

COMPLEX MULTIPLICATION ON ELLIPTIC CURVES

SHAWN DRENNING
DISCUSSED WITH PROFESSOR MARK KISIN

1. INTRODUCTION

It is well known that the maximal abelian extension of \mathbb{Q} is generated by all roots of unity. For an imaginary quadratic number field K , there is a similar construction of the maximal abelian extension using the torsion points (and j -invariant) of a particular elliptic curve. We will give an outline of the theory here, closely following the exposition of Silverman [6].

2. ELLIPTIC CURVES

Definition 2.1. An *elliptic curve* is a pair (E, O) , where E is a curve of genus 1 and $O \in E$. The elliptic curve E is *defined over* K , written E/K , if E is defined over K as a curve and $O \in E(K)$.

Using the Riemann-Roch theorem, we can show that every elliptic curve is isomorphic to a curve (defined over the same field) given by a Weierstrass equation

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Conversely, any smooth curve given by a Weierstrass equation is an elliptic curve with $O = [0, 1, 0]$. A Weierstrass equation defined over a field of characteristic different from 2, 3 can be simplified to the form

$$E : y^2 = x^3 + Ax + B.$$

Finally, to each curve we have a j -invariant $j(E) \in \overline{K}$. Two elliptic curves are isomorphic if and only if they have the same j -invariant.

One of the most important properties of an elliptic curve is that it can be made into an abelian group with O as an identity. This is done by using the Riemann-Roch theorem to give a bijection of sets between E and $\text{Pic}^0(E)$. When E is given by a Weierstrass equation, this group law has a geometric interpretation and can be written explicitly in terms of rational functions.

We would like to study morphisms of E (as a curve) that respect the group structure. It can be proven that any morphism that sends O to O is a group homomorphism. We call such a map an *isogeny* and denote the group (under addition) of isogenies from E_1 to E_2 by $\text{Hom}(E_1, E_2)$. The set $\text{End}(E) = \text{Hom}(E, E)$ becomes a ring under the multiplication law given by composition. For each m , we have a multiplication by m map

$$[m] : E \rightarrow E$$

on any elliptic curve. This map is actually an isogeny and gives an injection

$$[\] : \mathbb{Z} \rightarrow \text{End}(E).$$

When this map is not an isomorphism, we say that E has *complex multiplication*.

2.1. Elliptic Curves over \mathbb{C} . It will be convenient for us to be able to view elliptic curves over \mathbb{C} as lattices in \mathbb{C} . First note that an elliptic curve over \mathbb{C} is a complex Lie group since it is the zero set of a non-singular polynomial and the group law is given locally by rational functions. We now have the following equivalence of categories

Theorem 2.1. *The following categories are equivalent:*

- (1) *Objects: Elliptic curves over \mathbb{C} .
Maps: isognies*
- (2) *Objects: Elliptic curves over \mathbb{C} .
Maps: Complex analytic maps taking O to O .*
- (3) *Objects: Lattices $\Lambda \subset \mathbb{C}$, up to homothety.
Maps: $\text{Map}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$.*

Denote the elliptic curve given by a lattice Λ by E_Λ .

2.2. The Reduction of Elliptic Curves. Let K be a local field complete with respect to some discrete valuation v and E/K be an elliptic curve given by a Weierstrass equation. The Weierstrass equation can be renormalized so that its coefficients are in R , the ring of integers of K . If π is a uniformizer for R , we can reduce the Weierstrass equation modulo π to obtain a Weierstrass equation for a curve \tilde{E}/k , where k is the residue field of R . If $v(\Delta) = 0$ (where Δ is the discriminant for E), then \tilde{E} will be non-singular and thus, an elliptic curve over k . By looking at a renormalized Weierstrass equation for E/K with minimal $v(\Delta)$, it is possible to associate to each E/K a unique \tilde{E}/k . Now assume that K is a global field and let \mathfrak{P} be a finite prime of K . If E/K is an elliptic curve given by a Weierstrass equation, we can view E as being defined over the completion of K with respect to \mathfrak{P} and as above associate a curve \tilde{E}/k to E . If \tilde{E} is non-singular, E is said to have *good reduction* at \mathfrak{P} . We will need the following theorem about how torsion points behave with respect to reduction:

Theorem 2.2. *Let E/K be an elliptic curve and \tilde{E}/k be the reduction of E at a prime with good reduction. If $m \geq 1$ is an integer relatively prime to $\text{char}(k)$, then the reduction map*

$$E(K)[m] \rightarrow \tilde{E}(k)$$

is injective.

3. CLASS FIELD THEORY

In order to state and prove the theorems of complex multiplication, we will need some class field theory. We give an overview of the class field theory we will need here.

Let L/K be a finite Galois extension of a number field K with Galois group G . We denote by R_L and R_K the ring of integers of L and K respectively. Let \mathfrak{P} be a prime of L lying over the prime \mathfrak{p} of K . If \mathfrak{p} does not ramify in L , then the natural map from $D(\mathfrak{P})$ (the decomposition group of \mathfrak{P}) to $\text{Gal}((R_L/\mathfrak{P})/(R_K/\mathfrak{p}))$ is an isomorphism. By pulling back the Frobenius element of this group, we get a unique $\sigma_{\mathfrak{P}} \in D(\mathfrak{P})$ satisfying

$$(3.1) \quad \sigma_{\mathfrak{P}}(x) \equiv x^{\text{Nm}_{\mathbb{Q}}^K \mathfrak{p}} \pmod{\mathfrak{P}}$$

for all $x \in R_L$. If \mathfrak{P}_1 and \mathfrak{P}_2 are two primes lying over \mathfrak{p} , then $\sigma_{\mathfrak{P}_1}$ and $\sigma_{\mathfrak{P}_2}$ are in the same conjugacy class of G . Therefore, if G is abelian we can define a $\sigma_{\mathfrak{p}}$ satisfying (3.1) for all \mathfrak{P} lying over \mathfrak{p} .

Now let \mathfrak{c} be an ideal of R_K divisible by all the primes that ramify in L and $I(\mathfrak{c})$ be the group of all fractional ideals of K relatively prime to \mathfrak{c} . We define the *Artin Map*

$$(\cdot, L/K) : I(\mathfrak{c}) \rightarrow \text{Gal}(L/K)$$

to be the group homomorphism defined on prime ideals by

$$(\mathfrak{p}, L/K) = \sigma_{\mathfrak{p}}.$$

We can now state a version of Artin's reciprocity law for totally imaginary number fields.

Theorem 3.1. *Let L/K be a finite abelian extension of totally imaginary number fields. There exists an integral ideal $\mathfrak{c} \subset R_K$, divisible by precisely the primes of K that ramify in L , such that*

$$(\mathfrak{a}, L/K) = 1$$

for all

$$\mathfrak{a} \in P(\mathfrak{c}) = \{(\alpha) : \alpha \in K^*, \alpha \equiv 1 \pmod{\mathfrak{c}}\}.$$

If (3.1) holds for two ideals \mathfrak{c}_1 and \mathfrak{c}_2 , then it will hold for $\mathfrak{c}_1 + \mathfrak{c}_2$. As a consequence, there is a largest ideal $\mathfrak{c}_{L/K}$ for which (3.1) holds. We call this ideal the *conductor* of L/K .

Definition 3.1. Let \mathfrak{c} be an integral ideal of K . A *ray class field of K (modulo \mathfrak{c})* is a finite abelian extension $K_{\mathfrak{c}}/K$ with the property that for any finite abelian extension L/K ,

$$\mathfrak{c}_{L/K} | \mathfrak{c} \Rightarrow L \subset K_{\mathfrak{c}}$$

Theorem 3.2. *Let L/K be a finite abelian extension of number fields, and let \mathfrak{c} be an integral ideal of K .*

- (1) *The Artin map*

$$(\cdot, L/K) : I(\mathfrak{c}_{L/K}) \rightarrow \text{Gal}(L/K)$$

is a surjective homomorphism.

- (2) *The kernel of the Artin map is $(\text{Nm}_K^L I_L)P(\mathfrak{c}_{L/K})$, where I_L is the group of non-zero fractional ideals of L .*
 (3) *There exists a unique ray class field $K_{\mathfrak{c}}$ of K (modulo \mathfrak{c}). The conductor of $K_{\mathfrak{c}}/K$ divides \mathfrak{c} .*
 (4) *The ray class field $K_{\mathfrak{c}}$ is characterized by the property that it is an abelian extension of K and satisfies*

$$\{\text{primes of } K \text{ that split completely in } K_{\mathfrak{c}}\}$$

are the same as

$$\{\text{prime ideals in } P(\mathfrak{c})\}.$$

Definition 3.2. We call the ray class field of K modulo the unit ideal $\mathfrak{c} = (1)$ the *Hilbert Class Field* of K .

The *Hilbert Class Field* of K is the largest abelian extension of K in which no prime ramifies.

Finally, we will need an analytic result which allows us to characterize field extensions from the primes that split in them.

Definition 3.3. If S and T are two sets of primes in a number field K , $S \prec T$ if $S - Z \subset T$ where Z is a subset of primes of Dirichlet density 0.

Theorem 3.3. Let L/K be a Galois extension and E a finite extension of K . Denote by $S_{L/K}$ and $S_{E/K}$ the primes of K that split completely in L and E respectively. Then $S_{L/K} \prec S_{E/K}$ if and only if $E \subset K$.

4. THE MAXIMAL ABELIAN EXTENSION OF AN IMAGINARY QUADRATIC NUMBER FIELD

We now want to show how to explicitly generate the maximal abelian extension of an imaginary quadratic number field K using the theory of elliptic curves. This is done by studying elliptic curves with endomorphism ring R_K . Denote the set of isomorphism classes of such elliptic curves $\mathcal{E}\mathcal{L}\mathcal{L}(R_K)$. Observe that any fractional ideal \mathfrak{a} of K is a lattice in \mathbb{C} ; this gives us an elliptic curve $E_{\mathfrak{a}} \in \mathcal{E}\mathcal{L}\mathcal{L}(R_K)$. If \mathfrak{a} is a fractional ideal of K and Λ is a lattice in \mathbb{C} we define

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r : \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}.$$

It is then elementary to prove the following theorem:

Theorem 4.1. Let Λ be a lattice with $E_{\Lambda} \in \mathcal{E}\mathcal{L}\mathcal{L}(R_K)$, and let \mathfrak{a} and \mathfrak{b} be non-zero fractional ideals of K .

- (1) $\mathfrak{a}\Lambda$ is a lattice in \mathbb{C} .
- (2) $\text{End}(E_{\mathfrak{a}\Lambda}) \cong R_K$.
- (3) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\mathfrak{a} = \mathfrak{b}$ in $\mathcal{C}\mathcal{L}(R_K)$.
- (4) The action

$$\bar{\mathfrak{a}} * E_{\Lambda} = E_{\mathfrak{a}^{-1}\Lambda}$$

of $\mathcal{C}\mathcal{L}(R_K)$ on $\mathcal{E}\mathcal{L}\mathcal{L}(R_K)$ is simply transitive. In particular, $\mathcal{E}\mathcal{L}\mathcal{L}(R_K)$ is a finite set.

Since $\mathcal{E}\mathcal{L}\mathcal{L}(R_K)$ is finite, by looking at the action of $\text{Aut}(\mathbb{C})$ on $\mathcal{E}\mathcal{L}\mathcal{L}(R_K)$, it is easy to show that $j(E) \in \overline{\mathbb{Q}}$ for every $E \in \mathcal{E}\mathcal{L}\mathcal{L}(R_K)$. Using this, we can show that E can be defined over $\overline{\mathbb{Q}}$. As a result, we have a natural action of $\text{Gal}(\overline{K}/K)$ on $\mathcal{E}\mathcal{L}\mathcal{L}(R_K)$ given by

$$\sigma * E = E^{\sigma}.$$

Since the action of $\mathcal{C}\mathcal{L}(R_K)$ on $\mathcal{E}\mathcal{L}\mathcal{L}(R_K)$ is simply transitive, for each $\sigma \in \text{Gal}(\overline{K}/K)$ there is a unique $\bar{\mathfrak{a}} \in \mathcal{C}\mathcal{L}(R_K)$ with $E^{\sigma} = \bar{\mathfrak{a}} * E$. This gives us a map $F : \text{Gal}(\overline{K}/K) \rightarrow \mathcal{C}\mathcal{L}(R_K)$ with the following properties:

Theorem 4.2. Let K/\mathbb{Q} be a quadratic imaginary field. There exists a homomorphism

$$F : \text{Gal}(\overline{K}/K) \rightarrow \mathcal{C}\mathcal{L}(R_K)$$

uniquely characterized by the condition

$$E^{\sigma} = F(\sigma) * E$$

for all $\sigma \in \text{Gal}(\overline{K}/K)$ and all $E \in \mathcal{E}\mathcal{L}\mathcal{L}(R_K)$.

Proof. We have shown that such a map F exists and it is easy to see that F is actually a homomorphism. The crucial point in showing that the definition of F is independent of E is to show that if $\bar{\mathfrak{a}} \in \mathcal{CL}(R_K)$ and $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, then

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

Once this is known, it is an easy calculation to show that the definition of F is independent of E . \square

We can now give the first main result:

Theorem 4.3. $L = K(j(E))$ is the Hilbert class field H of K .

Proof. The first step is to show that the kernel of the map F from the previous theorem is $\text{Gal}(\bar{K}/L)$. It follows that F maps $\text{Gal}(L/K)$ injectively into $\mathcal{CL}(R_K)$ and, as a result, $\text{Gal}(L/K)$ is an abelian extension. The next step is to relate the map F to the Artin map. More precisely, it can be shown that

$$F((\mathfrak{a}, L/K)) = \bar{\mathfrak{a}} \text{ for all } \mathfrak{a} \in I(\mathfrak{c}_{L/K})$$

where $\mathfrak{c}_{L/K}$ is the conductor of L/K . It follows that

$$F((\alpha), L/K) = 1$$

for all principal ideals $(\alpha) \in I(\mathfrak{c}_{L/K})$ and since F is injective on $\text{Gal}(L/K)$

$$((\alpha), L/K) = 1$$

for all principal ideals $(\alpha) \in I(\mathfrak{c}_{L/K})$. Since the conductor of L/K is the largest ideal with this property, this shows that $\mathfrak{c}_{L/K} = (1)$ and no prime of K ramifies in L . Therefore, L is contained in the Hilbert class field of K . By comparing degrees of the two extensions, it follows that $L = K(j(E))$ is actually equal to the Hilbert class field of K . \square

From this result it follows that any elliptic curve in $\mathcal{ELL}(R_K)$ can be defined over the Hilbert class field of K .

Next we give a lemma that is essential to the proof of the main theorem

Lemma 4.4. Let K be a quadratic imaginary field, H the Hilbert class field of K , and E/H an elliptic curve with complex multiplication by R_K . For all but finitely many degree 1 prime ideals \mathfrak{p} of K that satisfy

$$(\mathfrak{p}, H/K) = 1,$$

E has good reduction at all primes \mathfrak{P} lying over \mathfrak{p} and there is a unique $\pi \in R_K$ so that $\mathfrak{p} = \pi R_K$ and $[\pi]$ reduces to the p th power Frobenius map (where \mathfrak{p} lies over p).

Let $E \in \mathcal{ELL}(R_K)$. For each $\alpha \in R_K$, we have a map $[\alpha] \in \text{End}(E)$. For any integral ideal \mathfrak{a} of R_K , we define

$$E[\mathfrak{a}] = \{P \in E : [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

We also denote by E_{tors} the union over all $m \in \mathbb{N}$ of $E[mR_K]$. We need one more definition before we state the main theorem.

Definition 4.1. Let E/H be an elliptic curve. A map

$$h : E \rightarrow E/\text{Aut}(E)$$

defined over H is called a *Weber function* for E/H .

Theorem 4.5. *Let K be a quadratic imaginary field, let E be an elliptic curve with complex multiplication by R_K , and let $h : E \rightarrow E/\text{Aut}(E)$ be a Weber function for E/H . Let \mathfrak{c} be an integral ideal of R_K . Then the field*

$$L = K(j(E), h(E[\mathfrak{c}]))$$

is the ray class field of K modulo \mathfrak{c} .

Proof. The first step is to verify that L/K is an abelian extension. Next, to show that L is the ray class field of K modulo \mathfrak{c} , we need to show that

$$(\mathfrak{p}, L/K) = 1 \Leftrightarrow \mathfrak{p} \in P(\mathfrak{c}).$$

Since the primes in the kernel of the Artin map are precisely the primes that split in L and the primes of degree greater than 1 have Dirichlet density 0, by (3.3) it is enough to show this for all but finitely many primes of degree 1.

Any degree 1 prime $\mathfrak{p} \in P(\mathfrak{c})$ is of the form $\mathfrak{p} = xR_K$ for some $x \equiv 1 \pmod{\mathfrak{c}}$. Since \mathfrak{p} is principal, $(\mathfrak{p}, H/K) = 1$; it follows that to show $(\mathfrak{p}, L/K) = 1$ it is enough to show that $(\mathfrak{p}, L/K)$ fixes any element of $h(E[\mathfrak{c}])$.

Ignoring a finite set of primes, we may assume that \mathfrak{p} satisfies the conditions of (4.4) and thus $\mathfrak{p} = \pi R_K$ where $[\pi]$ reduces to the p th power Frobenius map ϕ . It follows that $\pi = ux$ for some unit u of R_K . Now let $T \in E[\mathfrak{c}]$. From the definition of the Artin symbol and the fact that $[\pi]$ reduces to ϕ , we have

$$T^{\widetilde{(\mathfrak{p}, L/K)}} = \phi(\tilde{T}) = [\pi]\tilde{T}.$$

After ignoring another finite set of primes, theorem 2.2 implies that $T^{(\mathfrak{p}, L/K)} = [\pi]T$. From this and the fact that h is defined over H we have

$$h(T)^{(\mathfrak{p}, L/K)} = h\left(T^{(\mathfrak{p}, L/K)}\right) = h([\pi]T)$$

Since $\pi = ux$ and h is $\text{Aut}(E)$ -invariant, we have

$$h([\pi]T) = h([u] \circ [x]T) = h([x]T).$$

Finally, since $T \in E[\mathfrak{c}]$ and $x \equiv 1 \pmod{\mathfrak{c}}$, we have

$$h([x]T) = h(T).$$

We conclude that $h(T)^{(\mathfrak{p}, L/K)} = h(T)$ and thus, $(\mathfrak{p}, L/K) = 1$.

Now let \mathfrak{p} be a degree 1 prime with $(\mathfrak{p}, L/K) = 1$. Since $H \subset L$, we also have $(\mathfrak{p}, H/K) = 1$. After ignoring finitely many primes, (4.4) tells us that there is a π so that $\mathfrak{p} = \pi R_K$ and $[\pi]$ reduces to the Frobenius element. Now for any $T \in E[\mathfrak{c}]$, a straightforward calculation shows that

$$\tilde{h}([\pi]\tilde{T}) = \tilde{h}(\tilde{T})$$

Since \tilde{h} is a map into

$$E/\widetilde{\text{Aut}(E)} \cong \tilde{E}/\widetilde{\text{Aut } \tilde{E}},$$

where $\widetilde{\text{Aut}(E)}$ is the image of $\text{Aut}(E)$ in $\text{Aut}(\tilde{E})$, it follows that

$$[\pi]\tilde{T} = [u]\tilde{T}$$

for some $u \in \text{Aut}(E) = R_K^*$. After ignoring another finite set of primes, (2.2) implies $[\pi - u]T = O$. It is not hard to verify that $E[\mathfrak{c}]$ is a free R_K/\mathfrak{c} -module of

rank one. It follows that $[\pi - u]$ annihilates all of $E[\mathfrak{c}]$. We conclude that $\pi - u \in \mathfrak{c}$ and thus

$$\pi u^{-1} \equiv 1 \pmod{\mathfrak{c}}.$$

Since π and πu^{-1} generate the same ideal, $\mathfrak{p} \in P(\mathfrak{c})$. □

Corollary 4.6.

$$K^{ab} = K(j(E), h(E_{\text{tors}})).$$

Proof. If L/K is an abelian extension with conductor $\mathfrak{c}_{L/K}$, from class field theory and the theorem we have

$$L \subset K(j(E), h(E[\mathfrak{c}_{L/K}])) \subset K(j(E), h(E_{\text{tors}})).$$

On the other hand, the theorem tells us that $K(j(E), h(E_{\text{tors}}))$ is a compositum of abelian extensions and hence abelian. □

REFERENCES

- [1] S. Lang. *Algebraic Number Theory*. Springer-Verlag, 2nd edition, 1994.
- [2] J. Milne. *Class Field Theory*. www.jmilne.org/math, 1997.
- [3] J. Milne. *Algebraic Number Theory*. www.jmilne.org/math, 1998.
- [4] J.-P. Serre. Complex multiplication. In J. W. S. Cassels and Fr editors, *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society*, pages 190–197.
- [5] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
- [6] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.