The Only Imaginary Quadratic Fields With Class Number One Are...

by
Amy Rachel Goldlist
B.Sc.Hon. The University of King's College, 2003

AN ESSAY SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE

in

THE FACULTY OF GRADUATE STUDIES

Department of Mathematics
The University of British Columbia

April 2006

Contents

Acknowledgements

I would like to acknowledge the help and support of everybody I have worked with at UBC, especially my supervisor David Boyd for all of his help and support. Not any less important has been the help from Nike Vatsal regarding the class field theory, Mike Tsiang for his keen insight on all things mathematical and Ben Young for his help in LaTex. Also, I'd like to thank my parents and my brothers, Daniel and Michael Goldlist for listening to me talk about math, despite the fact that they really don't know what I'm talking about.

Last but not least, I send a special shout out to Erick Wong, for ensuring that this paper actually got written. Without him, you'd be reading 15 pages of point form notes, and nothing would converge.

1 Introduction

Some of the most interesting problems in number theory, nay, in mathematics involve the problem of factoring numbers in algebraic extensions of the integers. In some cases, such as the Gaussian integers, $\mathbb{Z}[i]$, we have unique factorization, mirroring factorization in the natural numbers. In other cases, such as $\mathbb{Z}[\sqrt{-5}]$, numbers can factor in more ways than one. In order to find out when unique factorization is possible, Kummer introduced the concept of *ideal numbers*, and from thisDedekind developed the concept of Ideals. It turns out that when we look at ideals, we can recapture the notion of unique factorization. In fact, if all ideals in our integer ring are equivalent - we are working in a Principal Ideal Domain - we have Unique Factorization with numbers, not just ideals. In other words, Unique Factorization follows from the class number being one.

Our challenge now lies in determining which number fields have class number one. In many ways, Imaginary Quadratic number fields are the simplest extensions of $\mathbb{Q}$. Many people worked on the class number one problem; determining exactly which quadratic number fields have class number one. It had been known that $\mathbb{Q}(\sqrt{d})$ where $d = -1, -2, -3, -7, -11, -19, -43, -67$ and -163 had class number one, and it was long conjectured that this was a complete list. The first proof of this fact was published in 1952 by Kurt Heegner [6], but his unfortunately proof was not accepted by the mathematical community. Heegner's method involves fairly basic mathematics, using modular functions to reduce the problem to finding solutions of a particular Diophantine Equation. Heegner leaned heavily on the work of mathematician H. Weber, particularly his 1908 book, *Lehrbuch der Algebra*. Unfortunately, Heegner failed to prove some of the claims in his paper, particularly when it came to showing that specific numbers lie in the Hilbert Class Field of $K = \mathbb{Q}(\sqrt{d})$.

Soon enough, the problem was solved separately using analytic methods by both Baker and Stark: Baker using Linear Forms in Logarithms, and Stark using L-functions. However, the elegant simplicity of Heegner's class field theoretic proof was irresistible, and in the late 1960s mathematicians began to look at it again. The supposed hole in Heegner's proof was then patched up by both Stark [11] and Deuring [5], both of them publishing elegant algebraic proofs. It is a version of these proofs which is presented here.

In order to build up our proof, we need to borrow from several areas of mathematics: Classical Algebraic Number Theory, Class Field Theory, Quadratic Forms, Complex Multiplication, Modular Functions and Forms, and finally Diophantine Equations.

2 Some Background Material

2.1 The Ideal Class Number

In order to find the Imaginary Quadratic fields with class number one, we first need to understand what the class number is.

Let K be an algebraic number field.

Definition 1. $\mathcal{O}$ is called an *order* of K if:

1. $\mathcal{O}$ is a subring of K containing 1;
2. $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module; and
3. $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

From the definition, one can easily show that an order consists of algebraic integers, that is elements whose minimal polynomial over $\mathbb{Z}$ is monic. In fact, the maximal order of K is the Ring of Integers, $\mathcal{O}_K := \{a \in K \mid \text{the minimal polynomial of } a \text{ is monic}\}$. That is, every order $\mathcal{O} \subset \mathcal{O}_K$.

We care mostly about $\mathcal{O}_K$, but in order to simplify our proofs, we will sometimes need to work with a general order in K. It is interesting to note that all of the theory of ideal classes can be generalized using any order.

In order to set up the class group, we introduce an equivalence relation on the ideals of $\mathcal{O}_K$. Two ideals $\mathfrak{a}$ and $\mathfrak{b} \subset \mathcal{O}_K$ are equivalent (denoted $\mathfrak{a} \sim \mathfrak{b}$) if there exists $a, b \in \mathcal{O}_K$ such that

$$a\mathfrak{a} = b\mathfrak{b}$$

The identity element in our group is $[(1)]$, the set of all principal ideals. When we are working with $\mathcal{O}_K$, we will by abuse of notations refer to ideals as being in K.

Definition 2. The Group formed by the equivalence classes of $\mathcal{O}_K$ is called the *Ideal Class Group*, I_K of K. The order of this group, that is the number of distinct Ideal classes in $\mathcal{O}_K$ is called the *Class Number* of $\mathcal{O}_K$ and is denoted $h(\mathcal{O}_K)$ or simply $h(K)$.

Remark 1. We note that our equivalence relation is independent of whether $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_K$, or in another order, $\mathcal{O}$. By restricting to ideals in a given order, $\mathcal{O}$, we can form an ideal class group over any order $\mathcal{O}$, with class number $h(\mathcal{O})$.

2.2 Imaginary Quadratic Fields

Let $d < 0$ be a square-free integer. Then $K = \mathbb{Q}(\sqrt{d})$ is called an *Imaginary Quadratic Number Field*. The discriminant of $\mathbb{Q}(\sqrt{d})$ is:

$$\Delta_d := \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{otherwise.} \end{cases}$$

When it is clear form the context what d is, we write Δ. Asking for d to be square-free ensures that each field is unique. We note that since $\mathbb{Q}(\sqrt{l^2 d}) = \mathbb{Q}(\sqrt{d})$, we need d to be square-free in order for the discriminant to be well defined.

The Ring of Integers, $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{d})$ is:

$$\mathcal{O}_K := \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{otherwise.} \end{cases}$$

Remark 2. By relaxing our restriction on d being square-free, that is letting $D = l^2\Delta$ for some l, we can find an order, $\mathcal{O}_l$, with discriminant $D = l^2\Delta$;

$$\mathcal{O}_l := \begin{cases} \mathbb{Z}[\frac{l+l\sqrt{d}}{2}] & \text{if } l^2 d \equiv 1 \pmod 4 \\ \mathbb{Z}[l\sqrt{d}] & \text{otherwise} \end{cases}$$

It can be shown that these are the only orders in a Imaginary Quadratic field.

Remark 3. An interesting fact, which we will exploit, is that any ideal in a number field can be viewed as being generated by at most two elements. That is, if $\mathfrak{a} \subset \mathcal{O}_K$, then $\mathfrak{a} = [\alpha, \beta]$ for some, $\alpha, \beta \in \mathcal{O}_K$, which are linearly independent over $\mathbb{Q}$. [2] This gives rise to a natural correspondence between an ideal $\mathfrak{a} = [\alpha, \beta] \subset K$ and a lattice in the Complex plane, $\Lambda = \alpha\mathbb{Z} \oplus \beta\mathbb{Z}$.

In fact, the lattices obtained in this way (and only this way) are special lattices known as *Complex Multiplication* or CM lattices; this leads us to our next topic.

2.2.1 Complex Multiplication

Definition 3. The *endomorphisms* $R(\Lambda)$ of a lattice are the complex numbers α such that $\alpha = 0$ or $\alpha\Lambda$ is a sublattice of Λ. These endomorphisms form a ring under the natural operations of Λ, $\alpha\beta\Lambda = \alpha(\beta\Lambda)$, $(\alpha + \beta)\Lambda = \alpha\Lambda + \beta\Lambda$. Thus, $R \supset \mathbb{Z}$. The same definition gives $R(c)$, the endomorphism ring of a class of lattices. We say that *complex multiplication* exists if this ring is strictly larger than $\mathbb{Z}$. [3]

The complex multiplications, the elements in R but not in $\mathbb{Z}$, are genuinely complex, that is nonreal. For any CM lattice Λ, R is an order of $K = \mathbb{Q}(\sqrt{d})$, for some $d < 0$. Any lattice with complex multiplication, then, is proportional to the lattice generated by $\mathcal{O}_K$, hence generated by an ideal in $\mathcal{O}_K$.

Using the natural correspondence between ideals and lattices, we can see that our ideal equivalence relationship is the same as the natural equivalence of their corresponding lattices. That is, $\mathfrak{a} \sim \mathfrak{b}$ if and only if the lattices they generate are equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$. We will return to this concept when we introduce the j-invariant, a natural way of classifying both lattices and ideals.

2.3 Ramification and the Hilbert Class Field

Let K be a number field, and L a Galois extension of K.

We are particularly interested in the case where L is an abelian extension of K, that is the Galois group $G = \mathrm{Gal}(L/K)$ is abelian.

We know that any ideal $\mathfrak{a} \subset \mathcal{O}_K$ factors uniquely into prime ideals, $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{p}_i \subset \mathcal{O}_K$. Any prime $\mathfrak{p} \subset \mathcal{O}_K$ divides a unique rational prime, p, that is $(p) \subset \mathfrak{p}$ or $\mathfrak{p} \mid p$ in $\mathcal{O}_K$.

However, when we take an extension of K, $\mathfrak{p}$ might not be prime in the extension L. Let $\mathfrak{p}$ be prime in $\mathcal{O}_K$. Then we can lift $\mathfrak{p}$ into L, by allowing $\mathfrak{p}\mathcal{O}_L$ to be called (by abuse of notation) simply $\mathfrak{p}$. Now we can decompose: $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$, where $\mathfrak{B}_i \subset \mathcal{O}_L$ are prime.

Diagrammatically we have:

$$\begin{array}{ccccc} L & \text{——} & \mathcal{O}_L & \supset & \mathfrak{B} \\ | & & | & & \\ K & \text{——} & \mathcal{O}_K & \supset & \mathfrak{p} \\ | & & | & & \\ \mathbb{Q} & \text{——} & \mathbb{Z} & \ni & p \end{array}$$

Where $\mathfrak{B} \mid \mathfrak{p} \mid p$, p in this context being the ideal generated by p in $\mathcal{O}_L$. We have the following tower of finite fields:

$$\mathbb{Z}/p\mathbb{Z} \subset \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_L/\mathfrak{B}\mathcal{O}_L$$

where each field is a finite field of characteristic p. The degrees of these extensions are important enough to give them a name:

Definition 4. 1. $[\mathcal{O}_L/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}] = f_i$ is called the *inertial degree of* $\mathfrak{p}$ *in* $\mathfrak{B}_i$.

2. e_i is called the *ramification index of* $\mathfrak{p}$ *in* $\mathfrak{B}_i$.

We now use a powerful theorem from Class Field theory:

Theorem 1. *If* $\mathfrak{p}$ *is prime in* K*, and* $\mathfrak{p} = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_g^{e_g}$ *in* $\mathcal{O}_L$*, then we have:*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

In addition, if L/K *is a Galois extension, then:*

1. $G = Gal(L/K)$ *acts transitively on primes dividing* $\mathfrak{p}$*, that is, if* $\mathfrak{B}_1, \mathfrak{B}_2 | \mathfrak{p}$ *then there exists* $\sigma \in G$ *such that* $\sigma(\mathfrak{B}_1) = \mathfrak{B}_2$.

2. *All* $\mathfrak{B}_i \subset L$ *containing* $\mathfrak{p}$ *have the same ramification index and inertial degree. Thus, we have:*

$$\mathfrak{p} = \mathfrak{B}_1^{e} \cdots \mathfrak{B}_g^{e}$$

where $[\mathcal{O}_L/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}] = f$ *and thus*

$$efg = [L : K].$$

For the proof of this theorem we refer to [9].

Definition 5. Let $\mathfrak{p} = \mathfrak{B}_1^{e} \cdots \mathfrak{B}_g^{e}$ decompose in L as above, then:

- If $e = 1$, we say $\mathfrak{p}$ is *unramified* in L;
- If $g = [L : K]$, and $e = f = 1$, we say that $\mathfrak{p}$ *splits completely* (or is completely split) in L;
- If $e > 1$, we say $\mathfrak{p}$ is *ramified* in L;
- If $e > 1$ and $f = 1$, then we say $\mathfrak{p}$ is *totally ramified* in L; and
- If $g = 1$ and $e = 1$, $\mathfrak{p}$ is *inert*.

We can show that there are only finitely many ramified primes in a given extension, by observing that a ramified prime must divide the discriminant.

One way to think of the ramification theory is to look at how rational primes act in $K = \mathbb{Q}(\sqrt{d})$. We note that since $[K : \mathbb{Q}] = 2$, we only have three options for rational primes:

- $g = 2$, $e = f = 1$: we know that p is the product of two distinct ideals, that is, p is split;
- $g = 1$, $e = 1$, $f = 2$: p is a prime ideal in K, so p is inert; or
- $g = 1$, $e = 2$, $f = 1$: p is the square of a prime ideal, and p is ramified.

Ramified primes are often referred to as 'bad' primes; we often try to avoid them.

The idea of class field theory, the so-called "dream of Kronecker's youth", is to concoct an extension L of K where primes in K behave in a suitable fashion. Our quest is for unique factorization, that is we need all of our ideals to be principal. If we can find an extension L where all ideals in K lift to principal ideals in L, tasks will be greatly simplified.

On the other hand, we note that many theorems will fail in the case where $\mathfrak{p}$ is ramified in L, so we think about finding an unramified extension. As well, things are easiest in Abelian extensions, so we might as well throw that onto our wishlist. Lastly, we would like to have some specific conditions which tell us when an (unramified) prime in K splits completely in L.

One of the miracles of class field theory is that such a field always exists. In fact, it is also unique, and thus deserves the grand name of the *Hilbert Class Field*.

Definition 6. The *Hilbert Class Field* of a number field K is the maximal (relatively) Abelian unramified extension L/K.

We now state without proof some interesting properties of the Hilbert Class Field, we refer the reader to [9]:

- For each K, L is unique.
- The Galois group $G = \mathrm{Gal}(L/K)$ is isomorphic to the ideal class group, I_K, and $[L : K] = h(K)$.
- Every ideal $\mathfrak{a} \subset K$ lifts to become principal in L. We note however that L may contain non-principal ideals as well.
- If $\mathfrak{p} \subset K$ is principal and unramified, it splits completely in L. This is the principalization property.
- There may exist intermediate fields $K \subset L' \subset L$ such that L' also has the principalization property.

- There are no nontrivial unramified relatively abelian extensions of K if $h(K) = 1$.

Remark 4. There are other class fields besides the Hilbert Class field. We can find these by restricting to an order $O \subset K$. In a quadratic imaginary field, we can build a class field which has the same properties, restricting to some O_l, with discriminant $l^2\Delta$. This class field has degree $h(O_l)$.

The last thing we will use about the Hilbert Class Field is some knowledge of its automorphisms, namely the Frobenius map. If $G = \mathrm{Gal}(L/K)$, then every $\sigma \in G$ is generated as the Frobenius automorphism of some $\mathfrak{B}$, that is for every $\alpha \in K$:

$$\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{B}}$$

We refer to σ as $(\frac{L/K}{\mathfrak{B}})$, which is called the *Artin Symbol*. If $\mathfrak{B}_1$ and $\mathfrak{B}_2$ both divide $\mathfrak{p}$, then their Frobenius automorphisms are conjugate. If G is abelian, then they are the same, and we write $\sigma = (\frac{L/K}{\mathfrak{p}})$.

2.4 Quadratic Forms

Quadratic forms turn out to be integral to the study of Quadratic Imaginary fields. We introduce an equivalence relation on quadratic forms, the show how this relates to the ideal class group, I_K.

Let $Q(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ be a quadratic form. We define the *discriminant* of Q to be:

$$D := b^2 - 4ac.$$

We say that two quadratic forms, Q and $\widetilde{Q}$ are equivalent if $Q(ax + b, cy + d) = \widetilde{Q}(x, y)$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, and we write $Q \sim \widetilde{Q}$. A calculation shows that under this unimodular transformation, the discriminant remains the same, therefore if $Q \sim \widetilde{Q}$, then Q and $\widetilde{Q}$ have the same discriminant. We call the number of equivalence classes of quadratic forms of discriminant D the form class number of D, denoted $h(D)$. It should be of no surprise to the reader that when $\mathbb{Z}[\sqrt{d}]$ is an order in an imaginary quadratic number field, then the form class number is actually equal to the ideal class number, and we call it just the class number.

Theorem 2. *The map $Q(x, y) = ax^2 + bxy + cy^2 \mapsto [a, \frac{b^2+\sqrt{d}}{2}]$ gives a bijection between the form class group and the ideal class group. This shows that the form class number $h(D)$ is equal to the ideal class number $h(K)$, where D is the*

discriminant of $Q(x, y)$ and the discriminant of the imaginary quadratic field, $K = \mathbb{Q}(\sqrt{d})$.

We note that the discriminant of $\mathcal{O}_K$ is equal to either d or $4d$.

Remark 5. Again, we use the order $\mathcal{O}_K$, but it should be noted that this proof extends to a general order, thus $h(l^2\Delta) = h(\mathcal{O}_l)$.

Proof. Let $f(x, y)$ and $g(x, y)$ be positive definite quadratic forms with discriminant D. By positive definite-ness, both f and g have no real roots, and thus have exactly one root lying in $\mathcal{H}$. Let $\tau, \tau' \in \mathcal{H}$ such that:

$$f(\tau, 1) = g(\tau', 1) = 0.$$

By the definition of equivalence under quadratic forms, $f \sim g$ if and only if $\tau' = \gamma\tau$, for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Now, since a is positive, $\tau = \frac{b^2+\sqrt{d}}{2a}$ (as this is in the upper half plane). Clearly, $\tau \in K$, and $a\tau \in \mathcal{O}_K$, as its minimal polynomial is monic. Consider the ideal:

$$\left[a, \frac{b^2 + \sqrt{d}}{2}\right] = [a, a\tau] = a[1, \tau] \subset \mathcal{O}_K$$

If $f \nsim g$, then as lattices $a[1, \tau] \nsim a'[1, \tau']$. Thus, we have shown that our map is injective.

Next, we show that the map is also surjective.

Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$. $\mathfrak{a}$ corresponds to a lattice, $\mathfrak{a} = [\alpha, \beta]$. By switching α and β as necessary, without loss of generality let $\tau = \frac{\beta}{\alpha} \in \mathcal{H}$. Let f be the minimal (positive definite) quadratic polynomial of τ. Then under our map $f \mapsto a[1, \tau]$, we have:

$$\mathfrak{a} = [\alpha, \beta] = \alpha\left[1, \frac{\beta}{\alpha}\right] = \alpha[1, \tau] \sim a[1, \tau]$$

from the definition of equivalence.

Thus the map is surjective, and hence a bijection. This proves that our two definitions of the class number are equal, that is $h(\mathcal{O}_K) = h(D)$ when D is the discriminant of $K = \mathbb{Q}(\sqrt{d})$. □

Remark 6. Gauss defined an operation, called composition, on the set of quadratic forms. Using composition, a group structure can be imposed on the set of equivalence classes of quadratic forms. In fact, we could make our theorem even stronger by looking at this group structure, and showing that as groups our two sets are isomorphic. However, as nice as this is, it is a little irrelevant to our purposes.

2.5 Modular Functions and the j-invariant

Definition 7. The *j-invariant* is defined on the upper half plane $\mathcal{H}$ as:

$$j(\tau) := \frac{1728 g_2^3(\tau)}{\Delta(\tau)}$$

where

$$\Delta(\tau) := g_2^3(\tau) - 27 g_3^2(\tau);$$

$$g_2(\tau) := 60 \sum_{\substack{c,d \in \mathbb{Z} \\ (c,d) \neq (0,0)}} \frac{1}{(c\tau + d)^4};$$

and

$$g_3(\tau) := 140 \sum_{\substack{c,d \in \mathbb{Z} \\ (c,d) \neq (0,0)}} \frac{1}{(c\tau + d)^6}.$$

The functions g_2 and g_3 are the weight four and six Eisenstein Series.

The j-invariant features heavily in the study of lattices in the Complex plane, and hence in the classification of ideals in Imaginary Quadratic number fields. It has the following important properties:

1. j is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, as fractional linear transformations, that is:
$$j(\gamma\tau) = j(\tau) \text{ for } \gamma \in \mathrm{SL}_2(\mathbb{Z})$$
where $\gamma\tau = \frac{a\tau+b}{c\tau+d}$ when $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
2. If $j(\tau) = j(\tau')$, then $\tau = \gamma\tau'$, for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$
3. j has a Fourier (or q) expansion, that is,
$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} a_n q^n$$
where traditionally we let $q = e^{2\pi i \tau}$.
4. j is analytic on the upper half plane, $\mathcal{H}$, with a simple pole at ∞.

j is an example of a more general class of functions called modular (or weakly modular) functions.

2.5.1 Congruence Subgroups

When working with modular functions, we will need the following important subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

Definition 8. Let

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a \equiv d \equiv 1, b \equiv c \equiv 0 \pmod{N} \right\}$$

be the *Principal Congruence Subgroup of Level N*.

Definition 9. A *Congruence Subgroup* is a subgroup, Γ, with $\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, for some N. The minimal N for which this is true is called the *level* of Γ.

The most important congruence subgroups for our purposes are

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}$$

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0, a \equiv d \equiv 1 \pmod{N} \right\}.$$

2.5.2 Modular Functions

Definition 10. For k a non-negative integer, the *weight k operator*, $[\gamma]_k$, is defined as:

$$f[\gamma]_k(\tau) = (c\tau + d)^{-k} f(\gamma\tau)$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Remark 7.

1. $[\gamma]_k$ has the following property: $[\gamma]_k[\gamma']_k = [\gamma\gamma']_k$ for any $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$.
2. For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, γ maps $\mathcal{H}$ onto $\mathcal{H}$, thus the action of $\mathrm{SL}_2(\mathbb{Z})$ is well defined on the upper half plane.

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of level N.

Definition 11. A *Modular Function of weight k for* Γ, $f(\tau)$, is a meromorphic function on the upper half plane, $\mathcal{H}$, such that:

1. $f[\gamma]_k(\tau) = f(\tau)$ for any $\gamma \in \Gamma$;
2. $f(\tau) = \sum_{n>M} a_n q_N^n$ where $q_N = e^{2\pi i\tau/N}$ and $M \in \mathbb{Z}$; in other words, f possesses a Fourier expansion with only finitely many negative terms; and
3. $f(\tau)$ is meromorphic at its cusps, that is, the Fourier expansion of $f[\gamma]_k(\tau)$ must have finitely many negative terms for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

We sometimes say that $f(\tau)$ is *weakly modular* (of weight k) for Γ. Often we will leave out the k and Γ, if it is clear from the context what they are.

From what we know about the j-invariant, we can now say that j is a modular function of weight 0 for $\mathrm{SL}_2(\mathbb{Z})$.

Fact 1. Any function f which is weakly modular for $\Gamma_0(N)$ of weight 0, which has rational coefficients in its q-expansion is rational in $j(\tau)$ and $j(N\tau)$, so $f(\tau) \in \mathbb{Q}(j(\tau), j(N\tau))$. [2]

Definition 12.
1. We say f is a *modular form* (of weight k for Γ) if:
   (a) f is weakly modular for Γ; and
   (b) f is holomorphic at its cusps (so the q-expansion of $f[\gamma]_k(\tau)$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ has no negative terms).

   We denote the space of modular forms by $M_k(\Gamma)$.
2. We say f is a *cusp form* (of weight k for Γ) if:
   (a) $f \in M_k(\Gamma)$; and
   (b) f vanishes at 0, so the coefficient $a_0 = 0$ in the q-expansion.

   We denote the space of cusp forms by $S_k(\Gamma)$.

2.6 The Dedekind η-Function

Most of the modular functions which we will be looking at are related to an important function called the *Dedekind η-function*, $\eta(\tau)$. We recall that $q = e^{2\pi i\tau}$.

Definition 13. The Dedekind-η function, (or η-product) is:

$$\eta(\tau) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

η is not itself a modular function; however it satisfies the following transformation properties.

Theorem 3. *Let $\sqrt{\tau}$ denote the principal branch of the square root. Then:*

1. $\eta(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}}\eta(\tau)$*; and*
2. $\eta(\tau + 1) = e^{2\pi i/24}\eta(\tau)$.

In order to prove these transformation properties, we need the weight two Eisenstein series, E_2.

Definition 14. The normalized weight two Eisenstein series is:

$$\begin{aligned} E_2(\tau) &:= \frac{3}{\pi^2} \sum_{c \in \mathbb{Z}} \sum_{\substack{d \in \mathbb{Z} \\ (c,d) \neq (0,0)}} \frac{1}{(c\tau + d)^2} \\ &= 1 - 24 \sum_{n=1}^{\infty} \sigma(n) q^n, \end{aligned}$$

where $\sigma(n) := \sum_{d|n} d$ is the divisor sum.

We need to justify that our two definitions are actually equal. Note that the first sum defining E_2 is not absolutely convergent, and thus we are interpreting the sum as the limit of a symmetric sum over $|c| \leq N$ as $N \to \infty$. Note:

$$
\begin{aligned}
E_2(\tau) &= \frac{3}{\pi^2} \sum_{c\in\mathbb{Z}} \sum_{\substack{d\in\mathbb{Z} \\ (c,d)\neq(0,0)}} \frac{1}{(c\tau+d)^2} \\
&= \frac{3}{\pi^2}\left[\sum_{d\neq 0} \frac{1}{d^2} + \sum_{c\neq 0}\sum_{d\in\mathbb{Z}} \frac{1}{(c\tau+d)^2}\right] \\
&= 1 + \frac{6}{\pi^2}\sum_{c=1}^{\infty}\left(\sum_{d\in\mathbb{Z}} \frac{1}{(c\tau+d)^2}\right) \\
&= 1 + \frac{6}{\pi^2}\sum_{c=1}^{\infty}(-2\pi i)^2 \sum_{m=1}^{\infty} m q^{cm} \\
&= 1 - 24\sum_{n=1}^{\infty}\sigma(n)q^n,
\end{aligned}
$$

recalling that:

$$
\frac{1}{\tau} + \sum_{d\neq 0}\frac{1}{\tau+d} = \pi\cot(\pi\tau) = \pi i - 2\pi i\sum_{m=0}^{\infty} q^m \tag{1}
$$

(see [4]), and differentiating equation 1 with respect to τ.

Lemma 1.

$$
\tau^{-2}E_2(-1/\tau) = E_2(\tau) + \frac{12}{2\pi i\tau}.
$$

Remark 8. In fact, E_2 obeys the following transformation, for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$:

$$
E_2[\gamma]_2(\tau) = E_2(\tau) - \frac{6ic}{\pi(c\tau+d)}.
$$

Proof.

$$\begin{aligned}
E_2\left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right]_2(\tau) &= \tau^{-2}E_2(-1/\tau) \\
&= \frac{3}{\pi^2}\sum_{c\in\mathbb{Z}}\sum_{\substack{d\in\mathbb{Z}\\(c,d)\neq(0,0)}}\frac{1}{\tau^2(\frac{-c}{\tau}+d)^2} \\
&= \frac{3}{\pi^2}\sum_{d\in\mathbb{Z}}\sum_{\substack{c\in\mathbb{Z}\\(c,d)\neq(0,0)}}\frac{-1}{(c\tau+d)^2} \\
&= \frac{3}{\pi^2}\sum_{d\in\mathbb{Z}}\sum_{\substack{c\in\mathbb{Z}\\(c,d)\neq(0,0)}}\frac{1}{(c\tau+d)^2} \\
&= \frac{3}{\pi^2}\left(2\sum_{d=1}^{\infty}\frac{1}{d^2}+\sum_{d\in\mathbb{Z}}\sum_{c\neq 0}\frac{1}{(c\tau+d)^2}\right) \\
&= 1+\frac{3}{\pi^2}\sum_{d\in\mathbb{Z}}\sum_{c\neq 0}\frac{1}{(c\tau+d)^2}.
\end{aligned}$$

Now, for any $c \neq 0$,

$$\sum_{d\in\mathbb{Z}}\left(\frac{1}{c\tau+d}-\frac{1}{c\tau+d+1}\right)=0$$

by telescoping sums. Therefore:

$$\begin{aligned}
E_2(\tau) &= 1+\frac{3}{\pi^2}\sum_{c\neq 0}\sum_{d\in\mathbb{Z}}\frac{1}{(c\tau+d)^2}-\frac{3}{\pi^2}\sum_{c\neq 0}\sum_{d\in\mathbb{Z}}\frac{1}{(c\tau+d)(c\tau+d+1)} \\
&= 1+\frac{3}{\pi^2}\sum_{c\neq 0}\sum_{d\in\mathbb{Z}}\left(\frac{c\tau+d+1-c\tau-d}{(c\tau+d)^2(c\tau+d+1)}\right) \\
&= 1+\frac{3}{\pi^2}\sum_{c\neq 0}\sum_{d\in\mathbb{Z}}\left(\frac{1}{(c\tau+d)^2(c\tau+d+1)}\right).
\end{aligned}$$

Noting that this double sum converges absolutely, we can switch the order of summation.

$$
\begin{aligned}
E_2(\tau) &= 1 + \frac{3}{\pi^2}\sum_{d\in\mathbb{Z}}\sum_{c\neq 0}\left(\frac{1}{(c\tau+d)^2} - \frac{1}{(c\tau+d)(c\tau+d+1)}\right) \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\sum_{d\in\mathbb{Z}}\sum_{c\neq 0}\frac{1}{(c\tau+d)(c\tau+d+1)} \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\lim_{N\to\infty}\sum_{d=-N}^{N-1}\sum_{c\neq 0}\left(\frac{1}{c\tau+d} - \frac{1}{c\tau+d+1}\right) \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\lim_{N\to\infty}\sum_{c\neq 0}\sum_{d=-N}^{N-1}\left(\frac{1}{c\tau+d} - \frac{1}{c\tau+d+1}\right) \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\lim_{N\to\infty}\sum_{c\neq 0}\left(\frac{1}{c\tau-N} - \frac{1}{c\tau+N}\right) \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\lim_{N\to\infty}\frac{1}{\tau}\sum_{c\neq 0}\left(\frac{1}{c-\frac{N}{\tau}} - \frac{1}{c+\frac{N}{\tau}}\right) \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\lim_{N\to\infty}\frac{1}{\tau}\sum_{c=1}^{\infty}\left[\left(\frac{1}{-c-\frac{N}{\tau}} - \frac{1}{-c+\frac{N}{\tau}}\right) + \left(\frac{1}{c-\frac{N}{\tau}} - \frac{1}{c+\frac{N}{\tau}}\right)\right] \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\lim_{N\to\infty}\frac{1}{\tau}\left[\left(\pi\cot\left(\frac{-\pi N}{\tau}\right) + \frac{\tau}{N}\right) - \left(\pi\cot\left(\pi\frac{N}{\tau}\right) - \frac{\tau}{N}\right)\right] \\
&= \tau^{-2}E_2(-1/\tau) + \frac{3}{\pi^2}\lim_{N\to\infty}\frac{2}{\tau}\left(\pi\cot\left(\frac{-\pi N}{\tau}\right) + \frac{\tau}{N}\right) \\
&= \tau^{-2}E_2(-1/\tau) - \frac{12}{2\pi i\tau}
\end{aligned}
$$

Note that $\Im(-\pi i/\tau) \to \infty$ as $N \to \infty$, so $\cot(-\pi i/\tau) \to \pi i - 2\pi i$ by (1).

□

Proof. (*of Theorem 3*) First we will take the logarithmic derivative of each side.

$$\begin{aligned}
\frac{d}{d\tau}\left[\log\left(\eta\left(\tau\right)\right)\right] &= \frac{d}{d\tau}\left(\frac{2\pi i\tau}{24} + \sum_{n=1}^{\infty}\log(1-e^{2\pi in\tau})\right) \\
&= \frac{2\pi i}{24} - \sum_{n=1}^{\infty}\left(\frac{2\pi in}{1-e^{2\pi in\tau}}\right) \\
&= \frac{2\pi i}{24}\left(1 - 24\sum_{n=1}^{\infty}\left(\frac{n}{1-q^n}\right)\right) \\
&= \frac{2\pi i}{24}\left(1 - 24\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}nq^{kn}\right) \\
&= \frac{2\pi i}{24}\left(1 - 24\sum_{n=1}^{\infty}\left(\sum_{d|n}d\right)q^n\right) \\
&= \frac{2\pi i}{24}\left(1 - 24\sum_{n=1}^{\infty}\sigma(n)q^n\right) \\
&= \frac{2\pi i}{24}E_2(\tau)
\end{aligned}$$

Thus:

$$\frac{d}{d\tau}\left[\log\left(\sqrt{\frac{\tau}{i}}\eta\left(\tau\right)\right)\right] = \frac{1}{2\tau} + \frac{2\pi i}{24}E_2(\tau)$$

and

$$\frac{d}{d\tau}\left[\log\left(\eta\left(-1/\tau\right)\right)\right] = \frac{2\pi i}{24}\tau^{-2}E_2\left(\frac{-1}{\tau}\right)$$

By lemma 1, the two sides differ only by a multiplicative constant, which must be 1 (by setting $\tau = i$).

Secondly, we note that:

$$\begin{aligned}
\eta(\tau+1) &= e^{(2\pi i\tau)/24+(2\pi i)/24}\prod_{n=1}^{\infty}(1-e^{2\pi i\tau n+2\pi in}) \\
&= e^{(2\pi i)/24}q^{1/24}\prod_{n=1}^{\infty}(1-1\cdot q^n) \\
&= e^{(2\pi i)/24}\eta(\tau).
\end{aligned}$$

□

From this we note that $\eta^{24}(\tau+1) = \eta^{24}(\tau)$, and $\tau^{-12}\eta^{24}(-1/\tau) = \eta^{24}(\tau)$. Since $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ corresponding to these two transformations, we see that η^{24} is a modular from of weight 12. In fact, as the first Fourier coefficient is 0, we see that η^{24} is a cusp form of weight 12, checking, of course, that we have holomorphy at the only cusp, ∞.

Fact 2. $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$.

This follows from the fact that η^{24} and Δ are cusp forms of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$, and this is a one dimensional space. See [8] for details.

2.7 γ_2 and the Weber Functions

Let

$$\gamma_2(\tau) = (j(\tau))^{1/3} = \frac{3g_2(\tau)}{4\pi^4\eta(\tau)^8}$$

where the cube root is taken to be real when τ is on the positive imaginary axis.

Theorem 4. *$\gamma_2(3\tau)$ is weakly modular for $\Gamma_0(9)$.*

Proof. We begin by noting that since

$$j(\tau) = q^{-1}\left(1 + \sum_{n=1}^{\infty} a_n q^n\right)$$

where $a_n \in \mathbb{Q}$ so:

$$\gamma_2(\tau) = q^{-1/3}\left(1 + \sum_{n=1}^{\infty} b_n q^n\right).$$

Since the a_n are rational, so are the b_n, and thus:

$$\gamma_2(-1/\tau) = \gamma_2(\tau)$$
$$\gamma_2(\tau+1) = \zeta_3^2\gamma_2(\tau)$$

where $\zeta_3 = e^{2\pi i/3}$.

Modularity follows via observing that $\gamma_2(3\tau)$ has a q-expansion in powers of $q^{1/9}$, which gives us the required meromorphy at the cusps. This tells us that $\gamma_2(3\tau) \in \mathbb{Q}(j(\tau), j(9\tau))$. For details, see [2]. □

The Weber functions are:

$$\mathfrak{f}(\tau) := e^{\frac{-\pi i}{24}} \frac{\eta((\tau+1)/2)}{\eta(\tau)} = q^{-1/48} \prod_{n=1}^{\infty} (1 + q^{n-1/2})$$

$$\mathfrak{f}_1(\tau) := \frac{\eta(\tau/2)}{\eta(\tau)} = q^{-1/48} \prod_{n=1}^{\infty} (1 - q^{n-1/2})$$

$$\mathfrak{f}_2(\tau) := \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2} q^{1/24} \prod_{n=1}^{\infty} (1 + q^n).$$

Proof. (of q-expansions) We begin by expanding out $\mathfrak{f}_2(\tau)$:

$$\begin{aligned}
\mathfrak{f}_2(\tau) &= \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} \\
&= \sqrt{2} e^{4\pi i\tau/24 - 2\pi i\tau/24} \prod_{n=1}^{\infty} \frac{(1-q^{2n})}{(1-q^n)} \\
&= \sqrt{2} q^{1/24} \prod_{n=1}^{\infty} (1+q^n)
\end{aligned}$$

Next, we note that:

$$\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \frac{\eta(\tau)}{\eta(2\tau)} \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2}.$$

Noting that we have absolute convergence:

$$\begin{aligned}
\mathfrak{f}_1(\tau) &= \frac{\sqrt{2}}{\mathfrak{f}_2(\tau/2)} \\
&= q^{-1/48} \prod_{n=1}^{\infty} (1 + q^{n/2})^{-1} \\
&= q^{-1/48} \prod_{n=1}^{\infty} \frac{(1-q^{n/2})}{(1-q^n)} \\
&= q^{-1/48} \prod_{n=1}^{\infty} \frac{(1-q^n)}{(1-q^n)} (1 - q^{n-\frac{1}{2}}) \\
&= q^{-1/48} \prod_{n=1}^{\infty} (1 - q^{n-1/2})
\end{aligned}$$

Finally, we let $z = \tau + 1$. Since $\eta(z-1) = e^{-2\pi i/24}\eta(z)$, we have:

$$\begin{aligned}
\mathfrak{f}(z) &= e^{-2\pi i/48}\frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} \\
&= e^{-2\pi i/48}\frac{\eta(z/2)}{\eta(z-1)} \\
&= e^{-2\pi i/48}e^{2\pi i/24}\frac{\eta(z/2)}{\eta(z)} \\
&= e^{2\pi i/48}\mathfrak{f}_1(z) \\
&= e^{2\pi i/48}\mathfrak{f}_1(\tau+1) \\
&= e^{2\pi i/48}q^{-1/48}e^{-2\pi i/48}\prod_{n=1}^{\infty}(1-q^n e^{2\pi i n}e^{-\pi i}) \\
&= q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2})
\end{aligned}$$

As desired. □

We then have the following important relationship:

Claim 1.

$$\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$$

Proof.

$$\begin{aligned}
\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) &= \sqrt{2}q^{-1/48-1/48+1/24}\prod_{n=1}^{\infty}(1+q^{n-1/2})(1-q^{n-1/2})(1+q^n) \\
&= \sqrt{2}\prod_{n=0}^{\infty}(1-q^{2n-1})\frac{(1-q^{2n})}{(1-q^n)} \\
&= \sqrt{2}\prod_{n\text{ odd}}(1-q^n)\prod_{n\text{ even}}(1-q^n)\prod_{n=1}^{\infty}(1-q^n)^{-1} \\
&= \sqrt{2}
\end{aligned}$$

□

Claim 2. The Weber functions have the following transformation properties:

$$\begin{aligned}
\mathfrak{f}(\tau+1) &= e^{-2\pi i/48}\mathfrak{f}_1(\tau)\\
\mathfrak{f}_1(\tau+1) &= e^{-2\pi i/48}\mathfrak{f}(\tau)\\
\mathfrak{f}_2(\tau+1) &= e^{2\pi i/24}\mathfrak{f}_2(\tau)\\
\mathfrak{f}(-1/\tau) &= \mathfrak{f}(\tau)\\
\mathfrak{f}_1(-1/\tau) &= \mathfrak{f}_2(\tau)\\
\mathfrak{f}_2(-1/\tau) &= \mathfrak{f}_1(\tau)
\end{aligned}$$

Proof. We saw earlier that:

$$\mathfrak{f}_1(\tau+1) = e^{-2\pi i/48}\mathfrak{f}(\tau)$$

Similarly:

$$\begin{aligned}
\mathfrak{f}(\tau+1) &= e^{-2\pi i/48}\prod_{n=1}^{\infty}(1+q^n e^{2\pi i n-\pi i})\\
&= e^{-2\pi i/48}\prod_{n=1}^{\infty}(1-q^n)\\
&= e^{-2\pi i/48}\mathfrak{f}_1(\tau)
\end{aligned}$$

and:

$$\begin{aligned}
\mathfrak{f}_2(\tau+1) &= e^{2\pi i/24}\sqrt{2}q^{1/24}\prod_{n=1}^{\infty}(1+q^n e^{2\pi i})\\
&= e^{2\pi i/24}\mathfrak{f}_2(\tau)
\end{aligned}$$

Next, we use the transformation properties of η.

$$\begin{aligned}
\mathfrak{f}_1\left(\frac{-1}{\tau}\right) &= \frac{\eta(\frac{-1}{2\tau})}{\eta(-1/\tau)}\\
&= \sqrt{\frac{2\tau}{i}}\sqrt{\frac{i}{\tau}}\frac{\eta(2\tau)}{\eta(\tau)}\\
&= \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}\\
&= \mathfrak{f}_2(\tau),
\end{aligned}$$

which also implies $\mathfrak{f}_2(-1/\tau) = \mathfrak{f}_1(\tau)$, and

$$\begin{aligned}\mathfrak{f}\left(\frac{-1}{\tau}\right) &= \frac{\sqrt{2}}{\mathfrak{f}_1(-1/\tau)\mathfrak{f}_2(-1/\tau)} \\ &= \frac{\sqrt{2}}{\mathfrak{f}_2(\tau)\mathfrak{f}_1(\tau)} \\ &= \mathfrak{f}(\tau)\end{aligned}$$

□

We need a few more facts about the Weber functions. First we note that from the above transformation properties, $\mathfrak{f}(8\tau)^6$ is weakly modular for $\Gamma_0(64)$. Also, from the q-product expansion of $\mathfrak{f}$, we can see that the q-series has rational coefficients. From this we note that $\mathfrak{f}(8\tau)^6 \in \mathbb{Q}(j(\tau), j(64\tau))$.

Theorem 5.

$$\gamma_2(\tau) = \frac{\mathfrak{f}(\tau)^{24} - 16}{\mathfrak{f}(\tau)^8} = \frac{\mathfrak{f}_1(\tau)^{24} + 16}{\mathfrak{f}_1(\tau)^8} = \frac{\mathfrak{f}_2(\tau)^{24} + 16}{\mathfrak{f}_2(\tau)^8}$$

Proof. Let e_1, e_2, e_3 be the points of order two of the Weierstrass $\wp$-function, that is the roots of the following cubic:

$$4X^3 - g_2(\tau)X - g_3(\tau)X$$

So:

- $e_1 = \wp(\tau/2)$
- $e_2 = \wp(1/2)$
- $e_3 = \wp((\tau + 1)/2)$

For more information on the derivation of these properties, see [2]. We use the following relationship between these numbers and η:

$$\begin{aligned}e_2 - e_1 &= \pi^2\eta(\tau)^4\mathfrak{f}(\tau)^8 \\ e_2 - e_3 &= \pi^2\eta(\tau)^4\mathfrak{f}_1(\tau)^8 \\ e_3 - e_1 &= \pi^2\eta(\tau)^4\mathfrak{f}_2(\tau)^8\end{aligned}$$

See [2] p. 257. This follows from the expansion of $\wp(\tau)$.

We also use the fact that (by definition) e_1, e_2 and e_3 are roots of the cubic equation:

$$4X^3 - g_2X - g_3.$$

We also have the following identities for e_i's, which follow from the fact the $e_1 + e_2 + e_3 = 0$

$$\begin{aligned} 3g_2(\tau) &= -12(e_1e_2 + e_1e_3 + e_2e_3) \\ &= 4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1)) \\ &= 4((e_2 - e_3)^2 - (e_2 - e_1)(e_1 - e_3)) \\ &= 4((e_3 - e_1)^2 - (e_3 - e_2)(e_2 - e_1)) \end{aligned}$$

Thus,

$$\begin{aligned} \gamma_2 &= \frac{3g_2(\tau)}{4\pi^4\eta(\tau)^8} \\ &= \frac{-12(e_1e_2 + e_1e_3 + e_2e_3)}{4\pi^4\eta(\tau)^8} \\ &= \frac{4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1))}{4\pi^4\eta(\tau)^8} \\ &= \frac{4((\pi^2\eta(\tau)^4\mathfrak{f}(\tau)^8)^2 - (\pi^2\eta(\tau)^4\mathfrak{f}_1(\tau)^8)(\pi^2\eta(\tau)^4\mathfrak{f}_2(\tau)^8))}{4\pi^4\eta(\tau)^8} \\ &= \mathfrak{f}(\tau)^{16} - \mathfrak{f}_1(\tau)^8\mathfrak{f}_2(\tau)^8 \\ &= \mathfrak{f}(\tau)^{16} - \frac{\sqrt{2}^8}{\mathfrak{f}(\tau)^8} \end{aligned}$$

So, $\mathfrak{f}$ is a root of:

$$X^{24} - \gamma_2(\tau)X^8 - 16 = 0$$

The other two equations follow from the other two expansions of $3g_2$.

□

What this means is that $\mathfrak{f}$, $e^{\pi i/8}\mathfrak{f}_1$ and $e^{\pi i/8}\mathfrak{f}_2$ are all roots of the polynomial:

$$X^{24} - \gamma_2(\tau)X^8 - 16 = 0. \tag{2}$$

3 Building the Hilbert Class Field

Let $D = l^2\Delta$ be the discriminant of an order $\mathcal{O} \subset K$. Let $\mu = \frac{D+\sqrt{D}}{2}$.

Heegner's proof lies on the following important fact.

Theorem 6. *$j(\mu)$ is an algebraic integer of degree exactly $h(\mathcal{O})$.*

This means that when $d \equiv 1 \pmod 4$, and $l = 1$, $j\left(\frac{d+\sqrt{d}}{2}\right)$ is of degree exactly $h(d)$, the class number of K. As well, when $l = 2$, this shows that $j(\sqrt{d})$ is of degree $h(4d)$. We will be able to use this to our advantage.

In order to show Theorem 6 we will show the stronger result that $K(j(\mu))$ generates the Hilbert Class Field of K: a surprising and constructive result, which pulls together modular functions and class field theory.

In order to prove this stronger result, we need to learn a little more about how j classifies ideals in $\mathcal{O}_K$ (or any order $\mathcal{O}$).

First we recall that there is a correspondence between proper ideals $\mathfrak{a} \subset \mathcal{O}_K$ and numbers $\tau \in K$ by the map $\mathfrak{a} = [\alpha, \beta] \mapsto \frac{\beta}{\alpha}$. Without loss of generality, we will always order α and β so that $\tau = \frac{\beta}{\alpha} \in \mathcal{H}$. By this correspondence, $j(\mathfrak{a}) = j(\tau)$.

Thus, by the properties of the j-invariant, j characterizes distinct ideal classes in the ideal class group, that is, $\mathfrak{a} \sim \mathfrak{b}$ if and only if $j(\mathfrak{a}) = j(\mathfrak{b})$.

To see this, let $\mathfrak{a} = [\alpha, \beta]$ and $\mathfrak{b} = [\delta, \epsilon]$. Then for some $a, b \in \mathcal{O}_K$, without loss of generality relatively prime,

$$\mathfrak{a} \sim \mathfrak{b} \leftrightarrow a[\alpha, \beta] = b[\delta, \epsilon]$$
$$\frac{\beta}{\alpha} = \frac{b\delta}{a\epsilon}$$

Which is a fractional linear transformation, so $j(\mathfrak{a}) = j(\mathfrak{b})$. The converse is clear.

3.1 The Modular and Class Equations

We now introduce an important matrix group:

Definition 15. Let

$$C(m) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| ad = m,\ a > 0,\ 0 \le b < d \right\}$$

$C(m)$ has the following property:

$$|C(m)| = m \prod_{p|m} \left(1 + \frac{1}{p}\right)$$

The key to our proofs lies in two important equations, the modular equation and the class equation:

Definition 16. Let

$$\Phi_m(X, j(\tau)) = \prod_{\gamma \in C(m)} (X - j(\gamma\tau))$$

.

We note that since $m\tau = \gamma\tau$ where $\gamma = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$, $\Phi_m(j(m\tau), j(\tau)) = 0$.

Fact 3. The modular equation is $\Phi_m(X, Y)$. It has the following important properties:

1. $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.
2. $\Phi_m(X, Y)$ is irreducible as a polynomial in X.
3. $\Phi_m(X, Y) = \Phi_m(Y, X)$.
4. If m is not a perfect square, then $\Phi_m(X, X)$ is a monic polynomial of degree > 1.
5. For p prime, $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p\mathbb{Z}[X, Y]}$.

We refer the reader to [2] p. 231.

Remark 9. In order to understand how automorphisms affect $j(\tau)$ and $j(\gamma\tau)$, we show a few calculations involving the modular equation:

First, we let $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$. Then, since:

$$\begin{aligned} j(\tau) &= \frac{1}{q} + 744 + \sum_{n=1}^{\infty} a_n q^n \\ j(\gamma\tau) &= \frac{1}{q^{a^2/m}} e^{-2\pi i ab/m} + 744 + \sum_{n=1}^{\infty} a_n e^{2\pi i abn/m} q^{a^2 n/m} \\ &= \frac{1}{q_m^{a^2}} \zeta_m^{-ab} + 744 + \sum_{n=1}^{\infty} a_n \zeta_m^{abn} q_m^{a^2 n} \end{aligned}$$

Where $\zeta_m = e^{2\pi i/m}$ and $q_m = e^{2\pi i\tau/m}$.

Then, for σ a Frobenius automorphism in the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, $\sigma : \zeta_m \mapsto \zeta_m^k$, we have:

$$\begin{aligned}\sigma(j(\gamma\tau)) &= \frac{1}{q_m^{a^2}}\zeta_m^{-kab} + 744 + \sum_{n=1}^{\infty} a_n \zeta_m^{kabn} q_m^{a^2 n} \\ &= j\left(\begin{pmatrix} a & kb \\ 0 & d \end{pmatrix}\tau\right)\end{aligned}$$

This shows that $\sigma : j(\mathfrak{a}) \mapsto j(\mathfrak{b})$ for some $\mathfrak{b}$. In particular, we observe that $j(\gamma\tau) \in \mathbb{Q}(\zeta_m)((q_m))$, the ring of formal meromorphic Laurent series.

Definition 17. The *Class Equation* is:

$$H_K(X) := \prod_{i=1}^{h(d)} (X - j(\mathfrak{c}_i))$$

where the $\mathfrak{c}_i$ represent distinct ideal classes. We call the $j(\mathfrak{c}_i)$ the *class invariants* of $\mathcal{O}_K$.

We note that we can form a class equation, $H_{\mathcal{O}}$ over any order, $\mathcal{O}$, in a similar fashion.

In order to prove Theorem 6, we first make the weaker claim, simply that $j(\mu)$ is an algebraic integer.

Lemma 2. $j(\mu)$ is an algebraic integer.

Proof. We note that $j(\mu)$ is a root of the modular equation $\Phi_{2D}(X, X)$. Since $2D$ is not a perfect square, $\Phi_{2D}(X, X)$ is monic over $\mathbb{Z}[X]$, and so $j(\mu)$ is an algebraic integer. □

3.2 Involving the j-invariant

Let M be the splitting field of $H_K(X)$ over K. Our goal is to prove first that $M = L$, where L is the Hilbert Class Field, and secondly that $M = K(j(\mu))$, i.e., that H_K is irreducible over K.

We will prove this for the special case $\mathcal{O} = \mathcal{O}_K$, that is $l = 1$, and $d \equiv 1 \pmod 4$, letting $\mu = \frac{d+\sqrt{d}}{2}$. As we shall see, this is the case we will need for our main theorem.

Now, in the usual way, we are going to exclude the bad primes from our work. The ramified primes are primes which divide:

$$R = 2d \prod \delta(j(\mathfrak{c}_i))$$

where the product is taken over the distinct ideal classes of K, and $\delta(\alpha)$ is the root discriminant, $\delta(\alpha) = \prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha))^2$. See [2]. For the rest of this section, we assume $p \nmid R$.

Lemma 3. Let $p = \mathfrak{p}\mathfrak{p}'$ in K, and let $\mathfrak{B} \mid \mathfrak{p}$ in M. Then for $\mathfrak{c}$ an ideal class in O_K:

$$j(\mathfrak{p}\mathfrak{c}) \equiv j(\mathfrak{c})^p \text{ or } j(\mathfrak{p}\mathfrak{c})^p \equiv j(\mathfrak{c}) \pmod{\mathfrak{B}}.$$

Proof. The proof follows from the properties of the modular equation. We have:

$$0 = \Phi_p(j(\mathfrak{a}), j(\mathfrak{p}\mathfrak{a})) \equiv (j(\mathfrak{a})^p - j(\mathfrak{p}\mathfrak{a}))(j(\mathfrak{a}) - j(\mathfrak{p}\mathfrak{a})^p) \pmod{\mathbb{Z}[j(\mathfrak{a}), j(\mathfrak{p}\mathfrak{a})]}$$

The lemma follows from the fact that $\mathfrak{B} \subset \mathbb{Z}[j(\mathfrak{a}), j(\mathfrak{p}\mathfrak{a})] \subset K$. □

Note that if we replace $\mathfrak{c}$ by $\mathfrak{c}\mathfrak{p}'$, we get:

$$j(\mathfrak{c}) \equiv j(\mathfrak{c}\mathfrak{p}')^p \text{ or } j(\mathfrak{c})^p \equiv j(\mathfrak{c}\mathfrak{p}') \pmod{\mathfrak{B}}.$$

In fact, a stronger fact which we need is that:

$$j(\mathfrak{p}'\mathfrak{c}) \equiv j(\mathfrak{c}) \pmod{\mathfrak{B}}$$

If we choose $\mathfrak{p}$ such that its inertial degree over M is 1, that is $\mathfrak{p}$ splits completely, this is possible. This fact follows from the fact that:

$$j(\mathfrak{c})^p \equiv j(\mathfrak{c}) \pmod{\mathfrak{B}}$$

Luckily, Chebotarev's Density Theorem tells us that we can find such a $\mathfrak{p}$, [2], p. 239.

And so we have:

Lemma 4. $H_K(X) \in \mathbb{Q}(X)$ and M/K is abelian.

Proof. Let $G = \mathrm{Gal}(M/K)$. By Chebotarev's Density Theorem, [2] p.170, every $\sigma \in G$ is generated as Frobenius maps of infinitely many primes $\mathfrak{B} \subset M$, so for any $\sigma = (\frac{M/K}{\mathfrak{B}})$:

$$\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{B}}$$

for all $\alpha \in \mathcal{O}_K$, where $\mathfrak{B} \mid p$. We can look at the roots of the class equation, and see that:

$$\sigma(j(\mathfrak{c})) \equiv j(\mathfrak{c})^p \pmod{\mathfrak{B}}$$

Noting that the $j(\mathfrak{c})$ are distinct mod $\mathfrak{B}$, we have:

$$\sigma(j(\mathfrak{c})) = j(\mathfrak{c}\mathfrak{p}').$$

From this we can see that for any $\sigma, \sigma' \in G$ we have:

$$\sigma'[\sigma(j(\mathfrak{c}))] = \sigma[\sigma'(j(\mathfrak{c}))]$$

That is, G is abelian.

The fact that $H_K(X) \in \mathbb{Q}(X)$ follows from noting that since our frobenius automorphism, σ, permutes the class invariants, $H(X)$ is invariant under σ. □

Lemma 5. *M is the Hilbert class field.*

In order to prove this, we need the following fact from class field theory:

Fact 4. $\mathfrak{p}$ splits completely in M if and only if $(\frac{M/K}{\mathfrak{B}}) = 1$. See [2] p. 107.

Proof. (*of Lemma 5*) Let $\sigma = (\frac{M/K}{\mathfrak{p}})$ be the Frobenius map corresponding to $\mathfrak{p}$ in G. Since we know M is abelian, this is well defined. Then:

$$\sigma(j(\mathfrak{c})) \equiv j(\mathfrak{c})^p \pmod{\mathfrak{B}}$$

for any $\mathfrak{B} \mid \mathfrak{p}$. We note that if $\sigma = 1$, then :

$$j(\mathfrak{c}) \equiv j(\mathfrak{c})^p \pmod{\mathfrak{B}}$$

This implies that $\mathfrak{c}$ is a principal ideal. The converse is also clear.

From the above fact, we now have: $\mathfrak{p}$ splits completely in M if and only if $(\frac{M/K}{\mathfrak{p}}) = 1$, which happens if and only if $\mathfrak{p}$ lifts to become principal in M.

We can also see that our σ are defined by how they act on the class invariants, that is, G is isomorphic to the class group I_K. This shows that M is indeed the Hilbert Class Field. □

We have now dealt with the majority of Theorem 6, and we can quickly show:

Proof. (*of Theorem 6*) $H_K(X)$ is a polynomial of degree $h(\mathcal{O}_K)$ over $\mathbb{Q}$, and its splitting field is of degree $h(\mathcal{O}_K)$. We can see that the σ act transitively on the class invariants. Therefore, $H_K(X)$ is irreducible. Thus, since $j(\mu)$ is a root of $H_k(X)$, it generates M, that is, the Hilbert class field, and so $j(\mu)$ is an algebraic integer of degree exactly $h(\mathcal{O}_K)$. □

We turn our attention back to the cube root of j. Surprisingly, we have:

Theorem 7. *If $d \equiv 1$ (mod 4), and $3 \nmid d$, then $K(\gamma_2(\mu)) = K(j(\mu))$.*

Proof. We recall that:

$$\gamma_2(\mu) \in \mathbb{Q}\left(j\left(\frac{\mu}{3}\right), j(3\mu)\right).$$

Clearly $\mu \sim 3\mu$ as ideals, and since $3 \nmid d$, $\mu/3$ is an ideal in O_K, (i.e., a root of the class equation). Thus, $K(\gamma_2(\mu)) \subset K(j(\mu))$. Clearly, $j(\mu) \in \mathbb{Q}(\gamma_2(\mu))$, since $j(\mu)^3 = \gamma_2(\mu)$, and this proves the theorem. □

4 The Main Theorem

Theorem 8. *The Quadratic Imaginary Fields of class number one are $\mathbb{Q}(\sqrt{d})$ where:*

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

4.1 An Easy Case...

When $d \not\equiv 1 \pmod 4$, $\Delta_d = 4d$. Thus, using our quadratic form equivalence, we can look at the number of quadratic forms of discriminant $4d$. It turns out that this is not that difficult, and we can find all Imaginary Quadratic fields of class number one where $d \not\equiv 1 \pmod 4$. We use the following important theorem from the study of quadratic forms:

Theorem 9. *Let n be a positive integer. Then*

$$h(-4n) = 1 \Leftrightarrow n = 1, 2, 3, 4 \text{ or } 7$$

Proof. We proceed in cases, following Cox's exposition of a proof by Landau, [2]. We first note that the form $x^2 + ny^2$ has discriminant $-4n$. We then construct a second form with the same discriminant, which is not equivalent to the first.

First, we look at the case where $n > 1$ is not a prime power. Then, we can factor n into two relatively prime factors, $n = ac$ such that $1 < a < c$. Then, the form:

$$ax^2 + cy^2$$

also has discriminant $-4n$. The forms are inequivalent. Thus, $h(-4n) \geq 2$.

Secondly, we let n be an odd prime power. If $n+1$ is not a prime power, then we have $n+1 = ac$, where $1 < a < c$. Then:

$$ax^2 + 2xy + cy^2$$

has discriminant $4 - 4ac = -4(ac-1) = -4n$, and as before, since the coefficients are relatively prime, our two forms are inequivalent, thus $h(-4n) \geq 2$.

If $n+1$ is a prime power, that is, a power of 2, then $n = p^r$ and $n+1 = 2^s$. If $s \geq 6$, then $8 \leq 2^{s-3} + 1$, and so:

$$8x^2 + 6xy + (2^{s-3}+1)y^2$$

has relatively prime coefficients and discriminant $d = 36 - 4 \cdot 8(2^{s-3}+1) = 36 - 4(2^s + 8) = 4(9 - (n+1+9) = -4n$, so this form is inequivalent to $x^2 + ny^2$.

When $s = 1, 2, 3, 4$ and 5, then $n = 1, 3, 7, 15, 31$. We discard $n = 15$, as it is not a prime power, and direct computation shows that $h(-4 \cdot 31) = 3$. Thus, for $n = 1, 3, 7$, $h(-4n) = 1$. This can be verified by direct computation.

Finally, we look at the case where $n = 2^r$. If $r \geq 4$ then:

$$4x^2 + 4xy + (2^{r-2}+1)y^2$$

has relatively prime coefficients and discriminant $d = 16 - 4 \cdot 4(2^{r-2}+1) = 4(4 - (2^r + 4)) = -4n$, and so is inequivalent to $x^2 + ny^2$.

For $r = 3$, we can check that $h(-4 \cdot 8) = 2$, and the remaining cases have class number one, by direct computation. This concludes the proof.

□

Corollary 1. If $K = \mathbb{Q}(\sqrt{d})$ for $d < 0$, $d \not\equiv 1 \pmod 4$, then $h(K) = 1$ if and only if $d = -1$ or -2.

4.2 Two Simplifications

Quadratic forms can further reduce the number of fields we need to check. We have reduced to the case where $d < 0$, $d \equiv 1 \pmod 4$, so $h(K) = h(d)$. We can further assume that d is prime, using the following lemma:

Lemma 6. Let $d \equiv 1 \pmod 4$ be negative. If d is not prime, then there are at least two forms with discriminant d, that is, $h(d) > 1$.

Proof. Since $|d| \equiv 3 \pmod 4$, $|d|$ is not a square. Let $d = -kl$, where k and l are odd and positive integers greater than 1, and $k < l$. Since $l \cdot k \equiv 3$, one of l or k must be $\equiv 3$, and the other $\equiv 1$, and so $l + k \equiv 0$ and $3k - l \equiv 0 \pmod 4$.

Thus the forms

$$Q(x, y) = \frac{k+l}{4}x^2 + \frac{l-k}{2}xy + \frac{k+l}{4}x^2$$

with discriminant $\left(\frac{l-k}{2}\right)^2 - 4\frac{(l+k)(l+k)}{16} = \frac{l^2-2lk+k^2}{4} - \frac{k^2+2lk+k^2}{4} = -lk = d$, and

$$\widetilde{Q}(x, y) = \frac{1-d}{4}x^2 - \frac{d+1}{2}xy + \frac{1-d}{4}x^2$$

with discriminant: $\left(\frac{d+1}{2}\right)^2 - 4\frac{(l-d)(1-d)}{16} = \frac{d^2+2d+1}{4} - \frac{1-2d+d^2}{4} = d$ are inequivalent. We can see this by noting that since both forms are symmetric in x and y we can rewrite them as:

$$Q(x, y) = \frac{l}{4}(x + y)^2 + \frac{k}{4}(x - y)^2$$

and

$$\widetilde{Q}(x, y) = \frac{|d|}{4}(x + y)^2 + \frac{1}{4}(x - y)^2$$

So we are just looking at the forms $Q(x, y) = (kx'^2 + ly'^2)/4$ and $\widetilde{Q}(x, y) = (x'^2 + |d|y'^2)/4$, where x' and y' must have the same parity (since $x + y$ and $x - y$ do).

With this restriction in place, note that the smallest positive value that $\widetilde{Q}$ takes is 1 (taking $[x', y'] = [2, 0]$), while the smallest three values that Q could take are k, $(k + l)/4$, and l (taking $[x', y'] = [2, 0], [1, 1]$ and $[0, 2]$). Since $3 \leq k < l$, these are all greater than 1. So the forms do not represent the same integers and are not equivalent.

□

We present one more simplification. Using some basic facts from the study of orders in Quadratic Imaginary number fields, we have the following:

Fact 5. Letting $\left(\frac{d}{2}\right)$ be the Kronecker symbol, so

$$\left(\frac{d}{2}\right) := \begin{cases} 0 & \text{if } d \not\equiv 1 \pmod 4 \\ 1 & \text{if } d \equiv 1 \pmod 8 \\ -1 & \text{if } d \equiv 5 \pmod 8 \end{cases}$$

We have:

$$\frac{h(4d)}{h(d)} = 2\left(1 - \left(\frac{d}{2}\right)\frac{1}{2}\right)$$

For a proof, see [2].

From Fact 5, we can see that if $d \equiv 1 \pmod 8$, then $h(4d) = h(d)$. From Lemma 6, we know that if $d \equiv 1 \pmod 8$, $d < 0$ and $h(4d) = 1$, then $d = -7$. Thus, we can concentrate on the case where $d \equiv 5 \pmod 8$.

4.3 The Harder Case

Following Stark's notation, we use the following terminology:

$$\begin{aligned} J &= j(\sqrt{d}) & F &= \mathfrak{f}(\sqrt{d}) \\ h &= h(d) & j &= j\left(\tfrac{-3+\sqrt{d}}{2}\right) \\ f &= e^{\pi i/8}\mathfrak{f}_2\left(\tfrac{-3+\sqrt{d}}{2}\right) & \gamma &= \gamma_2\left(\tfrac{-3+\sqrt{d}}{2}\right) \end{aligned}$$

We let $K = \mathbb{Q}(d)$ be an imaginary quadratic number field with class number one. We assume that $d \equiv 5 \pmod 8$. We also know that $d = -p$, where p is prime, hence we can assume that $3 \nmid d$, since direct computation shows that that $h(-3) = 1$. We note that $\frac{-3+\sqrt{d}}{2}$ is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $\frac{d+\sqrt{d}}{2}$. Then (given $3 \nmid d$), j and γ are integers, since they generate the Hilbert Class Field which is of degree $h = 1$ over K.

We recall that f is a root of $X^{24} - \gamma X^8 - 16 = 0$, and that J is a root of $X^{24} - J^{1/3}X^8 - 16 = 0$. We need to relate F^2, f^2, and J, in fact, we will show that they generate the same extension over $\mathbb{Q}$.

Claim 3. $f^2 = \frac{2}{F^2}$. Hence $\mathbb{Q}(F^2) = \mathbb{Q}(f^2)$.

Proof. Recalling that $\eta(\tau + 1) = e^{2\pi i/24}\eta(\tau)$, we see that $\eta(\sqrt{d}) = e^{2\pi i/8}\eta(\sqrt{d} - 3)$ and $\eta\left(\frac{1+\sqrt{d}}{2}\right) = e^{2\pi i/12}\eta\left(\frac{-3+\sqrt{d}}{2}\right)$, and so

$$\begin{aligned}\frac{2}{F^2} &= 2e^{\frac{2\pi i}{24}} \frac{\eta^2(\sqrt{d})}{\eta^2\left(\frac{1+\sqrt{d}}{2}\right)} \\ &= 2e^{2\pi i/24} \frac{e^{2\pi i/4}\eta^2(-3+\sqrt{d})}{e^{2\pi i/6}\eta^2\left(\frac{-3+\sqrt{d}}{2}\right)} \\ &= \left(e^{\pi i/8}\mathfrak{f}_2\left(\frac{-3+\sqrt{d}}{2}\right)\right)^2 \\ &= f^2\end{aligned}$$

□

We note that since

$$J = \left(\frac{F^{24}-16}{F^8}\right)^3$$

then $J \in \mathbb{Q}(F^2)$. We can strengthen this, as the following claim shows.

Claim 4. $F^2 \in \mathbb{Q}(J)$.

Remark 10. One of the problems in Heegner's original proof is that he claims the stronger result that $F \in \mathbb{Q}(J)$. Unfortunately, this is presented without proof. Though not needed for the class number one problem, this was later proven by B.J. Birch. This is one of the key reasons why many doubted the veracity of Heegner's proof. As to the more general result that $F^2 \in \mathbb{Q}(J)$, both Heegner and Deuring present this fact without proof, resting on earlier work of Weber. Stark, however, proves this fact by using a series of modular equations. Cox shows this by using some more sophisticated class field theory. Here, we present a more basic explanation, resting heavily on the properties of modular functions, For more elegant proofs, see [2] and [11].

Proof. We recall that since $\mathfrak{f}(8\tau)^6$ is weakly modular for $\Gamma_0(64)$, then $\mathfrak{f}(\sqrt{d})^6 \in \mathbb{Q}(j(\sqrt{d}/8), j(8\sqrt{d}))$.

Since $\frac{\sqrt{d}}{8}$ corresponds to the ideal $[8, \sqrt{d}] \in O_K$, then $j\left(\frac{\sqrt{d}}{8}\right)$ is a root of the class equation, and is in the class field, $\mathbb{Q}(j(\sqrt{d}))$. This proves that $F^6 \in \mathbb{Q}(J)$. Since

$$F^2 = \frac{(F^6)^4 - 16}{J \cdot F^6}$$

then $F^2 \in \mathbb{Q}(J)$ as well.

□

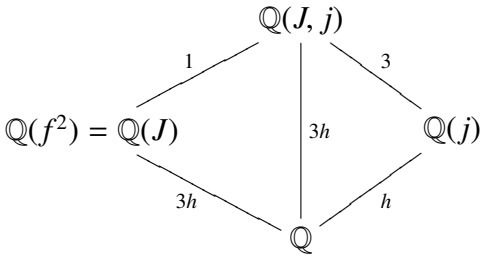
Using Fact 5, and the fact that $\left(\frac{d}{2}\right) = -1$, we have $h(4d) = 3h(d)$. We use the fact that $J = j(\sqrt{d})$ generates the class field corresponding to the order $O = 2O_K$. We know from earlier that $J = j(\sqrt{d})$ is an algebraic integer of degree $h(4d) = 3h(d)$, [2]. Thus, J is algebraic over $\mathbb{Q}$ of degree $3h$. In fact, from above, it is at most cubic over $\mathbb{Q}(j)$. Looking at the degrees of our field extension, we have:

$$[\mathbb{Q}(J, j) : \mathbb{Q}] = [\mathbb{Q}(J, j) : \mathbb{Q}(j)][\mathbb{Q}(j) : \mathbb{Q}] \leq 3h$$

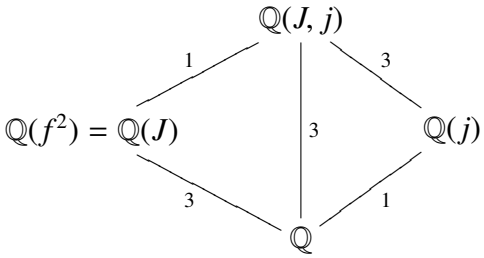
and

$$[\mathbb{Q}(J, j) : \mathbb{Q}] \geq [\mathbb{Q}(J) : \mathbb{Q}] = 3h$$

Hence



Since $[\mathbb{Q}(J, j) : \mathbb{Q}] = 3h$ and $\mathbb{Q}(J) = \mathbb{Q}(J, j) = \mathbb{Q}(F^2) = \mathbb{Q}(f^2)$. We note that since $h = 1$, we have:



Clearly, f^2 is of degree exactly 3 over $\mathbb{Q}$. Since f satisfies equation (2), a monic polynomial over $\mathbb{Z}$, f and hence f^2 are algebraic integers and hence f^2 satisfies the equation:

$$X^3 + aX^2 + bX + c = 0$$

for some $a, b, c \in \mathbb{Z}$. By rearranging and squaring both sides we have f^2 satisfying:

$$(X^3 + bX)^2 = (-aX^2 - c)^2$$
$$X^6 + 2bX^4 + b^2X^2 - a^2X^4 - 2acX^2 - c^2 = 0$$

So f^4 satisfies the cubic equation:

$$X^3 + (2b - a^2)X^2 + (b^2 - 2ac)X + (-c^2) = 0$$

or

$$X^3 + dX^2 + eX + g = 0$$

where

$$d = 2b - a^2$$
$$e = b^2 - 2ac$$
$$g = -c^2.$$

By separating and squaring again, we find that f^8 satisfies the cubic equation:

$$X^3 + (2e - d^2)X^2 + (e^2 - 2dg)X + (-g^2) = 0$$

but from the fact that f is a root of (2), f^8 is a root of the cubic:

$$X^3 - \gamma X - 16 = 0.$$

Since f^8 is of degree exactly 3 over $\mathbb{Q}$, and both polynomials are monic, we can conclude that they are equal, therefore:

$$2e - d^2 = 0 \tag{3}$$
$$e^2 - 2dg = -\gamma \tag{4}$$
$$g^2 = 16 \tag{5}$$

Clearly, $g = -4 = -c^2$ and $c = \pm 2$. Simple algebra shows that we can assume $c = 2$ without changing our equation, and from equation (3) we have the Diophantine Equation:

$$2(b^2 - 4a) = (2b - a^2)^2$$

.

Looking at this equation mod 4, we can see that a and b must be even. Making the substitution $X = -a/2$ and $Y = (b-a^2)/2$, we obtain the Diophantine equation:

$$2X(X^3 + 1) = Y^2. \tag{6}$$

This is called *Heegner's Diophantine Equation*. Luckily, finding all the integer solutions to equation (6) is not difficult.

Theorem 10. *The only solutions to equation (6) are:*

$$(X, Y) = (0, 0), (-1, 0), (1, \pm 2), \text{ and } (2, \pm 6).$$

Proof. This proof follows Cox's exposition, see [2].

We first note that X and X^3+1 are relatively prime. Thus in order for $2X(X^3+1)$ to be a square, $\pm(X^3 + 1)$ must be a square or twice a square. We then have four cases:

1. $X^3 + 1 = Z^2$
2. $X^3 + 1 = -Z^2$
3. $X^3 + 1 = -2Z^2$
4. $X^3 + 1 = 2Z^2$

The only solutions to the first case are $(X, Z) = (-1, 0), (0, \pm 1), (2, \pm 3)$ and to the second case, $(X, Z) = (-1, 0)$. The first case is the most difficult to show, and was first proven by Euler, using infinite descent. For details, see [2], pp. 283-285.

For the third case, we note that in $Z(\sqrt{-2})$, there are only two units, ± 1. Thus:

$$\begin{aligned} X^3 + 1 &= -2Z^2 \\ X^3 &= (\sqrt{-2}Z - 1)(\sqrt{-2}Z + 1) \end{aligned}$$

As both of these factors are relatively prime, they must each be a cube in $\mathbb{Z}(\sqrt{-2})$. So:

$$\begin{aligned} (\sqrt{-2}Z + 1) &= (a + \sqrt{-2}b)^3 \\ &= a^3 - 6ab^2 + \sqrt{-2}(3a^2b - 2b^3) \end{aligned}$$

Thus:

$$a(a^2 - 6b^2) = 1$$

Which implies that a is a unit, so $a = \pm 1$. Solving for b, we find that the only solution is $(X, Z) = (-1, 0)$. By a similar argument, the only solutions to the fourth case are $(X, Z) = (1, \pm 1)$. The rest of the proof follows.

□

Now we have the following solutions for (a, b), and from equation (4) we know $\gamma = -(b^2 - 4a)^2 - 8(2b - a^2)$. Using computations, we find that these values of γ correspond to known quadratic fields, $\mathbb{Q}(\sqrt{d})$, see [2], p.261.

X	Y	$a = -2X$	$b = 4X^2 + 2Y$	γ	d
0	0	0	0	0	-3
-1	0	2	4	-96	-19
1	2	-2	8	-5280	-67
1	-2	-2	0	-32	-11
2	6	-4	28	-640320	-163
2	-6	-4	4	-960	-43

These are the only solutions for $d \equiv 5 \pmod 8$.

5 Conclusion

The class number one problem has now been completely solved. Heegner's proof (modulo appropriate corrections) is alluring in its simplicity, and in its elegant use of elementary number theory. Lately, newer proofs have been published, utilizing the concept of moduli spaces and modernizing the language. See, for instance, the work of Imin Chen, [1].

After solving the class number one problem, Baker and Stark completed the classification for class number $N = 2$. Goldfeld showed that if the Birch - Swinnerton-Dyer Conjecture holds, the problem of finding all Quadratic Imaginary Fields of class number N was a finite computation. Using methods of Gross and Zagier, this was soon proven unconditionally, and the computation was possible. Using these computational methods involving elliptic curves, the cases $N \leq 7$ and odd $N \leq 23$ were solved.

A 2004 paper by Mark Watkins made a huge leap, classifying all Quadratic Imaginary Fields of class number $N \leq 100$ [12]. Watkins uses L-functions with low-height zeros at the critical point.

Today, many are trying to expand on this problem, by using these methods to classify other field extensions, such as Imaginary Quartic Fields. One of the interesting things about the class number problem, and a reason why it still maintains its glamour 40 years after the first proof is in its simplicity to state, and in the way that it pulls together many seemingly separate areas of number theory.

References

[1] Chen, Imin, "On Siegel's Modular Curve of Level 5 and the Class Number One Problem", 1998.

[2] Cox, David A, *Primes of the form* $x^2 + ny^2$, New York: John Wiley and Sons Inc, 1989.

[3] Cohn, Harvey. *Introduction to construction of class fields*, Cambridge: Cambridge University Press, 1985.

[4] Diamond, Fred and Jerry Shurman, *A First Course in Modular Forms*, New York: Springer, 2000.

[5] Deuring, Max, "Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins", Inventiones math. 5, pp.169-179, 1969.

[6] Heegner, Kurt, "Diophantische Analysis und Modulfunktionen", Math. Zeitschrichft, 59, 1952, pp. 227-253.

[7] Ireland, Kenneth and Michael Rosen, *A Classical Intorduction to Modern Number Theory*, 2nd Edition (1990), New York: Springer-Verlag, 1972.

[8] Koblitz, Neil, *An Introduction to Elliptic Curves and Modular Forms*, New York: Springer-Verag, 1983.

[9] Neukirch, Jürgen, *Algebraic Number Theory*, Berlin: Springer-Verlag, 1999.

[10] Stark, H.M, "Class-Numbers of Complex Quadratic Fields", Antwerp, International Summer School on Modular Functions, 1972, pp. 155-174.

[11] Stark, Harold M, "On the "Gap" in a theorem of Heegner", J. Number Theory 1, 1969, pp. 16-27.

[12] Watkins, Mark, "Class Numbers of Imaginary Quadratic Fields", Mathematics of Computation: Vol. 73, num 246, pp. 907-938, 2004.

Appendix - List of Notation

The Artin Symbol $(\frac{L/K}{\mathfrak{B}})$: the Frobenius automorphism in $\mathrm{Gal}(L/K)$ associated to $\mathfrak{B}$

$$C(m) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| ad = m,\ a > 0,\ 0 \le b < d \right\}$$

$\Delta_d = \Delta$: the discriminant of $\mathcal{O}_K$

$\Delta(\tau) := g_2^3(\tau) - 27g_3^2(\tau)$, the discriminant function

$D = l^2\Delta$: the discriminant of an order $\mathcal{O}_l \in K$

$$\eta(\tau) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$$

$$E_2(\tau) := \frac{3}{\pi^2} \sum_{c \in \mathbb{Z}} \sum_{\substack{d \in \mathbb{Z} \\ (c,d) \neq (0,0)}} \frac{1}{(c\tau + d)^2} = 1 - 24 \sum_{n=1}^{\infty} \sigma(n) q^n$$

$$\mathfrak{f}(\tau) := e^{\frac{-\pi i}{24}} \frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)} = q^{-1/48} \prod_{n=1}^{\infty} (1 + q^{n-1/2})$$

$$\mathfrak{f}_1(\tau) := \frac{\eta(\frac{\tau}{2})}{\eta(\tau)} = q^{-1/48} \prod_{n=1}^{\infty} (1 - q^{n-1/2})$$

$$\mathfrak{f}_2(\tau) := \sqrt{2} \frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2} q^{1/24} \prod_{n=1}^{\infty} (1 + q^n)$$

$f[\gamma]_k(\tau) := (c\tau + d)^{-k} f(\gamma\tau)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \ a \equiv d \equiv 1,\ b \equiv c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0,\ a \equiv d \equiv 1 \pmod{N} \right\}$$

$$g_2(\tau) := 60 \sum_{\substack{c,d \in \mathbb{Z} \\ (c,d) \neq (0,0)}} \frac{1}{(c\tau + d)^4}$$

$$g_3(\tau) := 140 \sum_{\substack{c,d \in \mathbb{Z} \\ (c,d) \neq (0,0)}} \frac{1}{(c\tau + d)^6}$$

$$\gamma_2(\tau) := (j(\tau))^{1/3} = \frac{3g_2(\tau)}{4\pi^4 \eta(\tau)^8}$$

$h(\mathcal{O}_K) = h(K)$: the ideal class number of a field

$h(D)$: the form class number

The *Hilbert Class Field* of a number field K is the maximal (relatively) Abelian unramified extension L/K

$H_K(X) := \prod_{i=1}^{h(K)} (X - j(\mathfrak{c}_i))$: the Class Equation

Heegner's Diophantine equation: $2X(X^3 + 1) = Y^2$

I_K: the Ideal Class Group

$$j(\tau) := \frac{1728 g_2^3(\tau)}{\Delta(\tau)}$$

K: an algebraic number field, usually $\mathbb{Q}(\sqrt{d})$ where $d < 0$

The Kronecker symbol: $\left(\frac{d}{2}\right)$ and:

$$\left(\frac{d}{2}\right) := \begin{cases} 0 & \text{if } d \not\equiv 1 \pmod 4 \\ 1 & \text{if } d \equiv 1 \pmod 8 \\ -1 & \text{if } d \equiv 5 \pmod 8 \end{cases}$$

$\mu = \frac{D+\sqrt{D}}{2}$

$\mathcal{O}$: an *order* of K

$\mathcal{O}_K := \{a \in K |$ the minimal polynomial of a is monic$\}$

$\Phi_m(X, j(\tau)) := \prod_{\gamma \in C(m)} (X - j(\gamma\tau))$

$\Phi_m(X, Y)$: the Modular Equation

$Q(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ is a quadratic form with discriminant $d := b^2 - 4ac$

$q = e^{2\pi i\tau}$

$R(\Lambda)$: the ring of complex multiplications of a lattice, Λ

$\sigma(n) := \sum_{d|n} d$: the divisor sum

Stark's Notation:

$$\begin{array}{llll} J & = j(\sqrt{d}) & F & = \mathfrak{f}(\sqrt{d}) \\ h & = h(d) & j & = j\left(\frac{-3+\sqrt{d}}{2}\right) \\ f & = e^{\pi i/8}\mathfrak{f}_2\left(\frac{-3+\sqrt{d}}{2}\right) & \gamma & = \gamma_2\left(\frac{-3+\sqrt{d}}{2}\right) \end{array}$$