Complex Multiplication and Elliptic Curves

Andrew Lin

Abstract

In this expository paper, we provide an introduction to the theory of complex multiplication (CM) of elliptic curves. By understanding the connection of an elliptic curve's endomorphism ring with the Galois group of the set of points on the curve $E[n]$ of order n, we can study abelian extensions of $\mathbb{Q}$ and $\mathbb{Q}[i]$ and understand a simple case of Hilbert's twelfth problem. Finally, we will present (in as much detail as reasonable) an explanation for the "almost-integer" $e^{\pi\sqrt{163}}$, which is the result of a connection between the j-invariant modular function and the study of complex multiplication.

1 Introduction

This paper will develop some basic results in the study of elliptic curves with complex multiplication, building off of the brief overview presented in the Spring 2020 instance of MIT's Seminar in Number Theory (18.784). One point discussed during class is that the Weierstrass identification between an elliptic curve and its corresponding complex torus allows for a natural group law to be defined on the elliptic curve, in which three collinear points on the curve correspond to three points on the torus that sum to zero. Because this group structure can be described in a geometric way, we are motivated to study the behavior of the whole complex torus under maps known as **endomorphisms**, and we will see through this discussion that the endomorphism rings can be particularly nicely described in terms of their **orders**.

The discussion begins in Section 2, where we introduce the concept of an endomorphism of an elliptic curve, as well the ring of endomorphisms for that curve. Section 3 will provide a natural connection of the number theoretic content to a more algebraic subject: we will discuss the Kronecker–Weber theorem (and prove a simple special case), which states that all abelian Galois extensions of $\mathbb{Q}$ are subfields of a special class of field extensions known as **cyclotomic fields**. We will then generalize this statement to a larger class of number fields, briefly discussing the formulation of Hilbert's twelfth problem, before bringing an explicit elliptic curve into the picture to understand a specific instance in which complex multiplication generates our desired field extensions. Finally, we will conclude in section 4 by introducing some class field theory, which will give us a brief glimpse into the connection between the j-invariant modular function and the properties of imaginary quadratic extensions. The role of complex multiplication here is to allow us to pick out specific **orders** of quadratic fields, and we will subsequently find an unlikely connection between the unique factorization of the ring of integers $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ and the value of the j-invariant at a specific (related) point.

Presentation of results will loosely follow [4], [6], and [7], with motivation and additional remarks coming from [3] and [5].

2 Endomorphism rings and complex multiplication

For any elliptic curve E, we denote the n**-torsion subgroup** $E[n]$ to be the set of points on an elliptic curve of order dividing n:

$$E[n] = \{P \in E : nP = \mathcal{O}\},$$

where $\mathcal{O}$ is the identity element under the elliptic curve group law (corresponding to the point at infinity).

Proposition 1. *For any n, $E[n]$ is isomorphic to the direct sum $(\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$.*

Proof. Recall that every elliptic curve E can be identified with a complex torus $\mathbb{C}/\Lambda$, where Λ is a lattice in the complex plane, and this identification is made such that the group law on the elliptic curve corresponds to adding the corresponding elements on the torus (that is, adding the cosets of Λ in $\mathbb{C}$). Thus, any point in $E[n]$ corresponds to a point $p \in \mathbb{C}/\Lambda$ such that $np \in \Lambda$: if Λ is generated by ω_1, ω_2, it is clear that any such element is of the form $p = \frac{a\omega_1}{n} + \frac{b\omega_2}{n}$ for integers $0 \le a, b < n$, showing the desired result. □

While it is useful to consider the structure of these finite sets of points, it is also interesting to look at maps on the entire elliptic curve, which motivates the next definitions:

Definition 2. *An* ***isogeny*** *of elliptic curves E_1, E_2 is a nonzero holomorphic group homomorphism (equivalently, an algebraic homomorphism) $\phi : E_1 \to E_2$.*

Definition 3. *An* ***endomorphism*** *of an elliptic curve E is an isogeny from E to itself. The* ***endomorphism ring*** *of E, denoted End(E), is the set of all endomorphisms of E, with addition being defined pointwise and multiplication being defined by composition.*

The sum of two endomorphisms is indeed an endomorphism (because each individual endomorphism fixes the origin $\mathcal{O}$, so their sum will also do so), and any composition of isogenies is an isogeny, so the set of endomorphisms is closed under addition and multiplication. In order to confirm that we have a ring, we just need to verify that we have a multiplicative identity (which is the identity endomorphism) and that distributivity holds (which comes from the fact that isogenies are group homomorphisms).

Example 4. *The multiply-by-n map, which sends a point $P \in E$ to $nP \in E$, is an endomorphism. (This corresponds to scaling the complex torus by n.)*

In particular, this means that every endomorphism ring contains a subring isomorphic to $\mathbb{Z}$, since we can always apply a multiply-by-n map for any integer n.

Example 5. *The elliptic curve $E : y^2 = x^3 + x$ has an endomorphism*

$$\phi(x, y) = (-x, iy),$$

since $(iy)^2 = (-x)^3 + (-x)$, ϕ^4 is the identity map, but (x, y) is not generally a point of any particular order, so ϕ is not a multiply-by-n map.

This last example is exceptional – most elliptic curves do not have such endomorphisms, and those that do are particularly nice to study.

Definition 6. *An elliptic curve E has* ***complex multiplication*** *(CM) if $End(E) \supsetneq \mathbb{Z}$.*

In other words, a CM elliptic curve has a nontrivial endomorphism. To motivate this name, consider what our endomorphisms look like on the complex plane for the corresponding complex torus of E. Because the endomorphisms preserve both group and local structure, an endomorphism ϕ must correspond to a holomorphic map $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ such that $f(w + z + \Lambda) = f(w + \Lambda) + f(z + \Lambda)$ for any $w, z \in \mathbb{C}/\Lambda$. As discussed in Section 1.3 of [1], such maps only exist when our function looks like

$$f(z) = mz, \quad m \in \mathbb{C}$$

in a neighborhood around $z = 0$, such that $m\Lambda \subseteq \Lambda$. Any integer m works (and corresponds to a multiplication-by-m map), but any other real number would not take elements of the lattice to elements of the lattice, so we would not have a well-defined endomorphism. Thus the name **complex multiplication** reflects the fact that our lattice is being "rotated" by a nontrivial endomorphism.

Definition 7. *If a CM elliptic curve has a complex multiplication $f(z) = mz$ for some m in the* ***upper half-plane*** $\mathbb{H} \equiv \{x + iy : y > 0, x \in \mathbb{R}\}$*, then we call m a* ***CM point****.*

By our above work, any such CM point m is associated to a lattice Λ_τ spanned by 1 and some $\tau \in \mathbb{H}$ (and therefore the elliptic curve $\mathbb{C}/\Lambda_\tau$). Then m must be an element of this lattice and so must m^2, which means that m^2 is some rational combination of 1 and m and thus an **algebraic number** of degree 2.

Finally, note that we can restrict any endomorphism of E to the finite set of points $E[n]$. Since this is a finite $\mathbb{Z}$-module of rank 2, and in particular a free $(\mathbb{Z}/n\mathbb{Z})$-module, we can represent the endomorphism by where two basis elements go. This yields a 2×2 matrix with entries in $\mathbb{Z}/n\mathbb{Z}$, and basis-independent invariants of this matrix, such as the trace and determinant, which are useful for studying properties of elliptic curves over finite fields. In particular, understanding the analogy of the determinant when we don't restrict to $E[n]$ is a key tool in proving Hasse's theorem for elliptic curves. More information about the **degree** of an endomorphism and its use can be found in lectures 7 and 8 of [6].

3 The Kronecker–Weber theorem and abelian extensions

The theory of CM elliptic curves has various applications in algebra and algebraic number theory, and we introduce one of those connections in this section with an introduction to Hilbert's twelfth problem.

3.1 Field extensions over the rationals

We begin by discussing a particular type of "nicely-behaving" field extension:

Definition 8. *A* ***cyclotomic extension*** *or* ***cyclotomic field*** *is a field $\mathbb{Q}(\zeta)$ obtained by adjoining a root of unity ζ to $\mathbb{Q}$.*

Denoting $\zeta_n = e^{2\pi i/n}$, we know that

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i),$$

and thus our cyclotomic extensions are Galois extensions over $\mathbb{Q}$ with splitting field $x^n - 1$ for some integer n. It is natural to ask about the Galois group of such an extension (the set of automorphisms of $\mathbb{Q}(\zeta_n)$ which fix $\mathbb{Q}$), and in this case the result is particularly simple:

Proposition 9. *There exists an injective homomorphism from Gal($\mathbb{Q}(\zeta_n)/\mathbb{Q}$) to $(\mathbb{Z}/n\mathbb{Z})^*$, the multiplicative group of integers mod n.*

In fact, the Galois group $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is actually isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, so there are exactly $\phi(n)$ elements in this group. However, since we are interested in considering subfields of cyclotomic extensions, we do not need the stronger result here.

Proof. All nth roots of unity are of the form ζ_n^k for some integer k. Since σ must preserve the order of ζ_n, we must send it to another primitive root of unity $\zeta_n^{m(\sigma)}$. It is easy to verify that the map $\sigma \to m(\sigma)$ is indeed a homomorphism (since σ is an automorphism). Any automorphism σ in the Galois group is uniquely determined by where it sends ζ_n (because $\mathbb{Q}$ is fixed, and ζ_n^j is sent to $\sigma(\zeta_n)^j$), so this map is also injective, as desired. □

The above result tells us that since $(\mathbb{Z}/n\mathbb{Z})^*$ is abelian, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is a subgroup of an abelian group, meaning it is also abelian. Notably, this means that any subgroup of the Galois group is abelian and therefore normal, and Galois theory now tells us that if we have an intermediate field $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta)$, we can use the Galois correspondence to say that

$$\frac{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta_n)/L)} = \text{Gal}(L/\mathbb{Q})$$

is a finite abelian group as well – in particular, L is Galois. In other words, every subfield of a cyclotomic field is finite abelian, and we actually have the striking result that the converse is also true:

Theorem 10 (Kronecker–Weber)**.** *Let F be a Galois extension over $\mathbb{Q}$ with finite abelian Galois group Gal($F/\mathbb{Q}$). Then F is contained in a cyclotomic extension $\mathbb{Q}(\zeta)$.*

This result was first introduced in 1853, but the first correct proof was presented in 1896 by Hilbert, and subsequent generalizations have been established with the help of class field theory. The proof of the theorem is outside the scope of this paper – a proof may be found in [2] – but we will present a special case here.

Proof for quadratic extensions. Note that any quadratic extension over $\mathbb{Q}$ can be formed by adjoining a single element of degree 2: by the quadratic formula, this element is of the form $\frac{a+\sqrt{b}}{c}$ for rational numbers a, b, c, and thus it suffices to adjoin a single element $\sqrt{N}$, where N is a squarefree integer. Our goal is to show that $F = \mathbb{Q}(\sqrt{N})$ is contained in a cyclotomic field.

But we can factor N as a product of primes (no prime shows up multiple times), and we can adjoin two roots of unity ζ_m and ζ_n by simply adjoining ζ_{mn} instead. In addition, $\sqrt{-1} = e^{\pi i/2}$ is already a root of unity. Therefore, it suffices to prove this result for the case where we adjoin $\sqrt{p}$ to $\mathbb{Q}$ for any prime p.

For $p = 2$, we can simply adjoin $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, and for odd primes, we can consider the complex number

$$\gamma = \sum_{i=0}^{p-1} \zeta^{i^2},$$

where $\zeta = e^{2\pi i/p}$. This sums over all quadratic residues twice (except it only counts ζ^0 once), so γ^2 is p when the prime is 1 mod 4 and $-p$ when the prime is 3 mod 4 (the details of evaluating this quadratic Gauss sum can be found in exercise 4.4 of [4]). In both cases, this means we can always consider a primitive $(4p)$th root of unity: since $\sqrt{p}$ and i will both be contained in $\mathbb{Q}(\zeta_{4p})$, we've found an explicit cyclotomic field containing $\sqrt{p}$, and this proves the theorem in our special case. □

We can begin to see the connection here to elliptic curves with the following result:

Proposition 11. *Let E be an elliptic curve of the form $y^2 = x^3 + ax^2 + bx + c$ with rational coefficients. Letting $\mathcal{O}$ denote the point at infinity, and suppose that*

$$E[n] = \{(x_1, y_1), \cdots, (x_m, y_m), \mathcal{O}\}$$

is the coordinate representation of the points of the n-torsion subgroup. Then

$$\mathbb{Q}(E[n]) \equiv \mathbb{Q}(x_1, y_1, \cdots, x_m, y_m)$$

is a (not necessarily abelian) Galois extension of $\mathbb{Q}$.

Proof. It is easy to show that x_1 and y_1 are algebraic over $\mathbb{Q}$ by explicitly writing out the group law, since we can write the x-coordinate of the point $n(x_i, y_i)$ as a rational function in x and set the denominator equal to zero. And because $y_i^2 = x_i^3 + ax_i^2 + bx_i + c$ for all i, this means y_i is also algebraic over $\mathbb{Q}$.

In order to check that the extension is Galois, we must check that any homomorphism $\sigma : \mathbb{Q}(E[n]) \to \mathbb{C}$ satisfies $\sigma(\mathbb{Q}(E[n])) \subset \mathbb{Q}(E[n])$ (where we fix some initial embedding of $\mathbb{Q}(E[n])$ into $\mathbb{C}$). For any point $P = (x, y) \in E[n]$, define $\sigma(P) = (\sigma(x), \sigma(y))$ (and define $\sigma(\mathcal{O}) = \mathcal{O}$). Then we know that $\sigma(P)$ and P must have the same order for any point P on the elliptic curve, which means that each point in $E[n]$ is sent to another point in $E[n]$. This means σ permutes $P_1, \cdots, P_m$, and thus any element which is generated (as an algebra) by the x_is and y_is must stay in $\mathbb{Q}(E[n])$ under σ, as desired. □

We will see the return of objects like $\mathbb{Q}(E[n])$ in a later section.

3.2 Hilbert's twelfth problem

A way to restate the Kronecker–Weber theorem is as follows: we have a base field $\mathbb{Q}$, and there is an analytic function

$$f(x) = e^{\pi i x}$$

which generates finite abelian extensions of $\mathbb{Q}$. Indeed, a cyclotomic extension arises by adjoining an element of the form $e^{2\pi i/n}$ for some integer n, so the implication here is that any abelian extension can be contained within the "information" of the above analytic function f by plugging in elements x of the base field $\mathbb{Q}$. The goal is to show that we can do something similar when our base field is not just $\mathbb{Q}$, and Hilbert's twelfth problem asks whether it is possible for us to do just that:

Problem 12 (Hilbert's twelfth problem)**.** *Given a base number field K, is it possible to construct a meromorphic function f such that for any field extension L with finite abelian Galois group over K, we can pick special values $a_1, \cdots, a_n$ (corresponding to what are known as **singular moduli**) such that $K \subset L \subset K(f(a_1), \cdots, f(a_n), \{g_i\})$, where g_i include certain values of the Weierstrass p function, as well as roots of unity?*

The interpretation of Hilbert's twelfth problem and its connection to Kronecker–Weber has had a slightly complicated mathematical history: various statements were put forward, with various scholars attempting different versions of the problem. Hilbert referred to "elliptic functions" both in the sense of general elliptic functions and the specific modular function j, and in fact in Kronecker's original formulation of "Abelian equations" only dealt with the case where the Galois group is actually cyclic. In addition, Hilbert's original formulation did not include the $\{g_i\}$ in the problem statement above. A further mathematical and historical discussion can be founded at [3].

Today, this problem is still open in general, but the theory of complex multiplication allows us to understand the case of imaginary quadratic fields (that is, the fields $\mathbb{Q}[\sqrt{d}]$ with d a squarefree negative integer). And with the theory established above, we're ready to see a concrete example of this in play.

3.3 A more general example

Recall that the equation $y^2 = x^3 + x$ defines a CM elliptic curve (which we described above). We want to use this to study field extensions, much like we did with the cyclotomic polynomials over $\mathbb{Q}$.

Theorem 13. *Consider the elliptic curve $E : y^2 = x^3 + x$. Then the field*

$$K_n = \mathbb{Q}(i)(E[n])$$

is a Galois extension of $\mathbb{Q}(i)$ with ***(finite) abelian*** *Galois group.*

Proof sketch. K_n is indeed a Galois extension, because $\mathbb{Q}(E[n])$ is Galois over $\mathbb{Q}$ by our above work, and adjoining i to this still yields a Galois extension. (Since K_n is Galois over $\mathbb{Q}$, it is also Galois over $\mathbb{Q}(i)$.) Thus, it remains to prove that the Galois group $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ is abelian. This demonstrates why we wanted to consider $\mathbb{Q}(i)$ instead of $\mathbb{Q}$: fixing i in all of our automorphisms ensures that our complex multiplication ϕ commutes with our Galois elements, which is nice when we are trying to show commutativity.

The central idea is to represent our Galois elements σ_i as matrices in $GL_2(\mathbb{Z}/n\mathbb{Z})$: the matrix representation is injective, because knowing where two generators go tells us everything about the image of $E[n]$. We can also represent ϕ as a matrix in $GL_2(\mathbb{Z}/n\mathbb{Z})$.

But now ϕ is not a scalar multiple of the identity, and ϕ commutes with all elements σ_i. Thus the elements σ_i must actually commute with each other, and we've shown the desired result. □

And just like in the cyclotomic case for $\mathbb{Q}$, we have a stronger result about fields of abelian Galois group over $\mathbb{Q}(i)$, which we state without proof:

Theorem 14. *If L is a finite abelian field extension of $\mathbb{Q}(i)$, then L is contained in K_n for some n.*

To demonstrate that this is indeed using special values of a meromorphic function f as in Hilbert's twelfth problem, consider the generators of the n-torsion subgroup $E[n]$ in the complex torus, denoted $\frac{\omega_1}{n}$ and $\frac{\omega_2}{n}$. Then we know that K_n is generated by integer combinations of these generators, and in fact the explicit correspondence between the elliptic curve and complex torus means that we can explicitly write down the Galois extension

$$K_n = \mathbb{Q}(i)\left(\left\{\wp\left(\frac{c\omega_1 + d\omega_2}{n}\right), \wp'\left(\frac{c\omega_1 + d\omega_2}{n}\right) \quad \forall\, 0 \le c, d < n\right\}\right),$$

where $\wp$ is the Weierstrass function defined relative to the lattice (ω_1, ω_2). A more extensive discussion of these two theorems and their consequences can be found in section 6.5 of [4], but the main point is that the action of the Galois group on K_n can be described with matrix multiplication. This demonstrates that a specific symmetry in a CM elliptic curve can help understand some algebraic properties – specifically, the behavior of abelian extensions of $\mathbb{Q}(i)$ – which initially may seem completely disjoint from the complex multiplication itself.

4 The almost-integer $e^{\pi\sqrt{163}}$

As defined in Section 1.1 of [1], the ***j*-invariant** is the modular function

$$j(\tau) = \frac{1728 g_2^3}{g_2^3 - 27g_3^2},$$

where g_2 and g_3 are multiples of the standard Eisenstein series on the upper half-plane $\mathbb{H}$. This modular function can be connected to a lattice function, and this lattice function in turn connected to the lattice for an elliptic curve $\mathbb{C}/\Lambda$:

Definition 15. *The **j-invariant** for an elliptic curve $E : y^2 = x^3 + ax + b$ is defined to be*

$$j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2}.$$

This appears similar in form to the j-invariant we have already studied, and it is an important meromorphic function in studying questions that arise in a special case of the aforementioned Hilbert's twelfth problem. As we have already seen, two elliptic curves have the same j-invariant if and only if they are isomorphic, and an important isomorphism to consider in the upcoming arguments will be the multiplication by m for a CM point.

Definition 16. *The **endomorphism algebra over** $\mathbb{Q}$ for an elliptic curve is the tensor product $End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

We state the next result, which helps us characterize these endomorphism algebras, without proof:

Proposition 17. *For any elliptic curve E over a field (not necessarily $\mathbb{C}$), the endomorphism ring is a free $\mathbb{Z}$-module of rank 1, 2, or 4, corresponding to an endomorphism algebra of $\mathbb{Q}$, an imaginary quadratic field $\mathbb{Q}(\alpha)$, or an (imaginary) quaternion algebra $\mathbb{Q}(\alpha, \beta)$, respectively.*

Lectures 13 and 17 of [6] provide more details. Notably, for the elliptic curves over $\mathbb{C}$ that we have been considering, the last case is not possible, and when we have complex multiplication, the endomorphism ring is not a rank-one $\mathbb{Z}$-module (because the ring is strictly large than $\mathbb{Z}$). Therefore, we only have one case remaining, and we can further characterize that case:

Definition 18. *Let K be a ring containing $\mathbb{Q}$ which is a finite-dimensional $\mathbb{Q}$-vector space of dimension r. An **order** of K is a subring of K which is a free $\mathbb{Z}$-module of rank r.*

So for our CM elliptic curves, the endomorphism ring is an order in an imaginary quadratic field. The reason this is important is that we can describe such subrings algebraically:

Proposition 19. *Let K be a quadratic extension of $\mathbb{Q}$, and let $\mathcal{O}_K$ be its ring of integers. Then the orders of K are of the form $\mathbb{Z} + c\mathcal{O}_K$ for positive integers c.*

Proof. We know that every order is contained in a **maximal order**, and this maximal order turns out to be unique for finite field extensions of $\mathbb{Q}$: it is the ring of integers $\mathcal{O}_K$. Because this ring of integers always contains 1 and it is a two-dimensional lattice in K, we know that it is generated as a $\mathbb{Z}$-module by $(1, \tau)$.

First of all, we verify that the sets $\mathbb{Z} + c\mathcal{O}_K$ are indeed orders: they are lattices generated by 1 and $c\tau$, so we just need to verify that we have closure under multiplication. Indeed, if we take $a + ca'$ and $b + cb'$ in our order, where $a, b \in \mathbb{Z}$ and $a', b' \in \mathcal{O}_K$, we have

$$(a + ca')(b + cb') = ab + c(a'b + ab' + ca'b'),$$

and now $ab \in \mathbb{Z}$ and $a'b + ab' + ca'b' \in \mathcal{O}_K$ because of the ring structure of the ring of integers.

Now, we show that these sets are the only orders. By definition, an order of a quadratic field can be thought of as a lattice, and because the maximal order is $\mathcal{O}_K$, this lattice must be a sublattice of the one generated by 1 and τ, and in fact it contains the element 1 (because it is also a subring). Define c' to be the smallest positive integer such that $c'\tau$ is in the order. Then the order contains $1, c'$, and $c'\tau$, so it contains $\mathbb{Z} + c'\mathcal{O}_K$. Now any other element of the order $a + b\tau$ must have b a multiple of c' (or else we could use the division algorithm to contradict the minimality of c'). Thus, any such order is indeed of the form we want. □

If the endomorphism ring of E is an order $\mathcal{O}$ of an imaginary quadratic field, we say that E **has complex multiplication by $\mathcal{O}$**. And now to start working towards our result, we want to combine some of these objects we have just introduced.

Theorem 20. *If $z_0 \in \mathbb{H}$ is a CM point, then $j(z_0)$ is an algebraic number.*

Proof. We have established above that z_0 is an algebraic number of degree 2, so we can write $az_0^2 + bz_0 + c = 0$ for some $a, b, c \in \mathbb{Z}$ (with $a > 0$ and $\gcd(a, b, c) = 1$). This means that we can find a matrix M with nonzero determinant, which fixes z_0 under the usual action but is **not** an integer multiple of a matrix in $SL_2(\mathbb{Z})$. (Note that c is nonzero because z is not an integer.) For example, $M = \begin{bmatrix} b & c \\ -a & 0 \end{bmatrix}$ works when $ac \neq 1$, and $M = \begin{bmatrix} 1 & -2 \\ 2 & 2b+1 \end{bmatrix}$ works when $a = c = 1$ (this only has determinant 1 when $b = -2$, corresponding to $z_0 = 1$, which isn't a CM point). The purpose of choosing such an M is to ensure that the functions $j(z)$ and $j(Mz)$ are not identical.

Now note that the functions $j(z)$ and $j(Mz)$ are both modular functions with respect to the congruence subgroup $G = SL_2(\mathbb{Z}) \cap M^{-1}SL_2(\mathbb{Z})M$ – because j is weight 0, we just need to check that $j(M\gamma z) = j(Mz)$ for any $\gamma \in G$, which is true because j is modular. (Specifically, we can write any such γ as $M^{-1}AM$ for $A \in SL_2(\mathbb{Z})$, and then the identity reduces to $j(AMz) = j(Mz)$.) But now G has finite index in $SL_2(\mathbb{Z})$ because M has some finite integer determinant m, meaning $M^{-1}AM$ contains the subgroup $\Gamma(m)$. Thus, $j(Mz)$ and $j(z)$ must be algebraically dependent, meaning there is a polynomial $p(x, y)$ such that $p(j(Mz), j(z)) = 0$.

We wish to pick such a p with integer coefficients, and we claim that this polynomial can be chosen only based on the **determinant** of M. Indeed, let $\mathcal{M}_m$ be the set of matrices in

$GL_2(\mathbb{Z})$ with determinant m. Then there are finitely many $SL_2(\mathbb{Z})$ orbits of $\mathcal{M}_m$, since

$$\mathcal{M}_m^* = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in GL_2(\mathbb{Z}) : ad = m, 0 \le b < d \right\}$$

characterize the sublattices of a fixed lattice of index m, so each of these elements gives us one of the orbits. Thus, we can pick the polynomial that satisfies the identity

$$p(x, j(z)) = \prod_{M' \in SL_2(\mathbb{Z}) \backslash \mathcal{M}_m} (x - j(M'z)).$$

This function is well-defined because each $j(M'z)$ is constant on each of the (finitely many) orbits $SL_2(\mathbb{Z}) \backslash \mathcal{M}_m$. And notice that its x-coefficients are holomorphic, $SL_2(\mathbb{Z})$-invariant functions, so they must be polynomials in j, and thus this function p is indeed a polynomial in x and $j(z)$.

And now we can check that p has integer coefficients by writing it out as an explicit product over the representatives in $\mathcal{M}_m^*$:

$$p(x, j(z)) = \prod_{ad=m,\, d>0} \prod_{b=0}^{d-1} \left(x - j\left(\frac{az+b}{d} \right) \right),$$

and now we can expand out the Fourier series for j, noting that all of its coefficients c_n are integers: letting $q = e^{2\pi i z}$ and $\zeta_d = e^{2\pi i/d}$, this becomes

$$= \prod_{ad=m,\, d>0} \prod_{b=0}^{d-1} \left(x - \sum_{n=-1}^{\infty} c_n \zeta_d^{bn} q^{an/d} \right).$$

But this is invariant if we replace ζ_d with ζ_d^r for any r with $\gcd(r, d) = 1$, since we multiply over all b anyway. Thus the coefficients of the $q^{an/d}$ terms are integers. Furthermore, if we consider a fixed (a, d) and look at the inner product, all terms in the inner sum vanish except integer powers of q. This is because replacing z with $z + 1$ is the same as adding a to each value of b, resulting in the same product over all b, but then the coefficients must be 1-periodic and therefore have Fourier expansion only coming from integer powers of q. This means that each term of the inner product has x-coefficients in $\mathbb{Z}[q, 1/q]$.

Therefore, the full product $p(x, j(z))$ also has x-coefficients that are in $\mathbb{Z}[q, 1/q]$, and those coefficients are also polynomials in j. So now employing "long division," prioritizing the lower-degree q exponents instead of the higher-degree ones, shows that the joint $x, j(z)$-coefficients are indeed integers because the **"leading" coefficient $\frac{1}{q}$ is 1**. To finish, we view the polynomial p as a function of x and y again (instead of x and $j(z)$). Note that dividing $p(x, y)$ by any factors of $(x - y)$ that divide it yields a polynomial $q(x, y)$ such that $q(x, x)$ is a **nonconstant** polynomial. (Here is where the choice of M at the beginning of our argument matters.) And now we can plug in $x = j(z_0) = j(Mz_0)$ (because M fixes z) into our polynomial, and $q(j(z_0), j(z_0)) = 0$ gives us a nontrivial polynomial relation (with coefficients in $\mathbb{Z}$) for $j(z_0)$, as desired. □

It is in fact true that $j(z_0)$ is an algebraic integer, which we will establish shortly, though the proof then becomes more involved. Section 6.1 of [7] discusses this idea in more detail, and it also establishes a more systematic method of analyzing values of j at such CM points.

But we will need to be more precise to get the result that we want, and here is where we must cite some deeper results without proof. The first should look similar to the result we just proved:

Theorem 21. *For an order $\mathcal{O}$, let $Ell_{\mathcal{O}}$ denote the set of j-invariants of elliptic curves with CM by $\mathcal{O}$. Then the* ***Hilbert class polynomial****, defined via*

$$H(x) = \prod_{j(E)\in Ell_{\mathcal{O}}} (x - j(E)),$$

is a polynomial with integer coefficients.

We will also employ the use of a powerful correspondence:

Theorem 22 (First main theorem of complex multiplication)**.** *Let $\mathcal{O}$ be the maximal order in an imaginary quadratic field of discriminant D, and let L be the splitting field of $H(x)$ over $K = \mathbb{Q}(\sqrt{D})$. The Hilbert class polynomial $H(x)$ is irreducible and has degree equal to the size of the ideal class group, and there is an isomorphism between the ideal class group and the Galois group $Gal(L/K)$.*

The proofs and necessary background to understand these ideas, as well as further discussion of topics like the splitting of primes in imaginary quadratic fields and the action of the Galois group $\mathrm{Gal}(L/K)$, can be found in lectures 21 and 22 of [6] and chapter 6 of [7]. But the main point to notice is that when our ideal class group is of order 1, there is **only one lattice** up to scaling (because ideals of the ring $\mathcal{O}_K$ are sublattices). That means that there is only one possible value of $j(E)$ in the Hilbert class polynomial, and thus the polynomial just looks like $(x - j(E))$, meaning $j(E)$ is an integer.

Now, we are finally ready to tackle our central question for this section. The ring of integers of the quadratic number field $F = \mathbb{Q}\left[\sqrt{-163}\right]$ is a unique factorization domain, meaning that it has class number 1. To apply the above results, we will want to consider the maximal order of F, which is $\mathbb{Z} + \mathcal{O}_K$, and this lattice corresponds to the CM point

$$z_0 = \frac{1}{2}(1 + \sqrt{-163}).$$

This CM point yields an algebraic integer $j(z_0)$, and by the argument above, unique factorization tells us that $j(E) = j(z_0)$ is an integer. So we can try plugging in our value of z_0 into the j-invariant modular function: we introduce the constant

$$q = e^{2\pi i z_0} \approx -3.8 \times 10^{-18},$$

because we know the Laurent expansion for the j-invariant modular function looks like

$$j(q) = \frac{1}{q} + 744 + O(q).$$

Since q is very small (the q-coefficients don't grow too quickly, because we have a modular function), this tells us that we have the almost-integer

$$\frac{1}{q} \approx j(q) - 744 \in \mathbb{Z},$$

and substituting in the value of z_0 again reveals that this constant is

$$\frac{1}{q} = e^{-2\pi i z_0} = e^{\pi\sqrt{163}}.$$

Indeed, plugging this number into a calculator shows that it is within 7.5×10^{-13} of the nearest integer.

Acknowledgements

The author would like to thank Professor Ju-Lee Kim for advice and guidance throughout the paper-writing process, as well as Calvin Yost-Wolff for helpful comments and corrections.

References

[1] F. Diamond and J. Shurman. *A First Course in Modular Forms.* Graduate Texts in Mathematics. Springer New York, 2006.

[2] O. Neumann. Two proofs of the Kronecker-Weber theorem 'according to Kronecker, and Weber'. *Journal fur die reine und angewandte Mathematik*, 1981(323):105–126, 1981.

[3] N. Schappacher. On the history of Hilbert's twelfth problem: a comedy of errors. *Matériaux pour l'histoire des mathématiques au XX e siécle*, pages 243–273, 1996.

[4] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves.* Springer International Publishing, 2015.

[5] J. Sotáková. Elliptic curves and complex multiplication. `https://sites.google.com/site/sotakovajanahomepage/notes`, April 2016. Notes from number theory seminar in Prague.

[6] A. Sutherland. 18.783 Lectures – Elliptic Curves. `https://math.mit.edu/classes/18.783/2019/lectures.html`, 2019.

[7] D. Zagier. *Elliptic Modular Forms and Their Applications.* Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.