NOTES ON MATHEMATICS

ASVIN GOTHANDARAMAN

CONTENTS

Complex multiplication refers to the study of Elliptic curves in characteristic 0 with an large ring of endomorphisms. These elliptic curves are intimately tied up to the arithmetic of quadratic imaginary fields and can be used to explicitly generate abelian extensions of these fields.

The following are the main theorems of Complex Multiplication and I will prove them here:

Theorem 1 (Complex Multiplication)**.** *The main theorems of CM curves are as follows:*

(1) For an Elliptic curve $E/\mathbb{C}$ with ring of endomorphisms R not equal to $\mathbb{Z}$, R is an order in a quadratic imaginary field K and $K(j(E))$ is the Ring class field of the order R.
(2) Furthermore, for an ideal $\mathfrak{m}$ of R, thinking of it as a modulus, the ring class field $K_{\mathfrak{m}}/K$ is generated by $j(E)$ and $h(E[\mathfrak{m}])$ where h is a Weber function.
(3) The reduction of E at a prime is determined purely by the splitting of that prime in $K/\mathbb{Q}$ (where we think of E as defined over $K(j(E))$.
(4) Finally, the L-series of such an elliptic curve is the product of two abelian L-functions.

(For the relevant notation, see later).

The proof strategy is as follows:

(1) Show that the set of Elliptic curves with endomorphism ring R is a torsor for $\mathrm{Pic}(R)$. Use this to construct a group homomorphism $f : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow \mathrm{Pic}(R)$ with kernel $K(j(E))$ (independent of E).

Date:

(2) Show that f is in fact the map constructed in class field theory and hence prove (1). This is achieved by showing that we can lift the Frobenius in char. p to an isogeny in char. 0 (up to an isomorphism) for a large density of primes and use this prove the splitting properties of the extension $K(j(E))/K$.
(3) Prove (3) by mucking around with elements of the endomorphism ring mapping to the Frobenius. Use this to show that this lifting can in fact be done for all primes and further, we can lift them on the nose.
(4) Use this lifting to prove the splitting properties for the conjectures ring class field and hence prove 2.
(5) Use the lifting to also find the local Euler factors for the L-function and factor them by hand into two conjugate degree 1 Euler factors.

1. Constructing the Galois Representation:

Let $E = \mathbb{C}/\Lambda$ be an Elliptic curve over $\mathbb{C}$. It is not hard to figure out that $\mathrm{End}_{\mathbb{C}}(E) > \mathbb{Z}$ precisely when Λ is a projective module over an order R in a quadratic imaginary field K. This is because $\mathrm{End}_{\mathbb{C}}(E) = \{z \in \mathbb{C} : z\Lambda \subset \Lambda\}$.

Similarly, one can show that the set of lattices Λ such that $\mathrm{End}_{\mathbb{C}}(E) = R$ is equal to the set of projective modules over R. Since the isomorphism class of the Elliptic curve is invariant under scaling of the lattice, we see that the set of Elliptic curves with endomorphism ring R corresponds precisely to the class group of $R, \mathrm{Pic}(R)$.

Denote the set of Elliptic Curves with endomorphism ring R by $(E)(R)$. Then, we can in fact define an action of $\mathrm{Pic}(R)$ on $\mathscr{E}(R)$ in the following way. For $\mathfrak{a} \in \mathrm{Pic}(R)$ and $E = \mathbb{C}/\Lambda \in \mathscr{E}(R)$, define $\mathfrak{a} * E = \mathbb{C}/\mathfrak{a}^{-1}\Lambda$.

It is easy to check that this action is faithful and transitive and hence makes $\mathscr{E}(R)$ into a $\mathrm{Pic}(R)$ torsor. In particular, $\mathscr{E}(R)$ is a finite set of size $h(R)$.

With that done, we can move on to the Galois action on $\mathscr{E}(R)$. For any automorphism $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, $\sigma(E)$ has the same endomorphism ring as E and hence $\mathrm{Aut}(\mathbb{C})$ acts on $\mathscr{E}(R)$.

Fixing any $E \in \mathscr{E}(R)$, this gives us a map $f_E : \mathrm{Gal}(\mathbb{C}/\mathbb{Q}) \longrightarrow \mathrm{Pic}(R)$ defined by $E^\sigma = f_E(\sigma) * E$. A priori, this is only a set map and is not necessarily surjective, independent of E or even a group homomorphism.

The key lemma to proving all the properties we want is the following:

Lemma 2. *For $\sigma \in \mathrm{Aut}(\mathbb{C})$, we have:*

$$(\mathfrak{a} * E)^\sigma = \mathfrak{a}^\sigma * E^\sigma.$$

This lemma is actually quite difficult, for a proof see Silverman. We will simply assume it.

Note that $\mathrm{Aut}_{\mathrm{Pic}(R)}(\mathscr{E}(R)) = \mathrm{Pic}(R)$ and therefore, if we restrict f_E to automorphisms that fix K, we in fact have a group homomorphim:

$$f_E : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}_{\mathrm{Pic}(R)}(\mathscr{E}(R)) = \mathrm{Pic}(R).$$

Showing that it is independent of E is not much harder. It is clearer still that the kernel of f_E is $\mathrm{Gal}(K(j(E))/K)$ and that this is independent of E shows that our map is surjective and this extension is Galois.

2. First Main Theorem of CM:

We want to show that $K(j(E))$ is the ray class field of R. For simplicity, we will assume that R is the maximal order of K from now on. Therefore, we want to show that $K(j(E))$ is the Hilbert Class field of K.

Since $K(j(E))$ is Galois, it suffices to show that the primes of K that split in $K(j(E))$ are precisely the principal ones. In fact, it suffices to show this equivalence on a density one set of primes.

We want to show that for $\sigma_{\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(\overline{K}/K)$, $E_{\mathfrak{p}}^{\sigma} = [\mathfrak{p}] * E$. We have defined $\sigma_{\mathfrak{p}}$ only up to a conjugacy class but since the image is an abelian group, this is ok.

Note that we can define isogenies $[\mathfrak{a}] : E \longrightarrow \mathfrak{a} * E$ of degree $N(\mathfrak{a})$ since $\Lambda \subset \mathfrak{a}^{-1}\Lambda$. If $\mathfrak{p}$ is a prime of good reduction, then $E_{\mathfrak{p}}^{\sigma}$ is characterized by it's reduction being equal to $E^{(N\mathfrak{p})}$, the base change of E by the Frobenius map of degree $N\mathfrak{p}$.

Therefore, to show that $E_{\mathfrak{p}}^{\sigma} = \mathfrak{p} * E$, we will instead show that the isogeny $[\mathfrak{p}] : E \longrightarrow \mathfrak{p} * E$ reduces to the Frobenius map *up to an isomorphism*. We already know that the degree of $[\mathfrak{p}]$ matches the degree of the Frobenius so this is a plausible thing to try and prove.

This by itself would not be enough to prove what we want. After all, there might be two different curves in $\mathscr{E}(R)$ that both reduce to $\widetilde{E^{(p)}}$. However, if we exclude those primes $\mathfrak{p}$ that divide the difference $j(E) - j(E')$ for $E \neq E' \in \mathscr{E}(R)$, this would be sufficient.

We only need to do this on a density one set of primes and therefore, we can restrict to $\mathfrak{p}$ that splits completely over $\mathbb{Q}$. That is, we are going to prove the following Lemma:

Lemma 3. *For a prime $\mathfrak{p}$ of degree one over $\mathbb{Q}$ such that $E \in \mathscr{E}(R)$ has good reduction, we have the following commuting diagram:*

$$\begin{array}{ccc} E & \xrightarrow{[\mathfrak{p}]} & \mathfrak{p} * E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{G} & \widetilde{E}^{(p)} \end{array}$$

Here, the vertical maps are the reduction maps while G is the absolute Frobenius of degree p composed with some isomorphism of $\widetilde{E}^{(p)}$.

Proof. The absolute Frobenius is characterized upto isomorphism by being an isogeny of degree p that is purely inseparable.

Therefore, we need to show that $\widetilde{[\mathfrak{p}]}$ is purely inseparable. The idea here is to reduce to the case where $\mathfrak{p}$ is principal. Suppose $\mathfrak{p} = (\pi)$, then the isogeny on the Kahler differentials is simply multiplication by π and hence on reduction, it is equal to 0.

However, $\mathfrak{p}$ will not always be principal. What we can always do is multiply $\mathfrak{p}$ by an ideal $\mathfrak{a}$ coprime to p such that $\mathfrak{a}\mathfrak{p}$ is principal. This corresponds to composing the isogenies and clearly the composite isogeny is inseparable.

We would be done if $[\mathfrak{a}]$ was separable but we can use the same trick again to make $[\mathfrak{a}]$ principal by multiplying by some ideal coprime to p.

□

3. Reduction of a CM curve being supersingular or not:

Throughout this section, for a prime p over which E has good reduction, F_p will denote the absolute Frobenius of good reduction while F will denote the smallest power of the Frobenius that is an endomorphism of $\widetilde{E}$.

We would like to extend the previous lemma to all primes in K (over which E has good reduction) and further, set $G = F$. We will do this in two stages.

3.1. **Split primes:** In the first stage, we will get a diagram as before with G instead of the Frobenius for all primes. So far, we have achieved this for primes that split over $\mathbb{Q}$.

Let us first carry out the second stage for primes that split over $\mathbb{Q}$. We know that $\widetilde{[\mathfrak{p}]} = \beta \circ F$ for some automorphism β. To show that we can lift on the nose, it is sufficient to show that β is in the image of the reduction map. That is, we want to prove the following lemma:

Lemma 4. *For $E \in \mathscr{E}(R)$ and p a a prime of good reduction, suppose that we have a diagram of the form:*

$$\begin{array}{ccc} E & \xrightarrow{[\mathfrak{p}]} & \mathfrak{p} * E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{G} & \widetilde{E}^{(p)} \end{array}$$

where $G = \beta \circ F$ for β and automorphism of $\widetilde{E}^{(N\mathfrak{p})}$ and F as defined at the start of this section. Then, β is in fact in the image of the reduction map on the endomorphism rings.

Proof. This is easily seen to be equivalent to β commuting with the image of the endomorphism ring under the reduction map (since this image is a rank two thing). That is, for $\alpha \in K$, we want to show that $\beta\widetilde{\alpha} = \widetilde{\alpha}\beta$.

We can do check this after composing on the left with $\widetilde{[\overline{p}]}F$ after which it is easy. □

3.2. **Inert primes:** Now, let $\mathfrak{p}$ be a prime that is inert over $\mathbb{Q}$. That is, $\mathfrak{p} = (p)$. To get a diagram as before, we want to show that $\widetilde{[p]}$ is totally inseparable. However, this is equivalent to E being supersingular in characteristic p. Thus we are naturally led to investigate the relation between supersingularity of $\widetilde{E}$ and the splitting of primes in $K/\mathbb{Q}$.

Let us suppose for the moment that E is supersingular above an inert prime (See Theorem 5). Then, we will have completed step 1 for the inert primes too. However, step 2 is already covered by lemma 4 for this case too and hence we are done.

Theorem 5 (Deuring's Criterion)**.** *For a prime p of $\mathbb{Z}$ over which E has good reduction, we have the following cases:*

1. *p is inert in K: Then, the reduction of E at a prime above p $\widetilde{E}$ is supersingular.*
2. *p splits in K: Then, $\widetilde{E}$ is ordinary at p.*
3. *p ramifies in K: Then also, $\widetilde{E}$ is supersingular at p.*

Proof. Recall that supersingularity is equivalent to either the Endomorphism ring being rank 4 or $\overline{F}$, the dual of the absolute frobenius, being inseparable. Since E is supposed to have complex multiplication, the first criterion is equivalent to the reduction map:

$$K = \mathrm{End}_{\mathbb{C}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathrm{End}_{\overline{\mathbb{F}_p}}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q} = A$$

not being surjective. (This map is always injective).

To prove (1), suppose $\mathfrak{p} = (p)$ is an inert prime and $\widetilde{E}$ is not supersingular. Then, we should be able to find an element $h \in K$ such that $N(h) = p^n$ where n is the degree of the finite field over which $\widetilde{E}$ is defined.

This is because F is a power of F_p and is in the endomorphism ring and thus there should be a h mapping ot F. However, the degree of F is p^n.

Since h is only divisble by p, we can infact find a unit u such that $h = up^{n/2}$. However, this implies that $\overline{h} = \overline{u}p^{n/2}$. Since the reduction of h is purely inseparable, so is the reduction of $\overline{h}$. Since this reduction is equal to $\overline{F}_p^n$, this shows that $\overline{F}_p$ is purely inseparable and hence $\widetilde{E}$ is supersingular which is the required contradiction.

To prove (2): Suppose $\theta = [\mathfrak{p}]$ is the isogeny in char 0 that lifts F. Such an isogeny exists by lemma 4. Then, necessarily, $[\overline{\mathfrak{p}}]$ reduces to the dual of the Frobenius on $\widetilde{E}$. Since $\overline{\mathfrak{p}}$ is coprime to $\mathfrak{p}$, this implies that $\overline{\mathfrak{p}}$ reduces to a separable morphism (by our old trick of composing with an isogeny to make it principal).

This shows that E is ordinary at p.

To prove (3): The same style of proof as in the first case works here too, the key is that $\overline{\mathfrak{p}} = \mathfrak{p}$.

□

3.3. **Ramified primes:** Finally, we want to show that there exists a lift of the Frobenius in the case where p is ramified in K. However, in this case $\mathfrak{p}$ is principal and things are much the same as in the inert case, just easier.

4. Second Main Theorem of CM:

4.1. **Why Weber functions:** In this section, $E[\mathfrak{a}]$ will denote the kernel of the isogeny $[\mathfrak{a}]$.

We would like to say that $K(j(E), E[\mathfrak{m}])$ is the ray class field of K and that the action of the Galois group on $E[\mathfrak{m}]$ is through the action of the ray class group of $\mathfrak{m}$.

But here already, we have a problem since we would expect the action of units to be trivial. However, units act as isomorphisms and certainly won't always be trivial.

There is also another problem in that $K(j(E), E[\mathfrak{m}])$ is not even necessarily Galois over $\mathbb{Q}$. See the comment here: https://mathoverflow.net/a/23390/58001 .

I thought we might be able to show this in the following way: We want to show that $K(j(E), E[\mathfrak{m}])$ is independent of the choice of E (as long as it has CM by the same ring). One might try to do this in the following way: Let E_1, E_2 be two such curves, we can find an isogeny of the form $[\mathfrak{q}]$ between them such that $\mathfrak{q}$ is coprime to $\mathfrak{m}$ and so the map on the $E[\mathfrak{m}]$ is an isomorphism under this isogeny.

Then, we want to show that for $P \in E[\mathfrak{m}]$ and $\sigma \in G_{K(j)}$, $\sigma([\mathfrak{q}]P) = [\mathfrak{q}]\sigma(P)$ to show that the map is Galois equivariant. However this is only true *upto units*! That is, $\sigma([\mathfrak{q}]P) = [u][\mathfrak{q}]\sigma(P)$ for $[u]$ an isomorphism of E_1.

Therefore, we need to first kill the action of isomorphisms if this is to work at all. That is the role of the Weber functions.

4.2. **Proof of the Second Main Theorem of CM:.** That is, we want to consider the image of the $\mathfrak{m}$ torsion under the map $h : E \longrightarrow E/Aut(E)$. Luckily enough, it is easy to make

sense of $E/Aut(A)$ as a scheme and even as a curve by considering instead the function field and taking invariants.

Then, by Riemann-Hurwitz it is easy to show that $E/\operatorname{Aut}(E)$ is always isomorphic to $\mathbb{P}^1$. Therefore, the Weber function $h : E \longrightarrow \mathbb{P}^1$ makes perfect sense and we can consider the image of the $\mathfrak{m}$ torsion under it.

Define $L = K(j(E), h(E[\mathfrak{m}]))$. We would like to show that this is the ray class field $K_{\mathfrak{m}}$ of K for the modulus $\mathfrak{m}$. Since L/K is clearly Galois, it suffices to show that the primes that split in L are precisely the principal primes that have a generator congruent to $1 \pmod{\mathfrak{m}}$.

This is not hard to do given what we know already. The idea is to use the fact that the reduction map is injective on $E[\mathfrak{m}]$ to translate the action of the isogeny $[\mathfrak{p}]$ on $E[\mathfrak{m}]$ in characteristic 0 to the action of the Frobenius in char p and then lift this to the action of the Frobenius in char 0.

First Direction:

Suppose $\mathfrak{p} = (\pi)$ is a prime of K that is principal and $\pi \equiv 1 \pmod{\mathfrak{m}}$. Then we need to show that $\mathfrak{p}$ splits in L.

This is equivalent to showing that $\sigma_{\mathfrak{p}}$, the frobenius of $\mathfrak{p}$, fixes E and $E[\mathfrak{m}]$. We know it fixes E by our results on the Hilbert Class field. To show that it fixes the $\mathfrak{m}$ torsion, consider the following diagram:

$$\begin{array}{ccc} E & \xrightarrow{[u\pi]} & E = \mathfrak{p} * E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{F_{\mathfrak{p}}} & \widetilde{E}^{(p)} \end{array}$$

where u is a unit. The endomorphism $[\pi]$ acts trivially on the $\mathfrak{m}$ torsion and therefore $u\pi$ acts trivially on the image $h(E[\mathfrak{m}])$. Since the reduction map is injective on $E[\mathfrak{m}]$, the same is true of $F_{\mathfrak{p}}$.

However, $F_{\mathfrak{p}}$ is also the reduction of the char 0 map that sends $P \longrightarrow \sigma_{\mathfrak{p}}(E)$ and once again, using that reduction is injective on the $\mathfrak{m}$ torsion, we obtain that $\sigma_{\mathfrak{p}}(E)$ acts trivially on $h(E[\mathfrak{m}])$ as required.

Second Direction:

Now suppose that $\mathfrak{p}$ is a prime of K that splits completely in L. In particular, it splits completely in $K(j(E))$ and is therefore principal.

Further, we can choose π to be a lift of $F_{\mathfrak{p}}$. Since $\mathfrak{p}$ splits completely, we know that the Frobenius acts trivially. As in the first direction but going in reverse, this lets us conclude that $[\pi]$ acts trivially on $E[\mathfrak{m}]$ for some generator π.

This is equivalent to saying that $\pi \equiv 1 \pmod{\mathfrak{m}}$ which is what we were required to show.

The L-function of a CM curve:

The final step is also quite easy given what we already know. Let $\mathfrak{q}$ be a prime of $K(j(E))$ over a prime $\mathfrak{p}$ of K. Let $F = F_{\mathfrak{p}}$ be the Frobenius in chat p of degree $N\mathfrak{p}$.

Note that, in char p, $F_{\mathfrak{q}} = F_{\mathfrak{q}}^n$ where n is the order of $\mathfrak{p}$ in the class group or equivalently, the inertia degree $f(\mathfrak{q}/\mathfrak{p}) = n$. Therefore, by our results on lifting Frobenius elements, we can lift the Frobenius $F_{\mathfrak{q}}$ over $\kappa(\mathfrak{q})$ to a principal isogeny $\pi(\mathfrak{q}/\mathfrak{p})$. We do this by taking the $n - th$ power of the lift of $F_{\mathfrak{p}}$.

Next, note that $N_{\mathfrak{q}} = |E(\kappa(\mathfrak{q}))| = \deg(F_{\mathfrak{q}} - 1) = \deg(\pi(\mathfrak{q}/fp) - 1)$. Since $\deg(\pi(\mathfrak{q}/\mathfrak{p})) = N(\mathfrak{q})$, we have:

$$N_{\mathfrak{q}} = N(\mathfrak{q}) + \pi - (\overline{\pi}) + 1$$

and therefore, we can factor the Euler factor $L(E, s) = L(\psi, K(j))L(\overline{\psi}, k(j))$ by setting $\psi(\mathfrak{q}) = \pi(\mathfrak{q}/fp) \in K^{\times} \subset \mathbb{C}$.

5. An extra result

The question is from here: https://mathoverflow.net/questions/134921/abelian-image-of-l-adic-representation .

Theorem 6. *Let E/F be an Elliptic curve defined over a number field F and suppose that E has complex multiplication by an order in K. Consider the representation:*

$$\rho_l : G_F \longrightarrow \mathrm{End}_{\mathbb{Z}_l}(V_l).$$

The image G is abelian precisely when F contains K.

Proof. One direction is trivial since if F contains K, the the action of G_F commutes with the action of K_l on V_l and therefore, G_F acts as K_l endomorphisms on the one dimensional (over K_l) vector space V_l.

In the other direction, suppose KF/F is a non trivial extension. It is a 2 element group, let τ be the non trivial element. We already know that the image of G_{KF} is abelian by the first part. Therefore, to show that G is not abelian is equivalent to the following:

Let H be the image of G_{FK} in G and denote the image of τ in G also by τ. Then, G is abelian precisely when the conjugation action of τ on H is non trivial.

Now, we know that H is a subgroup of $K_l^{\times}$. Let $\sigma \in G_{FK}$ map to $\alpha \in K_l^{\times}$. That is, for $P \in V_l, \sigma(P) = \alpha(P)$. I claim that $\tau\sigma\tau^{-1}$ maps to $\tau^{-1}(\alpha)$. This is because:

$$\tau\sigma\tau^{-1}(P) = \tau\sigma(\tau^{-1}(P)) = \tau\alpha(\tau^{-1}(P)) = \tau\tau^{-1}(\tau^{-1}(\alpha)(P)) = \tau^{-1}(\alpha).$$

Therefore, it suffices to find an $\alpha \in K^{\times} - \mathbb{Z}$ that is in the image of G_{FK}. I claim that the Frobenius of a prime in F that splits completely in FK will work. In fact, we might as well assume that the prime splits completely over $\mathbb{Q}$. In this case, we have a split prime in K that is principal and splits completely in FK.

Therefore, the isogeny corresponding to this will be an endomorphism (since it is principal) and moved by τ since it is split over $\mathbb{Q}$.

□