coefficients in $\mathbb{Q}(\zeta_N)$; in particular $\mathbb{Q}(\zeta_N) = \mathbb{C} \cap F_N$.*

4. *The field F_N is a Galois extension of F_1 with Galois group $GL_2(\mathbb{Z}/N)/\pm 1$. An element $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $GL_2(\mathbb{Z}/N)/\pm 1$ takes $h_{m,n;N}$ to $h_{am+bn,cm+dn;N}$. (Note that $h_{m,n;N} = h_{-m,-n;N}$.)*

2. Adelic formulation

In this section we introduce *adeles* and *ideles* associated to a number field k. The adele ring of k, denoted by $\mathbb{A}_k$, is the collection of elements $x = (x_v)$ where x_v belongs to the local field k_v, k completed at v, where v varies over the set of in-equivalent places of k; we require that for all but finitely many places v, x_v belongs to $\mathcal{O}_v$, the maximal compact subring of the non-Archimedean local field k_v. The set $\mathbb{A}_k$ forms a ring under natural addition and multiplication. Furthermore, there is a natural topology on $\mathbb{A}_k$ making it a locally compact topological ring with $k \hookrightarrow \mathbb{A}_k$, a discrete cocompact subgroup.

The units in $\mathbb{A}_k$ (i.e., the set of invertible elements) forms a group under multiplication, called the group of ideles. We will denote the ideles of k by $\mathbb{J}_k$. Ideles have a natural topology.

More generally, since $\mathbb{A}_k$ is an algebra over k, for any algebraic group G over k, one can talk about the adelic points of G, to be denoted by $G(\mathbb{A}_k)$. The group $G(\mathbb{A}_k)$ is a locally compact topological group containing $G(k)$ as a discrete subgroup.

The main theorem of Classfield theory (the Artin reciprocity) can be reformulated in the adelic language as the exactness of the following short exact sequence. In this, and in what follows, for a number field k, k^{ab} denotes the maximal abelian extension of k. (All the fields in these notes are subfields of $\mathbb{C}$.)

Theorem 2 *The following natural sequence is exact:*

$$0 \to \overline{k^* k_\infty^+} \to \mathbb{J}_k \to \mathrm{Gal}(k^{ab}/k) \to 1,$$

where k_∞^+ is the connected component of identity of $k_\infty^* = (k \otimes_{\mathbb{Q}} \mathbb{R})^*$, and where $\overline{k^* k_\infty^+}$ is the closure of $k^* k_\infty^+$ as a subgroup of $\mathbb{J}_k$.

The image of an element $x \in \mathbb{J}_k$ in $\mathrm{Gal}(k^{ab}/k)$ is denoted by $[x, k]$; it is the so-called Artin symbol attached to the element $x \in \mathbb{J}_k$. For an abelian extension L of k, the subgroup of $\mathbb{J}_k$ consisting of those elements x such that the action of the Artin symbol $[x, k]$ restricted to L is trivial is an open subgroup of $\mathbb{J}_k$ of finite index containing k^*, and the index equal to the degree of L over k. This gives a bijective correspondence between open subgroups of $\mathbb{J}_k$ of finite index containing k^*, and finite abelian extensions of k.

3. Lattices

If V is a finite dimensional vector space over $\mathbb{Q}$, then by a lattice $\mathcal{L}$ in V we mean a finitely generated subgroup $\mathcal{L}$ of V which contains a basis of V. Similarly define a lattice inside a vector space over $\mathbb{Q}_p$ to be a finitely generated $\mathbb{Z}_p$-submodule which contains a $\mathbb{Q}_p$-basis of the vector space.

The following lemma is well-known.

Lemma 1 *There exists a natural bijective correspondence between lattices $\mathcal{L}$ inside a vector space V over $\mathbb{Q}$, and lattices $\mathcal{L}_p$ inside $V_p =$*

$V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ such that $\mathcal{L}_p$ is the $\mathbb{Z}_p$-span of a fixed $\mathbb{Q}$-basis $\{e_1, e_2, \cdots, e_n\}$ of V for almost all primes p. The correspondence sends a lattice $\mathcal{L}$ in V to the lattices $\mathcal{L}_p = \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in $V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Conversely, given lattices $\mathcal{L}_p$ inside $V_p = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$, $\mathcal{L} = \cap_p(\mathcal{L}_p \cap V)$.

Lemma 2 *Let V be the n-dimensional $\mathbb{Q}$-vector space $V = \{e_1, e_2, \cdots, e_n\}$. We identify $Aut(V)$ to $GL_n(\mathbb{Q})$ through this basis. Under this identification, lattices inside V are in bijective correspondence with $GL_n(\mathbb{Q})/GL_n(\mathbb{Z})$. Furthermore, if we let $\hat{\mathbb{Z}}$ denote the profinite completion of $\mathbb{Z}$, and $\hat{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$, then we have*

$$\begin{aligned} GL_n(\mathbb{Q})/GL_n(\mathbb{Z}) &= GL_n(\hat{\mathbb{Q}})/GL_n(\hat{\mathbb{Z}}) \\ &= \prod_p GL_n(\mathbb{Q}_p)/GL_n(\mathbb{Z}_p), \end{aligned}$$

where we have abused notation to use the symbol of direct product when we mean the subset containing only those $x = (x_p) \in \prod_p GL_n(\mathbb{Q}_p)/GL_n(\mathbb{Z}_p)$, in which almost all the components are trivial.

Proof : The first part of the lemma follows because $GL_n(\mathbb{Q})$ acts transitively on the set of all basis vectors in V, and hence on the set of lattices, with the stabiliser $GL_n(\mathbb{Z})$ for the lattice $\{e_1, \cdots, e_n\}$. The second part follows from lemma 1 and the first part.

4. The main theorem of Complex Multiplication

Before we state the main theorem of Complex Multiplication, we need to fix some more notation. For an elliptic curve E over $\mathbb{C}$ given by

$$y^2 = 4x^3 - g_2 x - g_3,$$

and an automorphism σ of $\mathbb{C}$, we let E^σ denote the elliptic curve,

$$y^2 = 4x^3 - g_2^\sigma x - g_3^\sigma.$$

Notice that there is a homomorphism of groups (though non-algebraic) from $E(\mathbb{C})$ to $E^\sigma(\mathbb{C})$ given by $(x, y) \to (x^\sigma, y^\sigma)$. We will abuse notation to denote this map too by σ.

Observe that K^* operates on K by multiplication $(x, y) \to xy$, hence thinking of K as a 2-dimensional vector space over $\mathbb{Q}$, we have an embedding $K^* \hookrightarrow GL_2(\mathbb{Q})$. This is an embedding of algebraic groups, and hence gives rise to an embedding

$$\mathbb{J}_K \hookrightarrow GL_2(\mathbb{A}_{\mathbb{Q}}).$$

In particular, there is an action of the idele group of K on the set of lattices in K. In this action, the component at infinity plays no role.

Theorem 3 *(Main theorem of Complex Multiplication) Fix an isomorphism*

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}),$$

with Λ a lattice inside K. Then for any field automorphism $\sigma \in \mathrm{Aut}(\mathbb{C})$, with $\sigma|_K = id$, and with

$$\sigma|_{K^{ab}} = [s, K], \quad s \in \mathbb{J}_K,$$

there exists an isomorphism

$$\phi' : \mathbb{C}/s^{-1}\Lambda \to E^{\sigma}(\mathbb{C}),$$

such that the following diagram commutes.

$$\begin{array}{ccc} \oplus K_v/\Lambda_v = K/\Lambda & \xrightarrow{\phi} & E(\mathbb{C}) \\ {\scriptstyle s^{-1}}\big\downarrow & & \big\downarrow{\scriptstyle \sigma} \\ \oplus K_v/s_v^{-1}\Lambda_v = K/s^{-1}\Lambda & \xrightarrow{\phi'} & E^{\sigma}(\mathbb{C}) \end{array}$$

We will not be proving this theorem for which we refer to Shimura's book [Sh]. The proof is only a small variation on the proof of Theorem 8.3 given in E. Ghate's article [Gh].

5. Consequences

Theorem 4 *For any elliptic curve E over $\mathbb{C}$ with Complex Multiplication by an order inside K, $j(E)$ is algebraic, and generates an abelian extension over K. Moreover, for a torsion point $t \in E(\mathbb{C})$, $K(h(t))$ is an abelian extension of K.*

Proof: We first prove the statement about j-invariants. For this, it suffices to prove that if σ is an automorphism of $\mathbb{C}$ which is identity on the maximal abelian extension, K^{ab}, of K, then $j(E)^\sigma = j(E)$. We have,

$$\begin{aligned} j(E^\sigma) &= j(E)^\sigma \\ &= j(\mathbb{C}/s^{-1}\Lambda), \end{aligned}$$

where $s \in \mathbb{J}_K$ corresponds to the automorphism σ restricted to K^{ab} which by assumption is trivial, and hence $s = 1$. This proves that $j(E^\sigma) = j(E)$, proving that $j(E)$ belongs to K^{ab}.

Now to prove that $h(t)$ belongs to K^{ab} for any torsion point $t \in E(\mathbb{C})$, once again it suffices to prove that if σ is an automorphism of $\mathbb{C}$ which is identity on K^{ab}, then $h(t)^\sigma = h(t)$. Since E can be assumed to be defined over K^{ab}, $E^\sigma = E$, and moreover $s = 1$ too. Thus from the main theorem of CM, the action of σ on $h(t)$ is trivial.

Theorem 5 *For an elliptic curve E over $\mathbb{C}$ with Complex Multiplication by an order $\mathcal{O}$ inside K, the field $K(j(E))$ is an abelian extension of K with Galois group the class group of $\mathcal{O}$ which corresponds to the subgroup $K^*K_\infty^* \prod_p (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^*$ inside $\mathbb{J}_K$.*

Proof : Since two elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic if and only if $\Lambda_1 = \lambda\Lambda_2$ for some $\lambda \in \mathbb{C}^*$, the field $K(j(E))$ corresponds to the subgroup H of $\mathbb{J}_K$ such that $s \in H$ if and only if $s\Lambda = \lambda\Lambda$ for Λ the lattice inside K corresponding to E.

The endomorphism ring $\mathcal{O}$ of E is the subring of K, defined as

$$\mathcal{O} = \{t \in K | t\Lambda \subset \Lambda\}.$$

The lattice Λ is an invertible $\mathcal{O}$-module, i.e., there exists a lattice $\Lambda' \subset K$ which is also an $\mathcal{O}$-module such that $\Lambda\Lambda' = \mathcal{O}_K$. From this, it can be seen that,

$$\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \{s_p \in K \otimes_{\mathbb{Q}} \mathbb{Q}_p | s_p(\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p) \subset \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p\}.$$

Hence,

$$(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^* = \{s_p \in K \otimes_{\mathbb{Q}} \mathbb{Q}_p | s_p(\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p\}.$$

It follows that $H = K^*K_\infty^* \prod_p (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^*$.

Corollary 1 *The field generated (over K) by $j(E)$ where E runs over all elliptic curves over $\mathbb{C}$ with Complex Multiplication by K is an abelian extension of K corresponding to the subgroup $K^*K_\infty^*\mathbb{A}_\mathbb{Q}^* \subset \mathbb{J}_K$.*

Proof: This follows immediately from the theorem as,

$$\begin{aligned}\bigcap_{\mathcal{O}}\left[K^*K_\infty^*\prod_p(\mathcal{O}\otimes_\mathbb{Z}\mathbb{Z}_p)^*\right] &= K^*K_\infty^*\prod_p\mathbb{Z}_p^* \\ &= K^*K_\infty^*\mathbb{J}_\mathbb{Q}\end{aligned}$$

where the intersection is taken over all orders in K. (Note that every order $\mathcal{O}$ inside K appears as the endomorphism ring of an elliptic curve, e.g. the curve $\mathbb{C}/\mathcal{O}$.)

Theorem 6 *For an elliptic curve E over $\mathbb{C}$ with Complex Multiplication by K, fix an isomorphism*

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}),$$

with Λ a lattice inside K. Let $u \in K/\Lambda \subset \mathbb{C}/\Lambda$ be a point of finite order, and $\phi(u)$, the corresponding element in $E(\mathbb{C})$. Then $K(j(E), h(\phi(u)))$ is an abelian extension of K corresponding to the subgroup $W = K^*W_0 \subset \mathbb{J}_K$, with

$$W_0 = \{s \in \mathbb{J}_K | s\Lambda = \Lambda, su = u\},$$

where su for $s \in \mathbb{J}_K$ with $s\Lambda = \Lambda$ and $u \in K/\Lambda$ is defined as the component-wise multiplication of $s = (s_p)$ on $K/\Lambda = \oplus K_p/\Lambda_p$. (Note that since $s\Lambda = \Lambda$, $s_p\Lambda_p = \Lambda_p$.)

Proof : It suffices to prove that if for an element $s \in \mathbb{J}_K$, the Artin symbol $\sigma = [s, K]$ acts trivially on $K(j(E), h(\phi(u)))$ then s belongs to K^*W_0. If $[s, K]$ acts trivially on $K(j(E), h(\phi(u)))$, then in particular it acts trivially on $K(j(E))$, and hence $s\Lambda = \lambda\Lambda$ for some $\lambda \in K^*$. By changing s to $s\lambda^{-1}$, we can assume that $s\Lambda = \Lambda$. In this case the commutative diagram of the main theorem of Complex Multiplication becomes,

$$\begin{array}{ccc} \oplus K_v/\Lambda_v = K/\Lambda & \xrightarrow{\phi} & E(\mathbb{C}) \\ {\scriptstyle s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ \oplus K_v/\Lambda_v = K/\Lambda & \xrightarrow{\phi'} & E(\mathbb{C}) \end{array}$$

Since $\sigma = [s, K]$ operates trivially on $K(j(E), h(\phi(u)))$, we find that

$$su = \pm u.$$

(This is from part 2 of Proposition 1 according to which if $h(x) = h(y)$, then x and y differ by an automorphism of E, and as we are assuming that $g_2 g_3 \neq 0$, the only automorphisms of E are ± 1.) Since ± 1 anyway belongs to K^*, changing s by an element of K^*, we can assume that $su = u$, proving the theorem.

Corollary 2 *For an elliptic curve E over $\mathbb{C}$ with Complex Multiplication by K, let L be the field obtained by attaching to K the j-invariant $j(E)$ of the elliptic curve, and the values of the Weber function of E at all the torsion points of E. Then $L = K^{ab}$, the maximal abelian extension of K.*

Proof : The extension L clearly corresponds to the subgroup $K^* K_\infty^* G$ inside $\mathbb{J}_K$ where G is defined as

$$G = \{s \in \mathbb{J}_K | s\Lambda = \Lambda, su = u \text{ for all } u \in K/\Lambda\}.$$

For $s \in G$, $s\Lambda = \Lambda$, and hence $s_p \Lambda_p = \Lambda_p$. Thus componentwise multiplication of $s = (s_p)$ induces an automorphism of $K/\Lambda = \oplus K_p/\Lambda_p$. Clearly if the multiplication by s_p on K_p/Λ_p is trivial, then s_p must be 1, completing the proof of the corollary.

References

[Gh] E. Ghate, *Complex Multiplication*, This volume.

[La] S. Lang, *Elliptic Functions*, Second edition, Graduate texts in Mathematics **112**, Springer-Verlag, 1987.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Princeton University Press, Princeton, 1971.

Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211019, India.

Current Address: School of Mathematics, Tata Institute of Fundamental Research, Dr. Homi Bhabha Road, Mumbai 400 005, India.

E-mail address: dprasad@mri.ernet.in
dprasad@math.tifr.res.in