Modular forms and the Hilbert class field

Vladislav Vladilenov Petkov
VIGRE 2009, Department of Mathematics
University of Chicago

Abstract

The current article studies the relation between the $j-$invariant function of elliptic curves with complex multiplication and the *Maximal unramified abelian extensions* of imaginary quadratic fields related to these curves. In the second section we prove that the $j-$invariant is a modular form of weight 0 and takes algebraic values at special points in the upper halfplane related to the curves we study. In the third section we use this function to construct the *Hilbert class field* of an imaginary quadratic number field and we prove that the Galois group of that extension is isomorphic to the *Class group* of the base field, giving the particular isomorphism, which is closely related to the $j-$invariant. Finally we give an unexpected application of those results to construct a curious approximation of π.

1 Introduction

We say that an elliptic curve E has *complex multiplication* by an order O of a finite imaginary extension $K/\mathbb{Q}$, if there exists an isomorphism between O and the ring of endomorphisms of E, which we denote by $End(E)$. In such case E has other endomorphisms beside the ordinary "multiplication by n" - $[n]$, $n \in \mathbb{Z}$. Although the theory of modular functions, which we will define in the next section, is related to general elliptic curves over $\mathbb{C}$, throughout the current paper we will be interested solely in elliptic curves with complex multiplication. Further, if E is an elliptic curve over an imaginary field K we would usually assume that E has complex multiplication by the ring of integers in K.

Elliptic curves with complex multiplication are incredibly important in Number theory. In particular we will see how they allow us to connect the two very different concepts of *modular functions* and Galois extensions of imaginary number fields. We will be able to apply the results from analytic number theory to prove an important result in the Class field theory of imaginary quadratic fields, analogous to the famous Kronecker-Weber Theorem.

Finally we will give a peculiar implication of the results in the first two sections to provide a strange, but quite accurate approximation of π.

2 The values of the $j-$function at complex moduli are algebraic numbers

In this section we will consider the *$j-$invariant* of elliptic curves with complex multiplication and in particular consider its properties of a *modular form.* We will also prove that at some particular points, which we will call *complex moduli*, this function takes algebraic values. We would use this fact in the next section where we consider the algebraic extensions of particular imaginary quadratic fields by these algebraic values of the *$j-$invariant.* This would present a good example of the relation between the analytic and algebraic parts of Number theory.

We begin with some definitions.

Definition 1. *Let $\mathfrak{h}$ be the upper halfplane. A point $z \in \mathfrak{h}$ is called a* complex modulus *of discriminant D if it satisfies a quadratic equation with integer coefficients and negative discriminant $-D$. If $E = \mathbb{C}/\Lambda$ is an elliptic curve and $\Lambda = \{(n, mz)|n, m \in \mathbb{Z}\}$ we say that E corresponds to the* complex modulus z. *In particular E has complex multiplication by z.*

Definition 2. *Let $G = PSL_2(\mathbb{Z})$ be the quotient group of $SL_2(\mathbb{Z})$ after we identify $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. A modular function of weight $2k$ on $\mathfrak{h}$ is a meromorphic function f, such that $f(z) = (cz+d)^{(-2k)}f(Mz)$, for every $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.*

Holomorphic modular functions are called *modular forms.* A particular example is the *$j-$invariant* function.

Definition 3. *Let E be a non-singular elliptic curve with a Weierstrass form*

$$y^2 = 4x^3 - g_2x - g_3 \tag{1}$$

We define the j-invariant of E as

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

As we mentioned it is possible to consider j not only as a function on the space of elliptic curves, but also as a modular form. To do this we would need to extend our definition of g_2 and g_3.

Definition 4. *Let $k \in \mathbb{N}$. The* Eisenstein series *of weight $2k$ are defined as*

$$G_k(z) := \sum_{m,n} (mz+n)^{-2k}, \ \ (m,n) \neq (0,0) \tag{3}$$

These functions are modular forms of weight $2k$. We define $g_2 := 60G_2$ and $g_3 := 140G_3$. The need of the scalars is to avoid fractional coefficients in the Weierstrass form of an elliptic curve for which we substitute values in our modular functions. One can easily check that $\triangle = g_2^3 - 27g_3^2$ is a modular form of weight 12 and hence is not identically 0. Therefore, $j(z)$ is well defined by (2). Since g_2 is of weight 4 and g_3 is of weight 6 it follows that $j(z)$ is a modular function of weight 0. Note that if E corresponds to the complex modulus z then $j(E) = j(z)$, because if $E = \mathbb{C}/(1,z)$ then in its Weierstrass form (1) $g_2 = g_2(z)$ and $g_3 = g_3(z)$.

If E is an elliptic curve over a field K and σ is an automorphism of $\mathbb{C}$ that acts trivially on K, we would have from (2) the equality $j(E^\sigma) = j(E)^\sigma$. We would use this property in the next section. Nevertheless, $j(z)$ has several other important properties that we will shortly utilize.

Lemma 1. *Every modular form of weight 0 is a rational function in $j(z)$.*

Proof. [Serre].

□

We will need the following short notation.

Definition 5. *For $m \in \mathbb{N}$, denote $\sigma_1(m) = \sum_{d|m} d$.*

In order to prove that $j(z_0)$ is an algebraic number when z_0 is a complex modulus, we would construct a particular polynomial with a root $j(z_0)$. To do this we would first need the following more general result.

Theorem 1. *For every $m \in \mathbb{N}$ write $\mathbf{M_m}$ for the set of integer-entries matrices with determinant m. Then there exists a polynomial $\Phi(x,y) \in \mathbb{Z}[x,y]$, symmetric up to a sign in its two variables and of degree $\sigma_1(m) = \sum_{d|m} d$ in either, such that $\Phi(j(Mz), j(z)) = 0$ for every $M \in \mathbf{M_m}$.*

Proof. Let $G = PSL_2(\mathbb{Z})$. Note that the set of 2×2-matrices with integer entries $\mathbf{M_m^*} = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} |\mathbf{ad} = \mathbf{m}, \mathbf{0} \leq \mathbf{b} \leq \mathbf{d}\}$ is a full set of representatives for $G\backslash\mathbf{M_m}$. Hence $|\mathbf{M_m^*}| = \sigma_1(m)$.

Consider the following function

$$\Phi_m(x, j(z)) := \prod_{M \in \mathbf{M_m^*}} (x - j(Mz)), \tag{4}$$

where $x, z \in \mathbb{C}$ and $Im(z) > 0$. The function is well defined since $\mathbf{M_m^*}$ is a finite set and since $j(z)$ is $G-$invariant. By definition this function is a polynomial in x of degree $\sigma_1(m)$. Further, each coefficient of $\Phi_m(x)$ is a holomorphic $G-$invariant function of z. To continue the proof we would need the following result.

Lemma 2. *Every holomorphic $G-$invariant function defined on the upper halfplane with at most exponential growth at infinity is a polynomial function in $j(z)$.*

Proof. As we have shown, any modular form of weight 0, i.e. every holomorphic $G-$invariant function on the upper halfplane, is a rational function in $j(z)$. Since $j(z) = \sum_{n=-1}^{\infty} c_n q^n$ and $z \to \infty$ is equivalent to $q = e^{2\pi i z} \to 0$, any rational function in $j(z)$ with at most exponential growth at infinity must be in fact a polynomial. □

Using the result of Lemma 2 and the fact that $\Phi_m(x, j(z))$ has exponential growth at infinity, we get $\Phi_m(x, y) \in \mathbb{C}[x, y]$. To show that its coefficients are in $\mathbb{Z}$ we would use the Fourier expansion of $j(z)$ as a series in $q = e^{2\pi i z}$

$$j(z) = \sum_{n=-1}^{\infty} c_n q^n,$$

where $c_{-1} = 1$ and $c_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$. We have

$$\Phi_m(x, j(z)) = \prod_{ad=m} \prod_{b=0}^{d-1} (x - j(\frac{az+b}{d})) = \prod_{ad=m} \prod_{b=0}^{d-1} (x - \sum_{n=-1}^{\infty} c_n \zeta_d^n q^{an/d}), \quad (5)$$

where ζ_d is a d^{th} root of unity. Hence, $\Phi_m(x)$ is a polynomial with coefficients in the ring $\mathbb{Z}[q^{-1/d}, q^{1/d}][\zeta_d]$. Since Galois conjugation $\zeta_d \mapsto \zeta_d^k$ simply permutes the order of the terms in the inner product of the above expression, we can conclude that this product would have coefficients in $\mathbb{Z}$. Since $j(z+1) = j(z)$

$$\prod_{b=0}^{d-1} (x - \sum_{n=-1}^{\infty} c_n \zeta_d^n q^{an/d})$$

is invariant under $z \mapsto z + 1$. Therefore, the fractional powers of q in the expression disappear and $\Phi_m(x, j(z))$ belongs to $\mathbb{Z}[q^{-1}, q][x]$.

Finally the symmetry of $\Phi_m(x, y)$ (up to a sign) follows, since if $w = Mz$ for some matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{M_m}$, then $z = M'w$, where M' is the element $\begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \in \mathbf{M_m}$. □

We obtain the following corollary.

Corollary 1. *The values of $j(z)$ at complex moduli are algebraic numbers.*

Proof. Let z be the complex modulus corresponding to the elliptic curve E. By definition z satisfies some quadratic equation with integer coefficients and negative discriminant like $Az^2 + Bz + C = 0$, $AC > 0$. Then the 2×2-matrix $M = \begin{pmatrix} B & C \\ -A & 0 \end{pmatrix} \in \mathbf{M_{AC}}$ fixes z. Therefore, $\Phi_{AC}(j(z), j(z)) =$

$\Phi_{AC}(j(Mz), j(z)) = 0$ and $j(z)$ is an algebraic number of degree at most $\sigma_1(AC)$.

□

In the end of this section we take a step aside and look again at $j(z)$ as a function on the set of elliptic curves. If z_0 is a *complex modulus*, $K = \mathbb{Q}(z_0)$ is an imaginary quadratic extension of $\mathbb{Q}$ with ring of integers R_K and $E_0 = \mathbb{C}/R_K$, we saw that $j(E_0) = j(z_0)$. Hence by Corollary 1 the $j-$invariant of E_0 is an algebraic number. The following theorem shows that the same holds for all elliptic curves with complex multiplication by R_K.

Theorem 2. *Let E be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic number.*

Proof. Let $K = \mathbb{Q}(z_0)$ be an imaginary quadratic field, with ring of integers R_K, such that E has complex multiplication by R_K.

The statement of the theorem follows immediately from the fact that any elliptic curve has a Weierstrass form. Let $E = \mathbb{C}/\Lambda$ and let (ω_1, ω_2) generate Λ, i.e. $\Lambda = \{n\omega_1, m\omega_2 | n, m \in \mathbb{Z}\}$. Then $\tilde{E} = \mathbb{C}/\omega_1^{-1}\Lambda = \mathbb{C}/(1, z_1)$, where $z_1 = \omega_2/\omega_1$ is the elliptic curve isomorphic to E in Weierstrass form. Note that $\tilde{E}$ has complex multiplication by R_K since if for every $a \in R_K$ $a\Lambda \subset \Lambda$ it follows that $a\omega_1^{-1}\Lambda \subset \omega_1^{-1}\Lambda$.

Since $E_1 = \mathbb{C}/\Lambda_1$ is homeomorphic to $E_2 = \mathbb{C}/\Lambda_2$ if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}$ and j is holomorphic, $j(E)$ would be algebraic if $j(\tilde{E})$ is. As a result we simply need to show that z_1 is a *complex modulus.*

Since by definition $Im(\omega_2/\omega_1) > 0$ we know that $z_1 \in \mathfrak{h}$. Further, since $\tilde{E}$ has complex multiplication by $R_K = \mathbb{Z}(z_0)$ it follows that $z_0 = n + mz_1$ for some $n, m \in \mathbb{Z}$. Hence z_0 and z_1 are linearly related over $\mathbb{Z}$ and since z_0 is quadratic so must be z_1.

□

Therefore, j takes algebraic values at all elliptic curves with complex multiplication.

3 The Galois group of the Hilbert class field for imaginary quadratic fields

In this section we will consider a result, analogous to the following classic theorem.

Theorem 3. *(Kronecker - Weber) Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

This theorem helps to understand the Galois groups of abelian extensions of $\mathbb{Q}$. It is only a simple case of the large problem in Class field theory of understanding the Galois groups of *abelian* extensions of number fields, which is a step towards the understanding of the *Absolute Galois groups* of these fields.

We will discuss another interesting case - the *Maximal unramified abelian extension* of an imaginary quadratic field and discuss the relation between its Galois group and the j-invariant that we defined in the previous section. Henceforth, K will be an imaginary quadratic field with ring of integers R_K, unless we note otherwise.

Definition 6. *The* Class group *of K is defined as $\mathcal{CL}(R_K) = I(R_K)/P(R_K)$, where $I(R_K)$ is the set of non-zero fractional ideals of R_K and $P(R_K)$ is the set of principal ideals of R_K.*

A widely known fact is that the class group of a field is always finite. Its order is called the *class number* of the field.

Definition 7. *An extension of a field K is abelian, if it is Galois with an abelian Galois group. It is called unramified if no elements of K ramify in the extension. The* Hilbert class field *H/K is by definition the maximal unramified abelian extension of K.*

Now we have enough language to state the main theorem of this section.

Theorem 4. *Let H be the Hilbert class field of K. Let E be an elliptic curve with complex multiplication over R_K. Then we have $Gal(H/K) \cong \mathcal{CL}(R_K)$ and $H \cong K(j(E))$.*

Before we begin the proof of the main theorem we would need to define several important concepts. The first is the action of the class group $\mathcal{CL}(R_K)$ on the space of elliptic curves with complex multiplication by the ring R_K. To ease notation we will denote this space $\mathcal{ELL}(R_K)$.

Let $\mathfrak{a} \subset K \subset \mathbb{C}$ be a non-zero fractional ideal. Since K is a quadratic imaginary field $\mathfrak{a}$ must be a $\mathbb{Z}-$module of rank 2, which is not contained in $\mathbb{R}$. Therefore, $\mathfrak{a}$ is a lattice and hence there exist an elliptic curve $E_{\mathfrak{a}}$, such that

$$End(E_{\mathfrak{a}}) \cong \{\alpha \in \mathbb{C} | \alpha\mathfrak{a} \subset \mathfrak{a}\} = \{\alpha \in K | \alpha\mathfrak{a} \subset \mathfrak{a}\} = R_K$$

The last equality follows from the definition of a fractional ideal. Note for a given fractional ideal $\mathfrak{a}$ we would denote its class in $\mathcal{CL}(R_K)$ by $\bar{\mathfrak{a}}$.

Definition 8. *Let Λ be a lattice and $\mathfrak{a}$ be a fractional ideal. The product of $\mathfrak{a}$ and Λ as two lattices is defined as follows:*

$$\mathfrak{a}\Lambda := \{\sum_{i=1}^{r} \alpha_i \lambda_i | \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda, r \in \mathbb{N}\}.$$

Having defined the product of two lattices we can define the action of $\mathcal{CL}(R_K)$.

Definition 9. *The action of $\mathcal{CL}(R_K)$ on $\mathcal{ELL}(R_K)$ is defined as*

$$\bar{\mathfrak{a}} * E_{\Lambda} = E_{\mathfrak{a}^{-1}\Lambda} \tag{6}$$

To see that the action is correctly defined we need to prove the following two results.

Lemma 3. *$E_{\mathfrak{a}^{-1}\Lambda}$ is an elliptic curve with complex multiplication by R_K.*

Proof. W.l.g. we would prove the statement for $\mathfrak{a}$. Let α be any complex number. Then we have $\mathfrak{a}^{-1}\alpha\mathfrak{a} = \alpha R_K$. Since E_Λ has complex multiplication by R_K we have $R_K\Lambda = \Lambda$. Therefore,

$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \iff \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{a}\Lambda \iff \alpha\Lambda \subset \Lambda$$

Hence,

$$End(E_{\mathfrak{a}\Lambda}) = \{\alpha \in \mathbb{C} | \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} | \alpha\Lambda \subset \Lambda\} = End(E_\Lambda) = R_K.$$

□

Lemma 4. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two non-zero fractional ideals. Then, for a given E_Λ, $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$.*

Proof. We would use the following elementary fact about elliptic curves over $\mathbb{C}$: $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if there exists $c \in C^\times$, such that $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$. Hence,

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda.$$

Similarly we get:

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda.$$

If $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$, both $c\mathfrak{a}^{-1}\mathfrak{b}$ and $c^{-1}\mathfrak{a}\mathfrak{b}^{-1}$ must take Λ to itself and hence both must lie in R_K. However, since they are inverse to one another, they must both equal R_K. As a result $\mathfrak{a} = c\mathfrak{b}$ and therefore $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$.

□

The next concept we would need is the *Frobenius homomorphism.*

Definition 10. *Let $\bar{K}$ be the algebraic closure of K. Then the Frobenius homomorphism for K is defined as the homomorphism*

$$F : Gal(\bar{K}/K) \to \mathcal{CL}(R_K), \tag{7}$$

uniquely characterized by the condition

$$E^\sigma = F(\sigma) * E \tag{8}$$

for all $\sigma \in Gal(\bar{K}/K)$ and $E \in \mathcal{ELL}(R_K)$.

Of course we would need the following lemma.

Lemma 5. *F is a well defined homomorphism of groups.*

Proof. Let σ be any element of $Gal(\bar{K}/K)$ and let E be any elliptic curve in $\mathcal{ELL}(R_K)$. Then $End(E^\sigma) = End(E) = R_K$. The proof of this fact is not central for our work and may be found in [Silverman]. Hence for every σ there exists a unique $\bar{\mathfrak{a}} \in \mathcal{CL}(R_K)$ with $E^\sigma = \bar{\mathfrak{a}} * E$. Therefore, for a fixed E the above map (7) is well defined and determined by (8) for every $\sigma \in Gal(\bar{K}/K)$. The fact that the so defined F is a homomorphism for a fixed E follows, as

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

The last equality follows from the fact that for $K/\mathbb{Q}$ imaginary quadratic field $\mathcal{CL}(R_K)$ is an abelian group. It remains to show that F is independent of the choice of the elliptic curve E. To do this we would need the following fact, which proof is rather technical and may be found in [Silverman].

Lemma 6. *Let $E \in \mathcal{ELL}(R_K)$, $\sigma \in Gal(\bar{K}/K)$ and $\mathfrak{a} \in \mathcal{CL}(R_K)$. Then the following is true*

$$(\mathfrak{a} * E)^\sigma = \bar{\mathfrak{a}}^\sigma * E^\sigma \tag{9}$$

This equation might seem quite trivial at first sight, but in fact it gives us a relation between the action of the Absolute Galois group and that of the Class group. Assuming the above lemma let $E_1, E_2 \in \mathcal{ELL}(R_K)$ and let $\sigma \in Gal(\bar{K}/K)$. Write $E_1^\sigma = \bar{\mathfrak{a}}_1 * E_1$ and $E_2^\sigma = \bar{\mathfrak{a}}_2 * E_2$. We need to prove that $\bar{\mathfrak{a}}_1 = \bar{\mathfrak{a}}_2$. An easy observation that the action of $\mathcal{CL}(R_K)$ on $\mathcal{ELL}(R_K)$ is simply transitive ([Silverman]), allows us to find $\bar{\mathfrak{b}} \in \mathcal{CL}(R_K)$, such that $E_2 = \bar{\mathfrak{b}} * E_1$. Then

$$(\bar{\mathfrak{b}} * E_1)^\sigma = E_2^\sigma = \bar{\mathfrak{a}}_2 * E_2 = \bar{\mathfrak{a}}_2 * (\bar{\mathfrak{b}} * E_1) = (\bar{\mathfrak{a}}_2 \bar{\mathfrak{b}} \bar{\mathfrak{a}}_1^{-1}) * E_1^\sigma.$$

Note since $\bar{\mathfrak{b}} \subset K$ and $\sigma \in Gal(\bar{K}/K)$, $\bar{\mathfrak{b}}^\sigma = \bar{\mathfrak{b}}$. Hence using the result of Lemma 6 we may cancel $\bar{\mathfrak{b}}$ from both sides and obtain $E_1^\sigma = (\bar{\mathfrak{a}}_1^{-1}\bar{\mathfrak{a}}_2) * E_1^\sigma$. Therefore, $\bar{\mathfrak{a}}_1 = \bar{\mathfrak{a}}_2$ and F is independent of the choice of elliptic curve. □

The third concept that we will use is the *Artin map* and the related *conductor* of a field extension L/K. Let L be a finite unramified abelian extension of K and let R_L be the ring of integers in L. Let $\mathfrak{p}$ be a prime in K and $\mathfrak{P} \in L$ be a prime lying over $\mathfrak{p}$. Then $R_L/\mathfrak{P}$ and $R_K/\mathfrak{p}$ are finite fields and the first is a Galois extension of the later. We define the *decomposition group* of the element $\mathfrak{P}$ as $G(\mathfrak{P}) = \{\sigma \in Gal(L/K) | \mathfrak{P}^\sigma = \mathfrak{P}\}$. Then using restriction we get a map

$$G(\mathfrak{P}) \to Gal((R_L/\mathfrak{P})/(R_K/\mathfrak{p})). \tag{10}$$

This Galois group is cyclic and is generated by the usual *Frobenius automorphism* $x \mapsto x^{(R_K:\mathfrak{p})}$. Since $\mathfrak{p}$ is unramified this automorphism is uniquely extended to an element $\sigma_\mathfrak{P} \in G(\mathfrak{P})$. Changing $\mathfrak{P}$ would change $\sigma_\mathfrak{P}$ by conjugation, but since $Gal(L/K)$ is abelian $\sigma_\mathfrak{P}$ would be independent of the choice of $\mathfrak{P}$. Therefore, let us denote this *Frobenius element* $\sigma_\mathfrak{p}$. Formally this element is uniquely determined by the condition

$$\|\sigma_\mathfrak{p}(x) - x^{(R_K:\mathfrak{p})}\|_\mathfrak{p} < 1, \tag{11}$$

where $x \in L^\times$ and $\| \cdot \|_\mathfrak{p}$ is the normalized $\mathfrak{p}-$adic valuation. However, it is easier to think of the *Frobenius element* as determined from

$$\sigma_\mathfrak{p}(x) \equiv x^{(R_K:\mathfrak{p})} \mod \mathfrak{P}, \tag{12}$$

for $x \in R_L$.

Let $\mathfrak{c}$ be an integral ideal of K. By $I(\mathfrak{c})$ we would denote the group of fractional ideals of K that are relatively prime with $\mathfrak{c}$. (Note: the fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime if and only if $\mathfrak{a} + \mathfrak{b} = R_K$.)

Definition 11. *Let $\mathfrak{a} \in I(\mathfrak{c})$. Since R_K is a Dedekind domain we may write $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$. Then the **Artin Map** is defined as*

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

$$(\mathfrak{a}, L/K) = \left(\prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}, L/K \right) := \prod_\mathfrak{p} \sigma_\mathfrak{p}^{n_\mathfrak{p}}.$$

Let $P(\mathfrak{c})$ be the set of all principal ideal, which generator is congruent to 1 modulo $\mathfrak{c}$. Then the Artin map gives us the following result.

Lemma 7. *(Artin map reciprocity) Let L/K be a finite abelian extension. Define the Frobenius element as above for all unramified primes in K. Then there exists an integral ideal $\mathfrak{c} \in R_K$ such that all primes that ramify divide $\mathfrak{c}$ and $P(\mathfrak{c})$ lies in the kernel of the Artin map $(\cdot, L/K)$.*

Proof. [Silverman]. □

If $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are two ideals that satisfy the above lemma the same would hold for $\mathfrak{c}_1 + \mathfrak{c}_2$ as the Artin map is linear (a fact that follows easily form the definition). Therefore, there must exist a maximal ideal that satisfies the conditions of Lemma 7. We would call this ideal the *conductor* of L/K and denote it by $\mathfrak{c}_{L/K}$.

We would use the following important theorem from Class Field Theory about the Artin map and the conductor.

Theorem 5. *The Artin map $(\cdot, L/K) : I(\mathfrak{c}) \to Gal(L/K)$ is a surjective homomorphism. Further, $\ker(\cdot, L/K) \subset P(\mathfrak{c}_{L/K})$.*

We would also need a slightly modified version of Dirichlet's Theorem on primes in arithmetic progressions. For the proof of this theorem consult [Serre] and [Neukirch].

Theorem 6. *(Dirichlet) Let K be a number field and $\mathfrak{c}$ be an integral ideal of K. Then every ideal class in $I(\mathfrak{c})/P(\mathfrak{c})$ contains infinitely many degree 1 primes of K.*

Finally we would use the following lemma.

Lemma 8. *There exists a finite set $S \subset \mathbb{Z}$ of rational primes, such that if $p \notin S$ is a prime that splits in K, say as $pR_K = \mathfrak{p}\mathfrak{p}'$, then $F(\sigma_\mathfrak{p}) = \bar{\mathfrak{p}} \in \mathcal{CL}(R_K)$, where $\sigma_\mathfrak{p}$ is the* Frobenius element *corresponding to $\mathfrak{p}$ and F is the* Frobenius homomorphism*, which we have defined in Definition 10.*

Proof. [Silverman]. □

Having defined the *Artin map* and the other important concepts we now have the tools to prove the main result of this section (Theorem 4). We restate the theorem, slightly modifying it, in order to emphasize the connection with the modular function $j(z)$.

Theorem 7. *Let H be the Hilbert class field of K. Let E be an elliptic curve with complex multiplication over R_K. Then we have $Gal(H/K) \cong \mathcal{CL}(R_K)$ and $H \cong K(j(E))$. Further, for every non-zero fractional ideal $\mathfrak{a}$ of K we have*

$$j(E)^{(\mathfrak{a},H/K)} = j(\bar{\mathfrak{a}} * E). \tag{13}$$

Proof. Let L/K be the finite extension of K, such that L is the fixed field of the kernel of F - the Frobenius homomorphism in Definition 10. Recall that by $\bar{K}$ we denote the algebraic closure of K. Then we have,

$$Gal(\bar{K}/L) = \ker F = \{\sigma \in Gal(\bar{K}/K) | F(\sigma) = 1\},$$

since $\mathcal{CL}(R_K)$ acts simply transitively on $\mathcal{ELL}(R_K)$. Further, from the definition of F and the properties of $j(E)$ we obtain

$$\begin{aligned} Gal(\bar{K}/L) = \{\sigma \in Gal(\bar{K}/K) | E^\sigma = E\} &= \{\sigma \in Gal(\bar{K}/K) | j(E^\sigma) = j(E)\} \\ &= \{\sigma \in Gal(\bar{K}/K) | j(E)^\sigma = j(E)\} \\ &= Gal(\bar{K}/K(j(E))). \end{aligned}$$

It follows from basic Galois theory that $L = K(j(E))$. Further, since F maps $Gal(L/K)$ injectively into $\mathcal{CL}(R_K)$, (because $\ker F$ fixes L), and since $\mathcal{CL}(R_K)$ is an abelian group, L/K must be an abelian extension.

Fix $L = K(j(E))$ and let S be the finite set described in Lemma 8. Let $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$. Consider the composition of the *Artin map* and the *Frobenius homomorphism*

$$I(\mathfrak{c}_{L/K}) \xrightarrow{(\cdot,L/K)} Gal(L/K) \xrightarrow{F} \mathcal{CL}(R_K). \tag{14}$$

By Dirichlet's theorem (Theorem 6) there exists a degree one prime $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$, which is in the same ideal class as $\mathfrak{a}$ according to $P(\mathfrak{c}_{L/K})$ and does not lie over some prime in S. Then using Lemma 7 and Lemma 8 we obtain

$$F(\mathfrak{a}, L/K) = F(\mathfrak{p}, L/K) = \bar{\mathfrak{p}} = \bar{\mathfrak{a}}. \tag{15}$$

The above equality implies that for every $a \in K$, with (a) relatively prime with $\mathfrak{c}_{L/K}$, $F \circ ((a), L/K) = 1$. F is injective on $Gal(L/K)$ and hence $((a), L/K) = 1$.

But by definition the *conductor* $\mathfrak{c}_{L/K}$ is the smallest integral ideal $\mathfrak{c}$ with the property that

$$a \equiv 1 \mod \mathfrak{c} \Rightarrow ((a), L/K) = 1.$$

As a result $\mathfrak{c}_{L/K} = (1)$. Since every ramified prime must divide $\mathfrak{c}_{L/K}$ by definition we may conclude that L/K is an unramified extension. Therefore, L is contained by H, which is the maximal such extension. Yet the composition defined in (14) is surjective using Theorem 5 and $I(\mathfrak{c}_{L/K}) = I((1))$. Hence the Frobenius homomorphism $F : Gal(L/K) \to \mathcal{CL}(R_K)$ is an isomorphism. Note that the equality (15) gives the exact action of the *Artin map* on $j(E)$.

It remains to prove that $L = H$. However, since H is the maximal unramified abelian extension we have $\mathfrak{c}_{H/K} = (1)$ and

$$I(\mathfrak{c}_{H/K}) = I(R_K) = \{\text{all non-zero fractional ideals}\},$$

$$P(\mathfrak{c}_{H/K}) = P(R_K) = \{\text{all non-zero principal ideals}\}.$$

By Theorem 5 the *Artin map* is a surjective homomorphism and hence it defines an isomorphism from $I(\mathfrak{c}_{H/K})/\ker(\cdot, H/K)$ to $Gal(H/K)$. Using that by Lemma 7 $P(\mathfrak{c}_{H/K}) \subset ker(\cdot, H/K)$ and by Theorem 5 $\ker(\cdot, H/K) \subset P(\mathfrak{c}_{H/K})$ we see that the *Artin map* restricts to an isomorphism between the $\mathcal{CL}(R_K)$ and $Gal(H/K)$. Therefore, the order of $Gal(H/K)$ equals the class number h_K of K and hence equals also the order of $Gal(L/K)$. But $L \subset H$, hence $L = H$. □

4 Approximating π

As promised here we give a way to approximate π using the values of $j(z)$ at particular *quadratic* complex moduli. This approximation may be found in the lectures of Don Zagier on *Complex multiplication and Modular forms*, [Zagier]. As the author says this approximation is more interesting, because it uses hard results in an unexpected way, and is not very practical. In his own words: "It is more fun than serious."

Let $D = 163$. Then $K = \mathbb{Q}(-D)$ is an imaginary quadratic extension of $\mathbb{Q}$ of class number 1. In fact this is the smallest value of D for which K has such class number. We denote by $\mathfrak{z}_D$ the set of complex moduli of discriminant D and by $G\backslash\mathfrak{z}_D$ that set modulo $G = PSL_2(\mathbb{Z})$. Then the order of $G\backslash\mathfrak{z}_D$ equals the class number of K and hence we may choose a finite set of representatives of $G\backslash\mathfrak{z}_D$, say $\{z_{D,i} | 1 \leq i \leq h_K\}$. We define the *class polynomial* of K (or D) in a similar way to (4).

Definition 12. *(The Class Polynomial) The class polynomial of an imaginary quadratic field $K = \mathbb{Q}(-D)$ is defined as*

$$\Psi_D(x, j(z)) := \prod_{i=1}^{h_K} (x - j(z_{D,i})). \tag{16}$$

As Don Zagier proves ([Zagier], Proposition 25), the above polynomial is irreducible and of degree the class number h_K. Further, Ψ_D has integer coefficients. As a result the exact degree of the algebraic values of $j(z)$ at complex moduli would equal the *class number* of the underling field.

Therefore, in our case of $D = -163$, as $h_K = 1$, Ψ_D must be linear and hence the values of $j(z)$ should be a rational integer for $z \in \mathfrak{z}_D$. Moreover $j(z_{163})$ is very large, since $j(z) \approx q^{-1} = e^{-2\pi i z}$ and the value of q corresponding to z_{163} is of order 10^{-18}. However, from the series' expansion of $j(z) = q^{-1} + 744 + O(q)$ we get that q^{-1} must be a very good approximation of an integer. This in turn gives us the formula

$$e^{\pi\sqrt{163}} \approx 262537412640768743.999999999999$$

At the end of these calculations we find the desired approximation of π

$$\pi = \frac{1}{\sqrt{163}} \ln(262537412640768744) - O(10^{-31}).$$

Of course, this method of approximation of π is not practical since it would be much harder to evaluate $j(z_{163})$. More interesting is the fact that for z_{163} the inverse of the Fourier variable q is very close to an integer. This would obviously hold for all cases when $h_K = 1$. This in turn leads to the peculiar fact that there are only 9 values of D for which the last is true.

5 Conclusion

The results that we proved are a nice example where geometry, analytic and algebraic number theory come together. We see how geometric objects like elliptic curves could be used for the constructions of important field extensions, i.e. the *Hilbert class field.* Theorem 7 gives also the connection between the *Galois group* of this extension and the *Ideal class group* of the underling field. This is an important result since the later is usually much easier to be classified. We defined the action of the *Ideal class group* $\mathcal{CL}(R_K)$ on the space of elliptic curves $\mathcal{ELL}(R_K)$ and Theorem 7 provides its correspondence to the usual action of the Galois group, using the analytic properties of the $j-$function. Finally in the last section we saw that the relation between the algebraic concept of the *Ideal class group* and the geometry of elliptic curves goes even further. Having constructed the *Class polynomial* of an imaginary quadratic number field K, we saw that for an elliptic curve E with complex multiplication by the ring R_K the degree of the algebraic value of $j(z)$ at the complex modulus of E is equal to the *class number* of the ring R_K.

References

[Serre] Serre, J.-P.: *A Course in Arithmetic*, Springer-Verlag, New York,(1973).

[Silverman] Silverman, Joseph H.: *Advanced topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, (1994).

[Neukirch] Neukirch, J.: *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, (1999).

[Zagier] Bruinier, J. H., van der Geer, G., Harder, G., Zagier, D.: *The 1-2-3 of Modular Forms, Lectures at a Summer School in Nordfjordeid, Norway*, Springer, (2008).

[Evan] Jenkins, E.: *Complex Multiplication and Class Field Theory*, Discussed with professor Vladimir Drinfeld.

[Cornell] Cornell, G, Silverman, J. H., Stevens, G.: *Modular forms and Fermat's last theorem*, Springer-Verlag, New York, (1997).