MODULAR CURVES AND THE CLASS NUMBER ONE PROBLEM

JEREMY BOOHER

Gauss found 9 imaginary quadratic fields with class number one, and in the early 19th century conjectured he had found all of them. It turns out he was correct, but it took until the mid 20th century to prove this.

Theorem 1. *Let K be an imaginary quadratic field whose ring of integers has class number one. Then K is one of*

$$\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163}).$$

There are several approaches. Heegner [9] gave a proof in 1952 using the theory of modular functions and complex multiplication. It was dismissed since there were gaps in Heegner's paper and the work of Weber [18] on which it was based. In 1967 Stark gave a correct proof [16], and then noticed that Heegner's proof was essentially correct and in fact equivalent to his own. Also in 1967, Baker gave a proof using lower bounds for linear forms in logarithms [1].

Later, Serre [14] gave a new approach based on modular curve, reducing the class number one problem to finding special points on the modular curve $X_{ns}^+(n)$. For certain values of n, it is feasible to find all of these points. He remarks that when "$N = 24$ An elliptic curve is obtained. This is the level considered in effect by Heegner." Serre says nothing more, and later writers only repeat this comment. This essay will present Heegner's argument, as modernized in Cox [7], then explain Serre's strategy. We will work out unrecorded details of the argument for level 24, find the elliptic curve, and relate it to Heegner's original argument.

To answer the class number one problem, it is easier to generalize it to arbitrary orders in imaginary quadratic fields. In the first section, we do this and recall a few classical results about the class number of orders. Section 2 develops theory about the j invariant and the class equation. Section 3 then studies other modular functions, especially Weber's modular functions, which are the building block's of Heegner's argument. Next we use Weber's functions to calculate the j-invariants of all known imaginary quadratic fields of class number one so we can identify them based on their j invariant. Section 5 relates these modular functions to the class number using class fields and theory of complex multiplication. Heegner's argument is presented in section 6. Changing direction, the next section deals with the question of when modular curves are defined over the rationals, and section 8 describes the connection Serre found between $X_{ns}^+(n)$ and the class number one problem. Finally, section 9 solves the class number one problem using $X_{ns}^+(24)$ and relates it to Heegner's argument.

Solving the class number one problem requires a lot of background material. Things on the level of Part III at Cambridge University will be used without proof and sometimes without explicit mention. In particular, knowledge of basic algebraic number theory, the definitions of global class field theory, the basic theory theory of modular forms and functions, and the basic theory of elliptic curves over $\mathbb{C}$ will be essential. Slightly less basic but very important

Date: Submitted May 6, 2011, updated December 17, 2014.

is the relation between the modular curve $\Gamma\backslash\mathcal{H}^*$ and modular functions and its interpretation as a Riemann surface parametrizing elliptic curves with additional data. Besides these basic assumptions, everything will be proven completely except for Theorem 37 which relies on an unproven result about complex multiplication.

1. Class Numbers of Imaginary Quadratic Orders

The class group of an order $\mathcal{O}$ in an imaginary quadratic field K is the quotient of proper fractional ideals by principal fractional ideals. Recall that a fractional ideal is proper if it is invertible, and a fractional ideal is proper if its norm has no common factors with the conductor of $\mathcal{O}$. The class number of $\mathcal{O}$, denoted by $h(\mathcal{O})$, is the size of the class group. It is also written $h(D)$ where D is the discriminant of $\mathcal{O}$.

If $\mathcal{O} = \mathcal{O}_K$ is the maximal order, this recovers the usual definition of class number. There is a very easy way to check if $h(\mathcal{O}_K) = 1$.

Proposition 2. *Let p be a prime $p > 3$ with $p \equiv 3 \mod 4$. Then $h(-p) = 1$ if and only if $\left(\frac{l}{p}\right) = -1$ for all primes l less than $p/4$.*

Proof. Note $\left(\frac{l}{p}\right) = -1$ if and only if l is inert in $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$. So if $\left(\frac{l}{p}\right) = 1$ there are ideals of norm l. If $h(-p) = 1$, these ideals are principal, so there are half-integers x and y such that $x^2 + py^2 = l$. As l is not a square $y \neq 0$ so $l > py^2 \geq p/4$.

Conversely, $\left(\frac{l}{p}\right) = -1$ implies every prime ideal of norm less than $\sqrt{p/4}$ is non-split, hence principal. Every ideal class contains an integral ideal with norm in this range, so $h(-p) = 1$. □

This relation between the splitting of primes and the class number is the basis of Serre's approach. The class number of a general order is related to the maximal order.

Proposition 3. *Let $\mathcal{O}$ be an order of conductor f. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

where $\left(\frac{d_K}{p}\right)$ is the Kronecker symbol.

For more information about orders in imaginary quadratic fields and proofs, see Section 7 of Cox [7]. There is also a discussion of the connection between Gauss's work on quadratic forms and the modern formulation in terms of ideals.

The more general question of which imaginary quadratic orders have class number one is no harder to answer, and in fact was investigated first (in terms of classes of quadratic forms). There are several types of order for which the problem is simple.

Theorem 4 (Landau)**.** *Let n be a positive integer. Then*

$$h(-4n) = 1 \quad \textit{iff} \quad n = 1, 2, 3, 4, 7.$$

A very easy proof using quadratic forms is given in section 2 of Cox [7]. Another easy case is when n is the product of two primes.

Theorem 5. *Let n have at least two odd prime factors. Then $h(-n)$ is even.*

This can be proven using the genus theory of quadratic forms (section 3 of Cox) or of ideals (section 6 of Cox) [7].

The following theorem gives a complete list of orders with class number one.

Theorem 6. *Let $\mathcal{O}$ be an order in an imaginary quadratic field, and D be its discriminant. Then*

$$h(D) \iff D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

This reduces to the class number one problem for maximal orders. The idea is to use Proposition 3 to relate the class number of the order to that of the maximal order: the details are in section 7 of Cox [7]. The heart of the matter is proving Theorem 1.

2. The $j-$invariant and Class Equation

The most famous modular function is the $j-$invariant. The following standard properties and their proofs may be found in section 10 of Cox [7].

The j function is a function on lattices in $\mathbb{C}$ (equivalently, a modular function for $\mathrm{SL}_2(\mathbb{Z})$) and can be defined as

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

where g_2 and g_3 are the constants appearing in the differential equation for the Weierstrass $\wp$ function for the lattice L

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L). \tag{1}$$

They are given by

$$g_2(L) = 60\sum_{\omega\in L-\{0\}}\frac{1}{\omega^4}$$
$$g_3(L) = 140\sum_{\omega\in L-\{0\}}\frac{1}{\omega^6}.$$

The following result and its corollary are essential to the class number one problem. it allows the identification of imaginary quadratic fields by their $j-$invariants.

Theorem 7. *If L and L' are lattices, then $j(L) = j(L')$ if and only if L and L' are homothetic.*

Corollary 8. *Let K and K' be imaginary quadratic fields. Then $K = K'$ iff $j(\mathcal{O}_K) = j(\mathcal{O}_{K'})$.*

The j function can also be regarded as a function of the upper half plane by setting $j(z) = j([1, z])$. It is a modular function for $\mathrm{SL}_2(\mathbb{Z})$, and identifies the upper half plane and infinity with the Riemann sphere. Its definition in terms of lattices can expressed in terms of modular forms:

$$j(z) = 1728\frac{g_4(z)^3}{g_4(z)^3 - 27g_6(z)^2} = 1728\frac{g_4(z)^3}{\Delta(z)}$$

where g_{2n} is viewed as a normalization of the Eisenstein series of weight $2n$ and $\Delta(z) := g_4(z)^3 - 27g_6(z)^2$ is interpretted as the modular discriminant.

It also has an integral $q-$expansion.

Proposition 9. *Let $q = e^{2\pi i z}$. Then*

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

It is elementary, but very important later, that $j(z)$ (or any function with a rational $q-$expansion) is real on the positive imaginary axis.

2.1. Modular Functions for $\Gamma_0(N)$.

Recall that the field of modular functions for $\mathrm{SL}_2(\mathbb{Z})$ is generated by the $j-$function. We will reprove this important fact and then go on to show that $j(z)$ and $j(Nz)$ together generate the field of modular functions for $\Gamma_0(N)$ following Section 11 of Cox [7].

Theorem 10. *Every modular function for $\mathrm{SL}_2(\mathbb{Z})$ is a rational function of j. If it is holomorphic on the upper half plane, it is a polynomial.*

Proof. Let $f(z)$ be a modular function for $\mathrm{SL}_2(\mathbb{Z})$. It has a finite number of poles on the fundamental domain as the Riemann sphere is compact and the poles of a meromorphic function are isolated. Let Z be the set of poles, and $m(z)$ be the multiplicity of the pole. Assume that none of the poles occur at i or $\rho = \frac{-1+\sqrt{-3}}{2}$ for now. Define

$$g(z) := f(z) \prod_{w \in Z} (j(z) - j(w))^{m(w)}.$$

Then $g(z)$ is a holomorphic function on the upper half plane since $j(z) - j(w)$ has a zero of order 1 at w (note $j'(w) \neq 0$ for $z \neq i, \rho$). Now $g(z)$ is meromorphic at infinity, so there is a polynomial $P(w)$ such that $g(z) - P(j(z))$ is holomorphic at infinity (simply cancel the negative powers of q in the q expansion one by one). But the only holomorphic functions on the Riemann sphere are constants. Therefore $f(z)$ is a rational function of $j(z)$.

If a pole occurs at i or ρ, a standard result in the theory of modular forms says the order of vanishing is a multiple of $k = 2$ or 3). But $j(z) - j(w)$ has a zero of order k so using the factor $(j(z) - j(w))^{m(w)/k}$ makes the above argument work.

If $f(z)$ were already holomorphic on the upper half plane, we need not introduce any denominator. □

To deal with $\Gamma_0(N)$, we need information about the cusps. The following elementary lemma from the theory of modular forms is the key.

Lemma 11. *Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $C(N)$ be the set of matrices*

$$C(N) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = N, a > 0, 0 \leq b < d, \gcd(a,b,d) = 1 \right\}.$$

Then there exists a $\tilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma = \tilde{\gamma} \sigma$$

for some $\sigma \in C(N)$.

Proof. This is proven in many places, including section 11 of Cox [7]. □

Theorem 12. *Let $f(z)$ be a modular form for $\Gamma_0(N)$. Then $f(z)$ is a rational function in $j(z)$ and $j(Nz)$.*

The proof of this theorem is more involved. The first step is to show $j(Nz)$ is a modular function of weight N. Next we introduce the modular equation and use it write $f(z)$ as a rational function in $j(z)$ and $j(Nz)$.

Lemma 13. *$j(Nz)$ is a modular function for $\Gamma_0(N)$.*

Proof. For $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N)$, a direct calculation yields

$$j(N\frac{az+b}{Ncz+d}) = j(\frac{a(Nz)+bN}{c(Nz)+d}) = j(Nz).$$

The trickier part is the behavior at the cusps. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, it suffices to verify that $j(N\gamma z)$ is meromorphic at ∞. But by the lemma we know that there is a $\sigma \in C(N)$ and $\tilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$j(N\gamma z) = j(\tilde{\gamma}(\sigma z)) = j(\sigma z).$$

But $e^{2\pi i\sigma z} = e^{2\pi i(az+b)/d} = q^{a/d}e^{2\pi ib/d}$ so the q-expansion of $j(Nz)$ has only finitely many terms of negative degree. Therefore it is meromorphic at all of the cusps. □

Next we look at the modular equation. Let $\{\gamma_i\}_i$ be coset representatives of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, and consider the polynomial

$$\Phi_N(x,z) = \prod_i (x - j(N\gamma_i z))$$

Proposition 14. *$\Phi_N(x,z)$ is a polynomial in x and $j(z)$.*

Proof. Consider the coefficient of x^k in $\Phi_m(x,z)$. It is a symmetric polynomial in the $j(m\gamma_i z)$, and is holomorphic on the upper half plane. It is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ as the action simply permutes the cosets of $\Gamma_0(N)$ and hence leaves the product unchanged. To see that it is meromorphic at infinity, simply expand $j(N\gamma_i z)$ as a q-series. It has only a finite number of negative terms, and the coefficient is a polynomial in them. Thus the coefficients are meromorphic at infinity. By Theorem 10, the coefficients of x are polynomials in $j(z)$. □

Therefore there exists a polynomial of two variables $\Phi_N(x,y) \in \mathbb{C}[x,y]$ such that

$$\Phi_N(x,j(z)) = \prod (x - j(N\gamma_i z)).$$

This is called the modular equation.

Proposition 15. *The modular equation satisfies the following properties:*

(1) $\Phi_N(j(Nz),j(z)) = 0$.
(2) *$\Phi_N(x,y)$ is an irreducible polynomial in x.*
(3) *$\Phi_N(x,y)$ has integer coefficients.*
(4) *If N is not a perfect square, $\Phi_N(x,x)$ is a polynomial of degree > 1 whose leading coefficient is ± 1.*

Proof. To prove the first part, note that one of the coset representatives for $\Gamma_0(N)$ may as well be chosen to be the identity matrix. Then one of the terms in $\Phi_N(x,j(z))$ is $x - j(Nz)$.

To prove the second, let m be the degree of Φ_N viewed as a polynomial in x with coefficients in $\mathbb{C}[y]$. Note that because $\Phi_N(j(Nz),j(z)) = 0$, m is an upper bound for the degree of the field extension $\mathbb{C}(j(z),j(Nz))$ over $\mathbb{C}(j(z))$. If we had equality, $\Phi_N(x,j(z))$ would be the minimal polynomial and hence irreducible. For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, define $\psi_\gamma : \mathbb{C}(j(z), j(Nz)) \to \mathbb{C}((z))$ by $\psi_\gamma(f)(z) = f(\gamma z)$. This is an embedding of $\mathbb{C}(j(z), j(Nz))$ into $\mathbb{C}((z))$. Since $j(z)$ is a modular function for $\mathrm{SL}_2(\mathbb{Z})$, $\mathbb{C}(j(z))$ is fixed. The number of distinct such embeddings is the degree of the extension $\mathbb{C}(j(z), j(Nz))$ over $\mathbb{C}(j(z))$. However, we know that $j(N\gamma_i z) \neq j(N\gamma_j z)$ unless $i = j$ as the $\{\gamma_i\}$ are a set of coset representatives for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Since there are m distinct embeddings, Φ_N is irreducible.

For the third part, we will show that any symmetric function $f(z)$ in the $j(N\gamma_i z)$ is a polynomial in $j(z)$ with integer coefficients. By Lemma 11, we look at symmetric functions in $j(\sigma z)$ for $\sigma \in C(N)$. Simply writing down the q series, we see $f(z) \in \mathbb{Q}(\zeta_N)((q^{\frac{1}{N}}))$, the ring of formal Laurent series over $\mathbb{Q}(\zeta_N)$. The coefficients actually lie in $\mathbb{Q}$. To verify this, let $\psi_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ send ζ_N to ζ_N^k. For $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$,

$$\psi_k(j(\sigma z)) = \frac{\zeta_N^{abk}}{q^{\frac{1}{N}a^2}} + \sum_{n=0}^{\infty} c_n \zeta_N^{abk} (q^{1/N})^{a^2 n}.$$

But writing $abk = ab' \mod N$ and setting $\sigma' = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}$, we see that $\psi(j(\sigma z))$ is $j(\sigma' z)$. Since the function is symmetric in the $j(\sigma z)$, the $q-$series is in $\mathbb{Q}((q^{\frac{1}{N}}))$. We already know the coefficients are algebraic integers as $j(z)$ has integer coefficients, and that the only powers of q appearing are integer powers, so it actually lies in $\mathbb{Z}((q))$. To conclude it is a polynomial, simply run through the proof of Theorem 10 and note that being in $\mathbb{Z}((q))$ is enough to make the resulting polynomial have integer coefficients.

For the last part, look at the $q-$series obtained by substituting $j(z)$ for x. Use Lemma 11 to rewrite the factors in Φ_N as

$$(j(z) - j(N\gamma_i z)) = (j(z) - j(\sigma z)) = \frac{1}{q} - \frac{\sigma_N^{-ab}}{q^{a/d}} + \sum_{n=0}^{\infty} d_n (q^{\frac{1}{N}})^n$$

for $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(N)$. Since N is not a perfect square, $a = d$ will not occur, so the terms q^{-1} and $q^{-a/d}$ are different. Therefore the term with lowest exponent has coefficient a root of unity. Taking the product of all of these terms, we obtain the coefficient of the most negative power of q in $\Phi_N(j(z), j(z))$ is a root of unity. Since it is an integer, it is ± 1. This is the leading coefficient of $\Phi_N(x, x)$. □

It is now easy to prove Theorem 12. For a modular function $f(z)$ for the group $\Gamma_0(N)$, consider

$$G(x, z) = \Phi_N(x, j(z)) \sum \frac{f(\gamma_i z)}{x - j(N\gamma_i z)} = \sum_i f(\gamma_i z) \prod_{j \neq i} (x - j(N\gamma_j z))$$

where the γ_i are coset representatives for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Viewed as a polynomial in x, the coefficients are modular functions for $\mathrm{SL}_2(\mathbb{Z})$ by an argument very similar to the one given above for the modular equation. Thus they are rational functions in $j(z)$. But then there is a polynomial G' in $\mathbb{C}(y)[x]$ such that

$$G(x, z) = G'(x, j(z)) \in \mathbb{C}[x].$$

Letting $x = j(Nz)$ gives

$$G'(j(Nz), j(z)) = f(z)\frac{\partial \Phi_N}{\partial x}(j(Nz), j(z))$$

because by the product rule and choosing γ_1 to be the identity matrix

$$\frac{\partial \Phi_N}{\partial x}(j(mz), j(z)) = \prod_{j \neq 1}(j(Nz) - j(N\gamma_i z)).$$

However, the previous proposition showed that Φ_N is irreducible, hence separable, so the partial derivative is non-zero. Thus we can conclude

$$f(z) = \frac{G'(j(Nz), j(z))}{\frac{\partial \Phi_N}{\partial x}(j(Nz), j(z))}. \tag{2}$$

In fact, we can strengthen this result when $f(z)$ has rational coefficients.

Theorem 16. *Let $f(z)$ be a modular function for $\Gamma_0(N)$. If its $q-$expansion has rational coefficients then $f(z) \in \mathbb{Q}(j(z), j(Nz))$. Furthermore, if $f(z)$ is holomorphic on the upper half plane and z_0 is a point in the upper half plane for which*

$$\frac{\partial \Phi_N}{\partial X}(j(Nz_0), j(z_0)) \neq 0$$

then the denominator of this rational function is nonzero so $f(z_0) \in \mathbb{Q}(j(z_0), j(Nz_0))$.

Proof. We already know the denominator of (2) has rational coefficients by Proposition 15. To analyze the numerator, write

$$G'(j(Nz), j(z)) = \frac{P(j(Nz), j(z))}{Q(j(z))}$$

for polynomials $P(x, y)$ and $Q(x)$ with

$$P(x, y) = \sum_{j,k} a_{j,k} x^j y^k \quad \text{and} \quad Q(y) = \sum_l b_l y^l.$$

Then multiplying through by the denominator, we obtain

$$\sum_{j,k} a_{j,k} j(Nz)^j j(z)^k = f(z)\frac{\partial \Phi_N}{\partial x}(j(Nz), j(z)) \left(\sum b_l j(z)^l\right).$$

Substituting the $q-$series for $f(z)$, $j(z)$, and $j(Nz)$ and equating powers of $q^{\frac{1}{N}}$ gives a system of linear equations in the $a_{i,k}$ and b_l. The coefficients are rational since $f(z)$, $j(z)$, and $j(Nz)$ have rational $q-$expansions and the polynomial $\Phi_N(x, y)$ has rational coefficients as well. Since there is a complex solution and all of the coefficients are rational, there is a rational solution. Thus P and Q may be chosen to be rational polynomials.

The second statement follows by substituting $z = z_0$. The numerator $G'(j(Nz), j(z))$ is a polynomial in $j(z)$ and $j(Nz)$ as the coefficients of $G'(x, j(z))$ are holomorphic and invariant under $\mathrm{SL}_2(\mathbb{Z})$. By the same argument as above, we can force the coefficients to be rational. Consequently by substituting $z = z_0$ the numerator ends up in $\mathbb{Q}(j(z_0), j(Nz_0))$ and the denominator is a nonzero element of the same field. □

In practice, there is an easy way to tell when the above specialization argument will work.

Proposition 17. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K with $\mathcal{O}^\times = \{\pm 1\}$. Write $\mathcal{O} = [1, \alpha]$ and assume the for some integer s we have $s | tr_{K/\mathbb{Q}}(\alpha)$ and $\gcd(s^2, N_{K/\mathbb{Q}}(\alpha))$ is square-free. Then for any positive integer N,*

$$\frac{\partial \Phi_N}{\partial X}(j(N\alpha/s), j(\alpha/s)) \neq 0.$$

Proof. Since $\Phi_N((j(N\alpha/s), j(\alpha/s)) = 0$, it suffices to show $j(N\alpha/s)$ is not a multiple root of $\Phi_N(x, j(\alpha/s))$, which reduces to showing $j(N\alpha/s) \neq j(\sigma\alpha/s)$ for $\sigma \in C(N)$ and $\sigma \neq \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$. If this were so, the corresponding lattices would be homothetic so that

$$\lambda[1, N\alpha/s] = [d, a\alpha/s + b].$$

However, the lattices $[d, a\alpha/s + b]$ and $[1, N\alpha/s]$ have index N in $[1, \alpha/s]$, so λ has norm 1. Furthermore, $s\lambda \in s[d, a\alpha/s + b] \subset [s, \alpha]$. Writing $s\lambda = us + v\alpha$ for $u, v \in \mathbb{Z}$ and taking norms gives

$$s^2 = N(us + v\alpha) = u^2 s^2 + usv\mathrm{tr}_{K/\mathbb{Q}}(\alpha) + v^2 N_{K/\mathbb{Q}}(\alpha).$$

By the hypothesis, $s^2 | v^2 N_{K/\mathbb{Q}}(\alpha)$ and hence $s|v$. Thus $\lambda \in [1, \alpha]$. But the only units in $\mathcal{O}$ are ± 1, so the two lattices were equal. □

The modular equation also shows that the j-invariant is often an algebraic integer.

Proposition 18. *Let $\mathcal{O}$ be an order in an imaginary quadratic field, and $\mathfrak{a}$ be a proper ideal. Then $j(\mathfrak{a})$ is an algebraic integer of degree at most $h(\mathcal{O})$.*

Proof. Suppose there exists an $\alpha \in \mathcal{O}$ such that $N = N(\alpha)$ is square free and $\Phi_N(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0$. But since $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$, this implies $j(\mathfrak{a})$ is a root of $\Phi_N(x, x)$. By Proposition 15, the leading coefficient is ± 1 so $j(\mathfrak{a})$ is an algebraic integer. Furthermore, the conjugates of $j(\mathfrak{a})$ are also solutions to $\Phi_N(x, x) = 0$. The roots of this equation are $j(\sigma\mathfrak{a})$ for $\sigma \in C(N)$.[1] These take on only $h(\mathcal{O})$ values, as $\sigma\mathfrak{a}$ is a proper fractional ideal and there are only $h(\mathcal{O})$ equivalence classes of such ideals. Thus the degree of $j(\mathfrak{a})$ is at most $h(\mathcal{O})$.

Now let f be the conductor of $\mathcal{O}$, and d the discriminant of the maximal order. It is straightforward to see that $\alpha = f\frac{d+\sqrt{d}}{2}$ has the required properties. For a proof of this, and a proof that $\sigma\mathfrak{a}$ is proper, see Section 11 of Cox [7]. □

For the purposes of solving the class number one problem, additional modular functions will be crucial.

3. Other Modular Functions

The next modular function to consider is the cube root of the j function, $\gamma_2(z)$. Then we introduce Weber's three modular functions, useful in calculating $j(z)$, and study the transformation laws of these functions.

[1] Added later: this seems to be wrong. Theorem 10.23 of Cox, or Proposition 2.1 of Silverman's AEC give the correct elementary argument that the degree is at most $h(\mathcal{O})$.

3.1. **The Cube Root of the $j-$Function.**

Since the modular discriminant $\Delta(z)$ is non-vanishing on the upper half plane, it has a holomorphic cube root which can be chosen to be real valued on the positive imaginary axis. Define

$$\gamma_2(z) := 12\frac{E_4(z)}{\Delta(z)^{1/3}}. \tag{3}$$

It is a modular function as well.

Proposition 19. *We have $\gamma_2(z+1) = \zeta_3^2\gamma_2(z)$ and $\gamma_2(\frac{-1}{z}) = \gamma_2(z)$.*

Proof. Since j is a modular function for $\mathrm{SL}_2(\mathbb{Z})$, the two desired equalities hold up to third roots of unity. We know γ_2 is real on the positive imaginary axis, so picking $z = iy$ forces $\frac{-1}{z}$ to be on the imaginary axis as well. Hence $\gamma_2(\frac{-1}{z}) = \gamma_2(z)$. For the second, write $j(z) = q^{-1}h(q)$ where h is a holomorphic function on $|q| < 1$ with rational coefficients in its Taylor series about 0. Pick a cube root $u(q)$: note it has rational coefficients as well. Then $\gamma_2(z) = q^{-\frac{1}{3}}u(q)$. Evaluating $\gamma_2(z+1)$ using this gives $\gamma_2(z+1) = \zeta_3^{-1}\gamma_2(z)$. □

Using this and induction on the length of a word of $\mathrm{SL}_2(\mathbb{Z})$ in terms of

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

it follows that

$$\gamma_2(\frac{az+b}{cz+d}) = \zeta_3^{ac-ab+a^2cd-cd}\gamma_2(z).$$

For example,

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

and

$$\gamma_2(\frac{-cz-d}{az+b}) = \gamma_2\left(-\left(\frac{az+b}{cz+d}\right)^{-1}\right) = \gamma_2\left(\frac{az+b}{cz+d}\right) = \zeta_3^{ac-ab+a^2cd-cd}\gamma_2(z)$$

by induction. But

$$(-c)a - (-c)(-d) + c^2ab - ab = -ab - cd + ca(bc-1) = ac - ab + a^2cd - cd \mod 3$$

using $ad - bc = 1$. The inductive step for the matrix T is similar.

Now let

$$H := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 0 \mod 3 \quad \text{or} \quad b \equiv c \mod 3\right\}.$$

It is clear that the congruence conditions make $ac - ab + a^2cd - cd \equiv 0 \mod 3$, so γ_2 is invariant under H. A standard calculation with the $q-$series shows it is meromorphic at the cusps.

3.2. **Definitions and Basic Properties of the Weber functions.**

Weber defined several additional modular functions in terms of the Dedekind eta function. They are useful since they provide effective ways to calculate $\gamma_2(z)$. Recall that with $q = e^{2\pi iz}$, the eta function is defined as

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

This converges to a non-zero holomorphic function on the upper half plane.

Definition 20. The Weber functions $\mathfrak{f}$, $\mathfrak{f}_1$, and $\mathfrak{f}_2$ are defined to be

$$\mathfrak{f}(z) = \zeta_{48}^{-1}\frac{\eta((z+1)/2)}{\eta(z)}$$
$$\mathfrak{f}_1(z) = \frac{\eta(z/2)}{\eta(z)}$$
$$\mathfrak{f}_2(z) = \sqrt{2}\frac{\eta(2z)}{\eta(z)}$$

We get product formulas for $\mathfrak{f}$, $\mathfrak{f}_1$, and $\mathfrak{f}_2$ by canceling common factors in the definition.

Proposition 21. *The Weber functions have the following product expansions:*

$$\mathfrak{f}(z) = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2})$$
$$\mathfrak{f}_1(z) = q^{-1/48}\prod_{n=1}^{\infty}(1-q^{n-1/2})$$
$$\mathfrak{f}_2(z) = \sqrt{2}q^{1/24}\prod_{n=1}^{\infty}(1+q^{n})$$

The different functions are also dependent on each other.

Proposition 22. *We have that* $\mathfrak{f}_1(2z)\mathfrak{f}_2(z) = \sqrt{2}$ *and* $\mathfrak{f}(z)\mathfrak{f}_1(z)\mathfrak{f}_2(z) = \sqrt{2}$.

Proof. The first follows directly from the definitions. The second follows using the product expansions by showing that

$$\eta(z)\mathfrak{f}(z)\mathfrak{f}_1(z)\mathfrak{f}_2(z) = \sqrt{2}\prod_{n=1}^{\infty}(1-q^n)$$

□

The next goal is to derive a theorem relating $\gamma_2(\tau)$ with the Weber functions. It will be used in section 4 to calculate the j-invariants of the imaginary quadratic fields of class number one.

Theorem 23. *We have that*

$$\gamma_2(\tau) = \frac{\mathfrak{f}(\tau)^{24}-16}{\mathfrak{f}(\tau)^8} = \frac{\mathfrak{f}_1(\tau)^{24}+16}{\mathfrak{f}_1(\tau)^8} = \frac{\mathfrak{f}_2(\tau)^{24}+16}{f_2(\tau)^8}.$$

This will require some more work. The key is the following relation between special values of the Weierstrass $\wp$-function and other modular functions. Fix a lattice $[1, z]$. Write $e_1 = \wp(z/2)$, $e_2 = \wp(1/2)$, and $e_3 = \wp((z+1)/2)$.

Lemma 24. *With the above notation, we have that*

$$e_2 - e_1 = \pi^2\eta(z)^4\mathfrak{f}(z)^8$$
$$e_2 - e_3 = \pi^2\eta(z)^4\mathfrak{f}_1(z)^8$$
$$e_3 - e_1 = \pi^2\eta(z)^4\mathfrak{f}_2(z)^8.$$

The proof requires the Weierstrass $\sigma-$function and will be given in the next section. For now, it has several useful consequences.

Corollary 25. *The modular discriminant has a product expansion*

$$\Delta(z) = (2\pi)^{12}\eta(z)^{24} = (2\pi)^{12}q\prod_{n=1}^{\infty}(1-q^n).$$

Proof. The proof is based on the differential equation (1). The discriminant of the polynomial $4z^3 - g_2(z)x - g_3(z)$ can be expressed in terms of the coefficients and in terms of the roots. Since $\wp'$ is an odd function $\wp'(e_i) = 0$ for $i = 1, 2, 3$, and it follows that

$$\Delta(z) = g_2(z)^3 - 27g_3(z)^2 = 16(e_2 - e_1)^2(e_2 - e_3)^2(e_3 - e_1)^2.$$

Substituting and using Proposition 22 gives $(2\pi)^{12}\eta(z)^{24}$. □

It also gives an easy proof of Theorem 23.

Proof. Since the e_i are the roots of $4x^3 - g_2(z)x - g_3(z)$, we have

$$g_2(z) = -4(e_1e_2 + e_1e_2 + e_2e_3).$$

Since $e_1 + e_2 + e_2 = 0$, some algebra shows that

$$3g_2(z) = 4((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1)).$$

Using the lemma we obtain

$$3g_2(z) = 4\pi^4\eta(z)^8(\mathfrak{f}(z)^{16} - \mathfrak{f}_1(z)^8\mathfrak{f}_2(z)^8).$$

Substituting into (3) gives

$$\gamma_2(z) = \mathfrak{f}(z)^{16} - \mathfrak{f}_1(z)^8\mathfrak{f}_2(z)^8$$

Using Proposition 22 gives the first equality. The other two two follow through similar formula for g_2 in terms of the e_i. □

3.3. The Weierstrass $\sigma-$function.

The Weierstrass $\sigma-$function is less common than the Weierstrass $\wp-$function, but the same techniques can be used to analyze it. The proof of the following facts, necessary to establish Lemma 24, are given briefly here. Complete proofs are found in Lang [10].

Definition 26. For a fixed lattice $L = [1, \tau]$, define

$$\sigma(z) = z\prod_{w\in L-\{0\}}\left(1 - \frac{z}{w}\right)e^{z/w+(1/2)(z/w)^2}.$$

Its only zeros are at the lattice points and it is holomorphic. $\sigma(z)$ is an odd function, but is not quite periodic.

Proposition 27. *There exist complex numbers η_1 and η_2 depending on the lattice (unrelated to the $\eta-$function) such that*

$$\sigma(z+\tau) = -e^{\eta_1(z+\tau/2)}\sigma(z) \quad \textit{and} \quad \sigma(z+1) = -e^{\eta_2(z+1/2)}\sigma(z).$$

Furthermore, $\eta_2\tau - \eta_1 = 2\pi i$.

Proof. Take the logarithmic derivative of σ, and write it as the series

$$\zeta(z) = \frac{1}{z} + \sum_{w \in L - \{0\}} \left(\frac{1}{z-w} + \frac{1}{w} + \frac{z}{w^2} \right).$$

Differentiating it again gives $-\wp(z)$. Thus $\zeta(z+w) - \zeta(z)$ is constant for $w \in L$. Call this constant η_1 and η_2 for $w = \tau$ and $w = 1$. Then integrate and exponentiate. To evaluate the constant arising from the integration, use the fact that σ is odd and evaluate at $\tau/2$. To obtain the relation between η_2 and η_1, integrate ζ around a fundamental parallelogram like is done for the $\wp$-function. □

It is related to the more standard $\wp$-function.

Proposition 28. *For $w, z \notin L$, we have that*

$$\wp(z) - \wp(w) = -\frac{\sigma(z+w)\sigma(z-w)}{\sigma^2(z)\sigma^2(w)}.$$

Proof. Both sides are even elliptic functions in z. Compare the zeros and poles of both sides. Both have double poles at $z = 0$ and zeros at w and $-w$. Therefore they agree up to a multiplicative constant. To evaluate the constant, multiply by z^2 and take the limit as $z \to \infty$. □

In particular, this gives the following formula for the differences of the e_i, taking into account Proposition 27:

$$\begin{aligned} e_2 - e_1 &= e^{-\eta_2 \tau/2} \frac{\sigma(\frac{\tau+1}{2})^2}{(\sigma(\frac{1}{2})\sigma(\frac{\tau}{2}))^2} \\ e_2 - e_3 &= e^{\eta_2(\tau+1)/2} \frac{\sigma(\frac{\tau}{2})^2}{(\sigma(\frac{1}{2})\sigma(\frac{\tau+1}{2}))^2} \\ e_3 - e_1 &= e^{\eta_1(\tau+1)/2} \frac{\sigma(\frac{1}{2})^2}{(\sigma(\frac{\tau+1}{2})\sigma(\frac{\tau}{2}))^2}. \end{aligned}$$

There is also a product formula. As usual, let $q = e^{2\pi i z}$, but also define $q_\tau = e^{2\pi i \tau}$.

Proposition 29. *With the above notation, we have*

$$\sigma(z) = \frac{1}{2\pi i} e^{\eta_2 z^2/2} (q^{\frac{1}{2}} - q^{-\frac{1}{2}}) \prod_{n=1}^{\infty} \frac{(1 - q_\tau^n q)(1 - q_\tau^n/q)}{(1 - q_\tau^n)^2}.$$

Proof. Denote the product on the right side by $g(z)$. Consider the quotient $\frac{\sigma(z)}{g(z)}$. Using Proposition 27 and some algebra we see that the quotient is an elliptic function with respect to the lattice $[1, \tau]$. Comparing zeros we see that the quotient is holomorphic on $\mathbb{C} - L$ and also holomorphic at 0 since the order of vanishing matches. Thus $\sigma(z)$ and $g(z)$ agree up to a multiplicative constant. Let $z \to 0$ to show the constant is one. □

Finally, setting $z = \frac{1}{2}$, $z = \frac{\tau}{2}$, and $z = \frac{\tau+1}{2}$ and substituting the product formula into the formulas for $e_i - e_j$ gives Lemma 24.

3.4. **Transformation Laws for the Weber functions.** As a first step to understanding what kind of modular function the Weber functions are, we will investigate how they transform under the generators of $\mathrm{SL}_2(\mathbb{Z})$. The key fact is the transformation rule for the eta function.

Proposition 30. *The Dedekind eta function transforms as*

$$\eta(z+1) = \zeta_{24}\eta(z) \quad \eta(\frac{-1}{z}) = \sqrt{-iz}\eta(z)$$

where the branch of the square root is chosen so it is defined and positive on the positive imaginary axis.

Proof. This is another standard fact. It is often deduced from the transformation properties of the Eisenstein series of weight 2 by logarithmic differentiation. However, since the product formula for $\Delta(z)$ has already been proven using the Weierstrass σ-function, there is a much easier proof. Using Corollary 25, we see that

$$\eta\left(\frac{-1}{z}\right)^{24} = z^{12}\eta(z)^{24}$$

as $\Delta(z)$ is a modular form for $\mathrm{SL}_2(\mathbb{Z})$ of weight 12. Taking 24th roots gives that

$$\eta(\frac{-1}{z}) = \epsilon\sqrt{-iz}\eta(z).$$

The constant $\epsilon = 1$ since $\eta(z)$ is real on the positive imaginary axis. The fact that $\eta(z+1) = \zeta_{24}\eta(z)$ follows directly from the definition as a product in q. □

Since the Weber functions are defined in terms of $\eta(z)$, the following transformation laws for the Weber functions follow immediately.

Proposition 31. *We have that*

$$\mathfrak{f}(z+1) = \zeta_{48}^{-1}\mathfrak{f}_1(z)$$
$$\mathfrak{f}_1(z+1) = \zeta_{48}^{-1}\mathfrak{f}(z)$$
$$\mathfrak{f}_2(z+1) = \zeta_{24}\mathfrak{f}_2(z)$$

and also that

$$\mathfrak{f}(\frac{-1}{z}) = \mathfrak{f}(z)$$
$$\mathfrak{f}_1(\frac{-1}{z}) = \mathfrak{f}_2(z)$$
$$\mathfrak{f}_2(\frac{-1}{z}) = \mathfrak{f}_1(z).$$

These can be pieced together to show that powers of the Weber functions are modular functions for congruence subgroups. There are two approaches. The first is to use induction on the word length in generators of the congruence subgroup with the above Proposition. For example:

Proposition 32. $\mathfrak{f}^6$ *is a modular function for the group*

$$H' := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : b \equiv c \equiv 0 \mod 8\}$$

Proof. This is similar to the proof that γ_2 is a modular functions for the congruence subgroup H in Section 3.1, so only a sketch will be given here. Since $\mathfrak{f}(z)^6 = \zeta_8 \mathfrak{f}_1(z+1)^6$, we will prove that $\mathfrak{f}_1^6$ is invariant under $\Gamma(8)$ and then conjugate. The relevant formula, from Section 12 of Cox [7], is that

$$\mathfrak{f}_1(\gamma z)^6 = i^{-ac-(1/2)bd+(1/2)b^2c}\mathfrak{f}_1(z)^6 \quad \text{for} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, b \equiv 0 \mod 2.$$

Cox shows that the matrices $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $V = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ generate the group of such matrices. Then using Proposition 31 to compute $\mathfrak{f}_1(U\gamma z)^6$ and $\mathfrak{f}_1(V\gamma z)$ and induction establishes this transformation rule. Taking the appropriate congruences on $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ shows $\mathfrak{f}_1^6$ is invariant under $\Gamma(8)$. To check it is meromorphic at the cusps, use the same technique as for γ_2 using $q-$series. □

The alternative is to write down a general transformation law for the η function. It is even more complicated than the above transformation law for $\mathfrak{f}_1$, but can be proven by induction in exactly the same way. The following version comes from Schertz [12]. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and multiply by -1 if necessary so $c > 0$ or $c = 0$ and $d > 0$. Then

$$\eta(\gamma z) = \epsilon(M)\sqrt{cz+d}\,\eta(z)$$

where

$$\epsilon(\gamma) = \begin{cases} \left(\frac{a}{c}\right)\zeta_{24}^{ab+2ac-3c+cd(1-a^2)} & \text{if } c \equiv 1 \mod 2 \\ \left(\frac{c}{|a|}\right)\zeta_{24}^{ab-ac+3a-3+cd(1-a^2)} & \text{if } a \equiv 1 \mod 2, c \neq 0 \\ \zeta_{24}^{b} & \text{if } c = 0 \end{cases}$$

It is simple to use this to analyze the Weber functions. For example, we obtain the following.

Proposition 33. *The function $\mathfrak{f}_2(z)$ is a modular function for $\Gamma(24)$.*

Proof. By the definition of $\mathfrak{f}_2(z)$,

$$\mathfrak{f}_2(\gamma z) = \sqrt{2}\frac{\eta(2\gamma z)}{\eta(\gamma z)}.$$

Using the above transformation law for $\eta(z)$ gives something quite complicated. However, if $a \equiv d \equiv 1 \mod 24$ and $b \equiv c \equiv 0 \mod 24$ and $c \neq 0$, the exponents of the twenty-fourth root of unity is a multiple of 24. Thus we are left with

$$\sqrt{2}\frac{\left(\frac{c}{|a|}\right)\eta(2z)}{\left(\frac{c/2}{|a|}\right)\eta(z)}.$$

But as $|a| = \pm 1 \mod 8$, $\left(\frac{2}{|a|}\right) = 1$. Thus

$$\mathfrak{f}_2(\gamma z) = \mathfrak{f}_2(z).$$

This does not cover the case when $c = 0$, but that obviously follows from the third part of the definition of $\epsilon(\gamma)$. The standard argument with $q-$series shows it is meromorphic at the cusps of $\Gamma(24)$. □

4. Calculation of $j-$invariants for Imaginary Quadratic Fields of Class Number 1

Later sections will give, following Heegner and Serre, a complete list of the $j-$invariants of class number one fields of the form $\mathbb{Q}(\sqrt{-p})$ with the prime $p \equiv 3 \mod 8$ and $p > 7$. To show that the known imaginary quadratic fields $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, and $\mathbb{Q}(\sqrt{-163})$ exhaust all fields of this form, it suffices to show their j-invariants match the list as there may be only one ring of integers with a given $j-$invariant. In this section we will calculate these $j-$invariants following the approach outlined in Cox, Section 12.C [7]. The key tool is the formulas for γ_2 in terms of the other Weber functions. We will estimate those functions, and then use the fact that $\gamma_2(\frac{3+\sqrt{-p}}{2})$ is an integer when the class number is one.

Let $\tau_0 = \frac{3+\sqrt{-p}}{2}$. From Proposition 22, we know that

$$\mathfrak{f}_2(\tau_0) = \frac{\sqrt{2}}{\mathfrak{f}_1(2\tau_0)}$$

and hence using the transformation rules in Proposition 31 that

$$\mathfrak{f}_1(2\tau_0) = \mathfrak{f}_1(3+\sqrt{-p}) = \zeta_{48}^{-1}\mathfrak{f}(2+\sqrt{-p}) = \zeta_{48}^{-2}\mathfrak{f}_1(1+\sqrt{-p}) = \zeta_{48}^{-3}\mathfrak{f}(\sqrt{-p}).$$

Therefore $\mathfrak{f}_2(\tau_0) = \frac{\sqrt{2}\zeta_{16}}{\mathfrak{f}(\sqrt{-p})}$, and using Proposition 23 we conclude

$$\gamma_2(\tau_0) = \mathfrak{f}_2(\sqrt{-p})^{16} + \frac{16}{\mathfrak{f}_2(\sqrt{-p})^8} = \frac{256}{\mathfrak{f}(\sqrt{-p})^{16}} - \mathfrak{f}(\sqrt{-p})^8. \tag{4}$$

The next step is to estimate $\mathfrak{f}(\sqrt{-p})$ using the product formula in Proposition 21. Letting $q = e^{2\pi i\sqrt{-p}} = e^{-2\pi\sqrt{p}} < e^{-6\pi}$ and using the estimate $1+q < e^q$, we obtain

$$\mathfrak{f}(\sqrt{-p}) = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2}) < q^{(-1/48)}\prod_{n=1}^{\infty}e^{q^{n-1/2}}.$$

Summing the series in the exponent and using $q \le e^{-6\pi}$ shows that

$$f(\sqrt{-p}) \le q^{-1/48}e^{\frac{q^{1/2}}{1-q}} \le q^{-1/48}e^{\frac{q^{1/2}}{1-e^{-6\pi}}} \le q^{-1/48}e^{1.0001q^{\frac{1}{2}}}$$

On the other hand, the inequality

$$q^{-1/48} < \mathfrak{f}(\sqrt{-p})$$

follows immediately as $q > 0$. These two inequalities and (4) give the following bounds on $\gamma_2(\tau_0)$:

$$256q^{1/3}e^{-16.0016q} - q^{-1/6}e^{8.0008q} \le \gamma_2(\tau_0) \le 256q^{1/3} - q^{-1/6} \tag{5}$$

Let the difference between these bounds be E, so

$$E = 256q^{1/3} + q^{-1/6}e^{8.0008q^{\frac{1}{2}}} - q^{-1/6} - 256q^{1/3}e^{-16.0016q^{\frac{1}{2}}} = 256q^{1/3}(1-e^{16.0016q^{\frac{1}{2}}}) - q^{-1/6}(1-e^{8.0008q^{\frac{1}{2}}})$$

For $0 < x < 1$, we know that $1 - e^{-x} \le \frac{x}{1-x}$, so this can be bounded by

$$E \le 256q^{1/3}\frac{16.0016q^{\frac{1}{2}}}{1-16.0016q^{\frac{1}{2}}} + q^{-1/6}(e^{8.0008q^{\frac{1}{2}}} - 1).$$

But this is less than 1/2 for $q = e^{-2\pi\sqrt{p}}$ for any of the p in our list. Therefore any integer satisfying the inequalities (5) must equal $\gamma_2(\tau_0)$. This is enough to compute Table 1.

TABLE 1. $j-$invariants of Imaginary Quadratic Fields of Class Number 1

	$\gamma_2(\frac{3+\sqrt{-p}}{2})$	$j(\frac{3+\sqrt{-p}}{2}) = \gamma_2^3(\tau_0)$
$\mathbb{Q}(\sqrt{-11})$	-2^5	-32^3
$\mathbb{Q}(\sqrt{-19})$	$-2^5 \cdot 3$	-96^3
$\mathbb{Q}(\sqrt{-43})$	$-2^6 \cdot 3 \cdot 5$	-960^3
$\mathbb{Q}(\sqrt{-67})$	$-2^5 \cdot 3 \cdot 5 \cdot 11$	-5280^3
$\mathbb{Q}(\sqrt{-163})$	$-2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29$	-640320^3

5. Modular Functions and Class Fields

Heegner used results due to Weber about when modular functions generate the ring class field of an order in an imaginary quadratic field. Since Weber was working before the development of class field theory, they were phrased in other ways. The solution to the class number one problem is in fact much more elementary than the use of class fields would suggest. Parts of both approaches will be discussed below.

Theorem 34 (First Main Theorem of Complex Multiplication)**.** *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a}$ be a proper fractional $\mathcal{O}-$ideal. The $j-$invariant $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}$.*

This is Theorem 11.1 of Cox [7]. The proof is not simple, and relies on the Chebotarev Density Theorem. In order to focus on the class number one problem, we will not prove the general version of this theorem. Instead, following an observation by Stark [17] there is an elementary argument that gives enough information for the application to the class number one problem but uses nothing more than the class equation.

Proposition 35. *Let p be a prime with $p \equiv 3 \mod 8$. Suppose $h(p) = 1$. Then $j(\frac{-3+\sqrt{-p}}{2})$ is rational and $K(j(\sqrt{-p}))$ is a degree 3 extension of K for large enough p.*

Proof. If $h(-p) = 1$, then by Proposition 3 it follows that $h(-4p) = 3$. Let $K = \mathbb{Q}(\sqrt{-p})$ and $\tau_0 = \frac{-3+\sqrt{-p}}{2}$. Then using Proposition 18 we know $[K(j(\sqrt{-p})) : K] \leq 3$ and $[K(j(\tau_0)) : K] \leq 1$ and both $j-$invariants are algebraic integers. Since$j(\tau_0)$ is real, it must be rational. To show $j(\sqrt{-p})$ generates a degree 3 extension over $\mathbb{Q}$, it suffices to show that it is not rational or quadratic.

Looking at the modular equation for $m = 2$, we see that

$$\Phi_2(x, \tau_0) = (x - j(\tau_0))(x - j(\tau_1))(x - j(\tau_2))$$

where $\tau_i = \sigma_i \tau_0$ and $\sigma_1, \sigma_2, \sigma_3$ are the elements of $C(2)$:

$$\sigma_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}.$$

Thus

$$\Phi_2(x, \tau_0) = \left(x - j(\sqrt{-p})\right)\left(x - j\left(\frac{-3+\sqrt{-p}}{4}\right)\right)\left(x - j\left(\frac{-1+\sqrt{-p}}{4}\right)\right).$$

Now both $\frac{1+\sqrt{-p}}{4}$ and $\frac{-1+\sqrt{-p}}{4}$ lie in the interior of the usual fundamental domain provided $p > 16$. In particular $j(\frac{-3+\sqrt{-p}}{4}) = j(\frac{1+\sqrt{-p}}{4})$ and $j(\frac{-1+\sqrt{-p}}{4})$ are not real, as the only points in the interior of the fundamental domain that are real are those with real part 0.

We know that $\Phi_2(j(\sqrt{-p}), \tau_0) = 0$ by Proposition 15 since $j(2\tau_0) = j(-3 + \sqrt{-p}) = j(\sqrt{-p})$. If $j(\sqrt{-p})$ is rational or quadratic, $\Phi_2(x, \tau_0)$ will have a rational root. The above argument shows that root must be $j(\sqrt{-p})$, so we only need to rule out the case that $j(\sqrt{-p})$ is a rational integer. However, if we set $q = e^{2\pi i \tau_0}$ then using the q-series expansion for j in Proposition 9 shows

$$\begin{aligned} j(\tau_0) &= 1/q + 744 + 196884q + 21493760q^2 + O(q^3) \\ j(\sqrt{-p}) &= 1/q^2 + 744 + 196884q^2 + O(q^4). \end{aligned}$$

Squaring $j(\tau_0)$ and canceling low order terms shows

$$j(\tau_0)^2 - 1488j(\tau_0) + 160512 - j(\sqrt{-p}) = 42987520q + O(q^2).$$

By hypothesis the left side is a rational integer. The right side can be bounded between 0 and 1 when q is small enough using a technique similar to the one used in section 4. Stark's analysis showed $p > 60$ is sufficient. There are no integers between 0 and 1, so $j(\sqrt{-p})$ must generate a cubic extension of K. □

The cube root of the $j-$function usually generates this field as well.

Theorem 36. *Let $\mathcal{O} = [1, \tau_0]$ be an order of discriminant D in the imaginary quadratic field K. If $3 \not| D$, then $\gamma_2(\tau_0)$ is an algebraic integer and $K(\gamma_2(\tau_0))$ is the ring class field of $\mathcal{O}$.*

This can be deduced with some work using the main theorem of complex multiplication, as is done in Section 12 of Cox [7]. To focus on the class number one problem, we will omit it. Actually, all we need is that $\gamma_2(\tau_0) \in \mathbb{Z}$ when $\mathcal{O}$ is the ring of integers for $\mathbb{Q}(\sqrt{-p})$ with class number one and $p > 7$. An independent proof of this will be given in Section 9.2 using the modular curve $X_{ns}^{+}(3)$.

There are also times when the ring class field can be generated using Weber's functions.

Theorem 37. *Let $m \equiv 3 \mod 4$, and $\mathcal{O} = [1, \sqrt{-m}]$ be an order in $K = \mathbb{Q}(\sqrt{-m})$. Then $\mathfrak{f}(\sqrt{-m})^2$ is an algebraic integer and $K(\mathfrak{f}(\sqrt{-m})^2)$ is the ring class field of $\mathcal{O}$.*

Weber gave an incomplete proof [18], which is part of the reason Heegner's proof of the class number one problem was thought to be flawed. Stark fixed it [17], but the proof, though elementary, is integrated with the rest of Weber's work. A modern proof is given in section 7 of Birch [4]. Here we will follow the more elementary presentation given by Cox [7]. It requires the full force of Theorem 34 and one additional fact. Two proofs of this fact can be found in Lang [10]: one uses the reduction of elliptic curves, the other is more analytic in nature.

Theorem 38. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let L be the ring class field of $\mathcal{O}$. Given proper fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$, define*

$$\sigma_{\mathfrak{a}}(j(\mathfrak{b})) := j(\overline{\mathfrak{a}}\mathfrak{b}).$$

Then $\sigma_{\mathfrak{a}}$ is a well-defined element of $Gal(L/K)$ and $\mathfrak{a} \to \sigma_{\mathfrak{a}}$ induces an isomorphism between $C(\mathcal{O})$ and $\mathrm{Gal}(L/K)$.

The key to proving Theorem 37 is to show that $\mathfrak{f}(\sqrt{-m})^6 \in L$. Let L be the ring class field of $\mathcal{O} = [1, \sqrt{-m}]$, which we know to be $K(j(\sqrt{-m})$. The equation

$$\mathfrak{f}(\sqrt{-m})^{24} - \mathfrak{f}(\sqrt{-m})^8\gamma_2(\sqrt{-m}) - 16 = 0$$

from Proposition 23 implies that if $\mathfrak{f}(\sqrt{-m})^6$ is in L, then as $\gamma_2(\sqrt{-m}) \in L$ by Theorem 36 we know that $\mathfrak{f}(\sqrt{-m})^8 \in L$ is as well. Then $\mathfrak{f}(\sqrt{-m})^8/\mathfrak{f}(\sqrt{-m})^6 = \mathfrak{f}(\sqrt{-m})^2$ is in L. Using the above equation again shows $j(\sqrt{-m}) \in K(\mathfrak{f}(\sqrt{-m})^2)$, so the class field $L = K(\mathfrak{f}(\sqrt{-m})^2)$.

We will first show that $\mathfrak{f}(\sqrt{-m})^6$ is in the ring class field L' for the order $[1, 8\sqrt{-m}]$.

By Proposition 32, $\mathfrak{f}(\dfrac{az+b}{cz+d})^6 = \mathfrak{f}(z)^6$ when $b \equiv c \equiv 0 \mod 8$. Therefore for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(64), \quad \mathfrak{f}\left(8\frac{az+b}{cz+d}\right)^6 = \mathfrak{f}\left(\frac{a(8z)+(8b)}{(c/8)(8z)+d}\right)^6 = \mathfrak{f}(8z)^6$$

so $\mathfrak{f}(8z)^6$ is invariant under $\Gamma_0(64)$. It is also meromorphic at the cusps. To see this, use Lemma 11 to write $8\gamma z = \tilde{\gamma}\sigma z$ where $\tilde{\gamma} \in \mathrm{SL}_2(\mathbb{Z})$ and $\sigma \in C(8)$. Then using Proposition 31, writing $\tilde{\gamma}$ in terms of the generators for $\mathrm{SL}_2(\mathbb{Z})$ we get that $\mathfrak{f}(8\gamma z) = \mathfrak{f}(\tilde{\gamma}\sigma z)$ is a root of unity times $\mathfrak{f}(\sigma z)$, $\mathfrak{f}_1(\sigma z)$, or $\mathfrak{f}_2(\sigma z)$. But $e^{2\pi i \sigma z}$ is a root of unity times a power of $q^{\frac{1}{8}}$, so the product formulas for the Weber functions imply the $q-$expansion of $\mathfrak{f}(8\gamma z)$ involves only finitely many negative powers of $q^{\frac{1}{8}}$. Hence $\mathfrak{f}(8z)^6$ is a modular function for $\Gamma_0(64)$.

This is important because we know $\mathfrak{f}(8z)^6$ is a rational function in $j(64z)$, $j(z)$ by Theorem 16. We want to specialize at $z = \sqrt{-m}/8$. Proposition 17 with $m = 64$, $s = 8$ shows that $\mathfrak{f}(\sqrt{-m})^6$ lies in the field $\mathbb{Q}(j(8\sqrt{-m}), j(\sqrt{-m}/8))$. Write

$$\mathfrak{f}(\sqrt{-m})^6 = R(j(8\sqrt{-m}), j(\sqrt{-m}/8))$$

where R is a rational function with coefficients in $\mathbb{Q}$. Since $[1, 8\sqrt{-m}]$ and $[1, \sqrt{-m}/8]$ are proper fractional ideals in the order $\mathcal{O}' = [1, 8\sqrt{-m}]$, the main theorem of complex multiplication implies $\mathfrak{f}(\sqrt{-m})^6$ lies in the ring class field L'.

Finally consider the Galois extension L'/L. By class field theory, the Galois group is the kernel of the map $C(\mathcal{O}') \to C(\mathcal{O})$. It is straightforward to check when ideals in imaginary quadratic orders are principal, so a routine calculation shows that the ideals $\mathfrak{a} = [8, 2+\sqrt{-m}]$ and $\mathfrak{b} = [8, \sqrt{-m}]$ generate the kernel, which is the group $C_4 \times C_2$ of order 8. By Theorem 38, $\sigma_{\mathfrak{a}}$ and $\sigma_{\mathfrak{b}}$ generate the Galois group. To show that $\mathfrak{f}(\sqrt{-m})^6$ actually lies in L, it suffices to show that

$$\sigma_{\mathfrak{a}} R(j(8\sqrt{-m}), j(\sqrt{-m}/8)) = R(j(8\sqrt{-m}), j(\sqrt{-m}/8))$$
$$\sigma_b R(j(8\sqrt{-m}), j(\sqrt{-m}/8)) = R(j(8\sqrt{-m}), j(\sqrt{-m}/8)).$$

But using the definition of $\sigma_{\mathfrak{a}}$ and a direct calculation with the fractional ideals we have

$$R(j(\bar{\mathfrak{a}}[1, 8\sqrt{-m}]), j(\bar{\mathfrak{a}}[8, \sqrt{-m}])) = R(j([4, 3+2\sqrt{-m}]), j(8, 6+\sqrt{-m}))$$
$$R(j(\bar{\mathfrak{b}}[1, 8\sqrt{-m}]), j(\bar{\mathfrak{b}}[8, \sqrt{-m}])) = R(j([1, 8\sqrt{-m}]), j([8, \sqrt{-m}])).$$

Note that in multiplying the fractional ideals we need the fact that $m \equiv 3 \mod 4$. However, if $\gamma_1 = \begin{pmatrix} 2 & 11 \\ 1 & 6 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, a direct calculation also shows that

$$\mathfrak{f}(\gamma_1\sqrt{-m})^6 = R(j([4, 3+2\sqrt{-m}]), j(8, 6+\sqrt{-m}))$$
$$\mathfrak{f}(\gamma_2\sqrt{-m})^6 = R(j(1, 8\sqrt{-m}), j(8, \sqrt{-m})).$$

Writing γ_1 and γ_2 in terms of the generators for $\mathrm{SL}_2(\mathbb{Z})$ and using Proposition 31 shows γ_1 and γ_2 fix $\mathfrak{f}(z)^6$. All of this combines to show that $\mathfrak{f}(\sqrt{-m})^6$ is fixed by $\sigma_{\mathfrak{a}}$ and $\sigma_{\mathfrak{b}}$ and hence $f(\sqrt{-m})^6$ lies in L. Therefore $f(\sqrt{-m})^2$ generates the ring class field as claimed. □

6. Heegner's Approach to the Class Number One Problem

Heegner started by using elementary results to find all imaginary quadratic fields $\mathbb{Q}(\sqrt{-n})$ with class number one except when n is a prime congruent to 3 modulo 8. He then used results about the Weber functions to come up with two expressions for the minimal polynomial of the algebraic integer $-\mathfrak{f}_2\left(\frac{3+\sqrt{-p}}{2}\right)^8$. One of the coefficients is the integer $\gamma_2(\frac{3+\sqrt{-p}}{2})$. Equating coefficients gives a system of Diophantine equations with a finite number of solutions. This gives a finite list $j-$invariants for imaginary quadratic fields of class number one.

All orders in imaginary quadratic fields with even discriminant and class number one have already been determined by elementary methods (Theorem 4). Furthermore, we know that if n has two or more odd prime factors, the class number is a multiple of two (Theorem 5). Finally, if $p \equiv 7 \mod 8$ then by Proposition 3

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

and hence the list in Theorem 4 implies that p is seven[2]. Therefore we may assume that $p \equiv 3 \mod 8$. Note that in this case $h(-4p) = 2h(-p)\left(1+\frac{1}{2}\right) = 3$.

Let $K = \mathbb{Q}(\sqrt{-p})$. By Proposition 35, $K(j(\sqrt{-p}))$ is a degree 3 extension of K. As $j(\sqrt{-p})$ is real, $\mathbb{Q}(j(\sqrt{-p}))$ is a degree 3 extension of $\mathbb{Q}$. But Weber gave an alternate description for the ring class field. By Theorem 37, $K(\mathfrak{f}(\sqrt{-p})^2) = K(j(\sqrt{-p}))$. Since $\mathfrak{f}(\sqrt{-p})$ is real $\mathbb{Q}(\mathfrak{f}(\sqrt{-p})^2)$ is also a cubic extension of $\mathbb{Q}$.

Now let $\tau_0 = \dfrac{3+\sqrt{-p}}{2}$, and set $\alpha = \zeta_8^{-1}\mathfrak{f}_2(\tau_0)^2$. By Proposition 31,

$$\mathfrak{f}_1(2\tau_0) = \mathfrak{f}_1(3+\sqrt{-p}) = \zeta_{16}^{-1}\mathfrak{f}(\sqrt{-p}).$$

Furthermore, by Proposition 22 we know

$$\alpha = \zeta_8^{-1}\mathfrak{f}_2(\tau_0)^2 = \frac{2}{\zeta_8\mathfrak{f}_1(2\tau_0)^2} = \frac{2}{\mathfrak{f}(\sqrt{-p})^2}$$

and so α and α^4 generate the cubic extension $\mathbb{Q}(\mathfrak{f}(\sqrt{-p}))$. In addition, by Theorem 23

$$\gamma_2(\tau_0) = \frac{\mathfrak{f}_2(\tau_0)^{24}+16}{\mathfrak{f}_2(\tau_0)^8} \tag{6}$$

so it follows that α is an algebraic integer. Heegner's insight is that since both α and α^4 are algebraic integers in $\mathbb{Q}(\mathfrak{f}(\sqrt{-p}))$, there are severe restrictions on their minimal polynomials.

On the one hand, we know that $\gamma_2(\tau_0)$ is an integer as it generates the ring class field for $[1,\tau_0]$ in $\mathbb{Q}(\sqrt{-p})$ by Theorem 36, which was assumed to have class number 1. Then (6) implies that $\alpha^4 = -\mathfrak{f}_2(\tau_0)^8$ is a root of the cubic equation

$$x^3 - \gamma_2(\tau_0)x - 16 = 0. \tag{7}$$

On the other hand, α is the root of some cubic equation

$$x^3 + ax^2 + bx + c = 0$$

where $a, b, c \in \mathbb{Z}$ as α is an algebraic integer. The equation for α^4 puts strong constraints on a, b, and c. Separating the even and odd degree terms and squaring, we get a monic cubic

[2] This is the most important place where the theory of orders and not just rings of integers is used.

with α^2 as a root:

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

Write $e = 2b - a^2$, $f = b^2 - 2ac$, and $g = -c^2$. Separating the even and odd degree terms and squaring again, we get a monic cubic with α^4 as a root:

$$x^3 + (2f - e^2)x^2 + (f^2 - 2eg)x - g^2 = 0$$

Since the minimal polynomial for α^4 is unique, this is the same as the polynomial (7). This gives the system of equations

$$\begin{aligned} 2f - e^2 &= 0 \\ f^2 - 2eg &= -\gamma_2(\tau_0) \\ g^2 &= 16. \end{aligned}$$

Thus $g = \pm 4$. Since $g = -c^2$, $g = -4$ and $c = \pm 2$. We may assume $c = 2$, as replacing α by $-\alpha$ flips the signs of a and c. Therefore solving for $\gamma_2(\tau_0)$ in terms of a and b gives

$$\gamma_2(\tau_0) = -f^2 - 8e = -(b^2 - 4a)^2 - 8(2b - a^2).$$

There will be only a finite number of choices for a and b, which will then give all possible values of $\gamma_2(\tau_0)$.

Since $2f - e^2 = 0$, we have that

$$2(b^2 - 4a) = (2b - a^2)^2 \tag{8}$$

from which it follows that a and hence b are even integers. Let the integers x and y be given by $x = -a/2$, $y = (b - a^2)/2$. Then

$$2b^2 - 8a = 2(b^2 - 4a) = (2b - a^2)^2 = (b + 2y)^2 = b^2 + 4yb + 4y^2$$

Solving for y^2 in terms of a and b gives

$$y^2 = \frac{-b^2 - 8a + 2a^2 b}{4}.$$

On the other hand, solving (8) for a^4 shows that

$$2x(x^3 + 1) = a^4/8 - a = \frac{2b^2 - 8a - 4b^2 + 4ba^2}{8} - a = \frac{-b^2 - 8a + 2a^2 b}{4}.$$

Thus x and y are solutions to the Diophantine equation

$$2x(x^3 + 1) = y^2. \tag{9}$$

This Diophantine equation can be solved using elementary methods. It has a finite number of solutions.

Proposition 39. *The only solutions to* (9) *are* $(x, y) = (0, 0), (-1, 0), (1, \pm 2)$, *and* $(2, \pm 6)$.

We will prove this at the end of this section. For now, note that these correspond to $(a, b) = (0, 0), (2, 4), (-2, 8), (-2, 0), (-4, 28)$ and $(-4, 4)$.

Using these solutions and the fact that $\gamma_2(\tau_0) = -(b^2 - 4a)^2 - 8(2b - a^2)$ gives $\gamma_2(\tau_0) = 0, -96, -5280, -32, -640320$, and -960. All of these are accounted for in the list of known class number one fields presented in Table 1. Since there is at most one imaginary quadratic field with given $j-$invariant by Corollary 8, our list of imaginary quadratic fields with class number 1 is complete.

It is worth noting that nothing in this proof is particularly deep. Although phrased in terms of ring class fields, the results in Section 5 can all be proven using much more elementary methods at the expense of additional work. For example, we showed how to replace Theorem 34 with the more elementary Proposition 35. Stark remarks that the class number one problem could have been solved up to 60 years before he did using Weber's work: nothing more modern is required [17].

Proof. To solve $2x(x^3+1) = y^2$, we will reduce it to one of four subsidiary equations solved in Lemma 40 by standard techniques. We may deal with $x = 0, -1$ separately. Otherwise x and x^3+1 are relatively prime so $\pm(x^3+1)$ is a square or twice a square. Thus $x^3+1 = \pm\{1, 2\}z^2$ for some integer z. These give three of the equations in the Lemma. For $x^3 + 1 = 2z^2$, we need additional information. Substituting into the original equation gives $4xz^2 = y^2$, so we see x is a perfect square as well. Writing $w^2 = x$ gives the third equation in Lemma 40. Taking the solutions to those equations and solving for y gives the list in the proposition. □

Lemma 40. *The subsidiary Diophantine equations have the following integral solutions:*

1. *The equation $x^3 + 1 = z^2$ has solutions $(x, z) = (-1, 0)$, $(0, \pm 1)$, $(2, \pm 3)$.*
2. *The equation $x^3 + 1 = -z^2$ has solutions $(x, z) = (-1, 0)$.*
3. *The equation $w^6 + 1 = 2z^2$ has solutions $(w^2, z) = (1, \pm 1)$.*
4. *The equation $x^3 + 1 = -2z^2$ has solutions $(x, z) = (-1, 0)$.*

These can all be proven by elementary methods. The first is the most involved. It was solved by Euler. The strategy is first to show there are no positive integers b and c with $b \neq c$, $3 \nmid c$, and $bc(c^2 - 3bc + 3b^2)$ a perfect square using infinite descent. If $x = \frac{a}{b}$ is a solution to $x^3 + 1 = z^2$, then set $a + b = c$ and note that $b(a^3 + b^3) = bc(c^2 - 3bc + 3b^2)$ is a perfect square. Using the previous result, it is not hard to deduce we have all solutions. More details are found at the end of Section 12 of Cox [7].

The remaining equations can be solved with the standard technique of factoring over a ring of integers with class number one. For the second use $\mathbb{Z}[i]$, the third use $\mathbb{Z}[\omega]$, and the fourth $\mathbb{Z}[\sqrt{-2}]$.

There are also general methods to solve equations of this form. They are examples of Mordell's equation. Details on how to solve them are given by Hemer̃citehemer. Even more generally, there are methods to find all integral points on arbitrary elliptic curves. Such an algorithm is implemented in Sage [11] and quickly finds that the only integral points are those listed here. The algorithm Sage uses to find the integral points is described in Cohen [6]. The basic idea is to bound the size of the coordinates of the integral points, then cleverly cut down the search space so a brute force search is feasible. For the examples here, this takes under a second. It is interesting that the bounds come from generalizations of Baker's work on lower bounds for logarithms, which gave one of the original solutions to the class number one problem.

7. The Modular Curve $H\backslash X(N)$ as an Algebraic Curve

Serre approaches the class number one problem much more geometrically than Heegner appears to. We will construct a curve $X_{ns}^{+}(n)$ on which special correspond to imaginary quadratic fields of class number one. For small values of n, it is possible to find such points and hence find all imaginary quadratic fields of class number one. The curve $X_{ns}^{+}(n)$ will be a quotient of the parameter space of elliptic curves with a basis for the n-torsion. We study these quotients in general and find out when they are algebraic curves defined over $\mathbb{Q}$.[3]

Consider the set of elliptic curves E over $\mathbb{C}$ with an isomorphism $E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. The same technique used to show $X_0(N)$ is a Riemann surface shows this is as well (see for example Chapter 2 of Diamond and Shurman [8]). It can be compactified by adding in the cusps to obtain a compact Riemann surface $X(N)$. It is known as the modular curve of elliptic curves with full level N structure. We are interested in when this a rational algebraic curve. The approach adapts Chapter 7 of Diamond and Shurman [8] to the curve $X(N)$. However, it is essential to remember that the notation $X(N)$ in Diamond and Shurman is something different. It refers to $\Gamma(N)\backslash\mathcal{H}^*$, the parameter space for elliptic curves with two points P and Q that generate the N torsion and also have specified Weil pairing. The notation $X'(N)$ will be used here for this parameter space.

First, note that $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(N)$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ sending a pair $(E,(P,Q))$ to $(E,(aP+bQ,cP+dQ))$. This preserves the fibres of the projection map $X(N) \to X(1)$ sending $(E,(P,Q))$ to E.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let $e_N(P,Q)$ denotes the Weil pairing of P and Q. Then by the bi-linearity of the pairing, $e_N(aP+bQ,cP+dQ) = e_N(P,Q)^{\det\gamma}$. The Weil pairing is a continuous map from $X(N)$ to the set of primitive Nth roots of unity, so the pairs with specified Weil pairing are connected components of $X(N)$. Each of these components is a copy of $X'(N)$.

Since $X(N)$ has multiple connected components, it is easier to do algebraic geometry on a quotient with only one connected component. If the determinant map sends $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ onto $(\mathbb{Z}/N\mathbb{Z})^\times$, the quotient has only one component. Note that $H\backslash X(N)$ will then equal $\Gamma_H\backslash X'(N)$ where $\Gamma_H = H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Alternately, this can be written as $\Gamma'_H\backslash\mathcal{H}^*$ where Γ'_H are the elements of $\mathrm{SL}_2(\mathbb{Z})$ that reduce modulo N to Γ_H.

In summary, we have the following theorem.

Theorem 41. *$X(N)$ has $\phi(N)$ connected components, each isomorphic to $X'(N) = \Gamma(N)\backslash\mathcal{H}^*$. If H is a subgroup of $\mathrm{GL}_2(N)$ such that $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, we have $H\backslash X(N) = \Gamma_H\backslash X'(N)$ where $\Gamma_H = H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

The next step is to determine the field of meromorphic functions on $X'(N)$ and the group $\mathrm{Gal}(\mathbb{C}(X'(N))/\mathbb{C}(X(1)))$. Let E_j be the universal elliptic curve

$$E_j : y^2 = 4x^4 - \frac{27j}{j-1728}x - \frac{27j}{j-1728}.$$

The name comes from the fact that for $j \neq 0, 1728$ it specializes to an elliptic curve with j-invariant j.

Recall that for a lattice $\Lambda = [\tau, 1]$ there is an identification $C/\Lambda \to E$ sending $z \to (\wp(z), \wp'(z))$ where E is the elliptic curve defined by

$$E : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau).$$

[3] Added later: this section is sloppy about the issue of whether a rational form of a modular curve over $\mathbb{C}$ actually represents the moduli problem. The difficulty is that there may be multiple curves over $\mathbb{Q}$ which become isomorphic over $\mathbb{C}$ to a modular curve. Simply finding a rational defining equation is not enough.

It will be convenient to rescale so that we map $z \to \left(\frac{g_2(\tau)}{g_3(\tau)}\wp(z), \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{\frac{3}{2}}\wp'(z)\right)$ and end up on the curve

$$E_{j(\tau)} : y^2 = 4x^3 - \frac{g_2(\tau)^3}{g_3(\tau)^2}x - \frac{g_2(\tau)^3}{g_3(\tau)^2}.$$

Since $\frac{g_2(\tau)^3}{g_3(\tau)^2} = \frac{27g_2(\tau)^3}{g_2^3(\tau)-\Delta(\tau)} = \frac{27j(\tau)}{j-1728}$, this is in fact the universal elliptic curve.

The N torsion points for a lattice $[1,\tau]$ are $\frac{c+d\tau}{N}$ for $0 \le c < N$ and $0 \le d < N$. The $x-$coordinates of the N torsion points on the universal elliptic curve are the functions

$$f^{(c,d)}(\tau) = \frac{g_2(\tau)}{g_3(\tau)}\wp_\tau\left(\frac{c+d\tau}{N}\right).$$

Denote the collection of these functions by $x(E_j[N])$.

Theorem 42. *$\mathbb{C}(X'(N))$ equals $\mathbb{C}(j, x(E_j[N]))$. $\mathrm{Gal}(\mathbb{C}(X'(N))/\mathbb{C}(X(1))) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, and the action of $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathbb{C}(X'(N))$ via $\gamma(f) = f \circ \gamma$ agrees with the Galois group's action.*

The first step is to show that the $E_j[N]$ are meromorphic functions defined on $X'(N)$. Writing the function in terms of lattices,

$$f^{(c,d)}(\lambda\Lambda, (\lambda P, \lambda Q)) = \frac{\lambda^{-4}g_2(\Lambda)}{\lambda^{-6}g_3(\Lambda)}(\lambda^{-2}\wp_\Lambda(cP + dQ))$$

so we conclude that $f^{(c,d)}$ transforms correctly under $\Gamma(N)$.

Next, a basic calculation shows that for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in \mathrm{SL}_2(\mathbb{Z})$

$$f^{(c',d')}(\gamma z) = \frac{(cz+d)^4 g_2(z)}{(cz+d)^6 g_3(z)}\wp_{\gamma z}\left(\frac{c'(cz+d) + d'(az+b)}{(cz+d)N}\right) = f^{(c'',d'')}(z)$$

where $[d'', c''] = [d', c']\gamma$.

To check they are meromorphic at the cusps, note that we may move any cusp to infinity using an element of $\mathrm{SL}_2(\mathbb{Z})$. But $f^{(c,d)}(\gamma\tau) = f^{(c',d')}(\tau)$. Thus it suffices to check that $f^{(c,d)}$ are meromorphic at infinity. $\frac{g_2(\tau)}{g_3(\tau)}$ certainly is, and a simple calculation shows $\lim_{\tau\to\infty}\wp_\tau(\frac{c+d\tau}{N})$ is finite. Therefore we have the following containment of fields:

$$\mathbb{C}(X(1)) = \mathbb{C}(j) \subset \mathbb{C}(j, x(E_j[N])) \subset \mathbb{C}(X(N)).$$

Now note that if $f^{(c,d)}(z) = f^{(c',d')}(z)$ then $\wp_z(\frac{c+dz}{N}) = \wp_z(\frac{c'+d'z}{N})$ and hence

$$\frac{c+dz}{N} = \pm\frac{c'+d'z}{N} \mod \Lambda = [1, z].$$

Thus $(c,d) = \pm(c', d') \mod N$. Therefore $f^{(c,d)}(\gamma z) = f^{(c',d')}(z)$ implies that $\gamma \in \pm\Gamma(N)$.

Now consider the map

$$\theta : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}(X'(N)))$$

defined by $\theta(\gamma)$ acting on $f \in \mathbb{C}(X'(N))$ by sending it to $f \circ \gamma$ using the action of $\mathrm{SL}_2(\mathbb{Z})$ on $X'(N)$. This is a group homomorphism, and $\pm\Gamma(N)$ certainly lie in the kernel. On the other hand, if $\gamma \in \ker\theta$, then γ fixes all of the $f^{(c,d)}$. But that implies $\gamma \in \pm\Gamma(N)$. Therefore we conclude

$$\theta(\mathrm{SL}_2(\mathbb{Z})) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \subset \mathrm{Aut}(\mathbb{C}(X'(N))).$$

Since $\theta(\mathrm{SL}_2(\mathbb{Z}))$ fixes exactly $\mathbb{C}(X(1)) \subset \mathbb{C}(X'(N))$, $\mathbb{C}(X'(N))/\mathbb{C}(X(1))$ is Galois with group $\theta(\mathrm{SL}_2(\mathbb{Z}))$. Since $\mathbb{C}(j, x(E_j[N]))$ is only fixed by the identity, it is all of $\mathbb{C}(X'(N))$. Note that the Galois group is compatible with the action of $\mathrm{SL}_2(\mathbb{Z})$ on $X'(N)$ since we constructed it in terms of the action. □

We can finally prove the desired theorem.

Theorem 43. *Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that surjects onto $(\mathbb{Z}/N\mathbb{Z})^\times$ by the determinant map. Then $H\backslash X(N)$ is a connected algebraic curve defined over $\mathbb{Q}$.*

Let $H_{\mathbb{Q}}$ be the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_N, j, x(E_j[N]))/\mathbb{Q}(j))$.[4] Generators for the $N-$torsion can be selected so the $x-$coordinates are $p_\tau = f^{(1,0)}(\tau)$ and $q_\tau = f^{(0,1)}(1)$. Then the $x-$coordinate of any N-torsion point is a linear combination of these, say $ap_\tau + bq_\tau$. Note a and b are unique modulo N.

Now any $\sigma \in H_{\mathbb{Q}}$ permutes the $N-$torsion points, so

$$\begin{pmatrix} p_\tau^\sigma \\ q_\tau^\sigma \end{pmatrix} = \rho(\sigma) \begin{pmatrix} p_\tau \\ q_\tau \end{pmatrix}$$

for some linear transformation $\rho(\sigma) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The assignment

$$\rho : H_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$$

is a group homomorphism.

Now let $\sigma \in H_{\mathbb{Q}}$ and let μ be a primitive Nth root of unity with $e_N(P, Q) = \mu$. Then $\sigma(e_N(P, Q)) = e_N(P^\sigma, Q^\sigma) = e_N(P, Q)^{\det(\rho(\sigma))}$ by the bi-linearity of the Weil pairing. Thus we have

$$\mu^\sigma = \mu^{\det(\rho(\sigma))}. \tag{10}$$

Consider the extension $\mathrm{Gal}(j, \mu_N, x(E_j[N]))/\mathrm{Gal}(j, x(E_j[N]))$, also Galois. The above calculation with the Weil pairing shows that any element σ of this Galois group must fix μ as $\det(\rho(\sigma)) = 1$. Thus $\mu \in \mathbb{Q}(j, x(E_j[N]))$.

Now we consider the following fields and Galois groups: $\mathbb{Q}(j, x(E_j[N]))$, $\mathbb{Q}(\mu_N, j)$, and $\mathbb{Q}(j)$, with $H_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}(j, x(E_j[N]))/\mathbb{Q}(j))$ and $H_{\mathbb{Q}(\mu_N)} = \mathrm{Gal}(\mathbb{Q}(j, x(E_j[N]))/\mathbb{Q}(\mu_N, j))$. Restricting ρ to $H_{\mathbb{Q}(\mu_N)}$, we get

$$H_{\mathbb{Q}(\mu_N)} \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$$

This map is injective since if $\sigma \in H_{\mathbb{Q}(\mu_N)}$ fixes p_τ and q_τ then $x(E_j[N])$ must be fixed as well.

Now we recall a standard but very useful fact about compositums. It is proven in section 7.6 of Diamond and Shurman [8].

Lemma 44. *Let k and F be field extensions of f with F/f Galois, and let $K = kF$. Then K/k is Galois and there is a natural injection*

$$\mathrm{Gal}(K/k) \hookrightarrow \mathrm{Gal}(F/f)$$

with image $\mathrm{Gal}(F/(k \cap F))$.

In particular, this implies that $\mathrm{Gal}(\mathbb{Q}(\mu_N, j)/\mathbb{Q}(j)) = \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times$.

This will also let us transfer knowledge about function fields over $\mathbb{C}$ to function fields over $\mathbb{Q}$. Letting $f = \mathbb{Q}(\mu_N, j)$, $F = \mathbb{Q}(j, x(E_j[N]))$, $k = \mathbb{C}(j)$, and $K = \mathbb{C}(j, x(E_j[N]))$, this implies $\mathrm{Gal}(\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j))$ injects into $H_{\mathbb{Q}(\mu_N)}$ with image $\mathrm{Gal}(F/k \cap F)$. But we

[4] This extension is Galois: the algebraic part of the argument in Theorem 42 adapts to show this.

know that $\mathrm{Gal}(\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j)) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ by Theorem 42. Since these are finite groups and ρ is an injection in the other direction, the groups must be isomorphic. By Galois theory, $k \cap F = \mathbb{C}(j) \cap \mathbb{Q}(j, x(E_j[N])) = \mathbb{Q}(\mu_N, j)$. Intersecting with $\overline{\mathbb{Q}}$ shows that

$$\mathbb{Q}(j, x(E_j[N])) \cap \overline{\mathbb{Q}} = \mathbb{Q}(\mu_N). \tag{11}$$

Finally, we know $2|H_{\mathbb{Q}}| = 2|H_{\mathbb{Q}(\mu_N)}||\,\mathrm{Gal}(\mathbb{Q}(\mu_N, j)/\mathbb{Q}(j))| = |\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})||(\mathbb{Z}/N\mathbb{Z})^\times| = |\,\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})|$. Therefore $H_{\mathbb{Q}} = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$.

It remains to consider which curves are defined over $\mathbb{Q}$. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let

$$K_1 := (\mathbb{Q}(j, \mu_N, x(E_j[N])))^{H'}.$$

If the determinant map is surjective, then H' permutes the roots of unity by (10). Thus $K_1 \cap \mathbb{Q}(\mu_N) = \mathbb{Q}$, so using (11)

$$K_1 \cap \overline{\mathbb{Q}} = \mathbb{Q} \quad \text{and} \quad K_1 = (\mathbb{Q}(j, x(E_j[N])))^{\Gamma_H/\{\pm 1\}}.$$

Therefore the curve with function field K_1 is defined over $\mathbb{Q}$.

Finally, recall from Theorem 42 that the action of $\Gamma_H \subset \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on $X'(N)$ is compatible with the Galois action of $\Gamma_H/\{\pm 1\} \subset \mathrm{Gal}(\mathbb{C}(j, x(E_n[N]))/\mathbb{C}(j))$ on $\mathbb{C}(X'(N))$, so $H\backslash X(N) = \Gamma_H\backslash X'(N)$ has function field

$$K_2 = \mathbb{C}(j, x(E_j[N]))^{\Gamma_H/\{\pm 1\}}.$$

Now extend the curve K_1 from the rationals to the complex numbers. $K_1 = K_2$, so since $H\backslash X(N)$ and the extension have the same function fields they are isomorphic over $\mathbb{C}$. Therefore $H\backslash X(N)$ is an algebraic curve defined over $\mathbb{Q}$. □

Note that if this were done for $X_0(N)$, the minimal polynomial for the extension would be the modular equation as the field of meromorphic functions is $\mathbb{C}(j(z), j(Nz))$. However, the approach taken in Section 2 r is more explicit and give additional information.

8. $X^+_{ns}(n)$ and The Class Number One Problem

Let n be a positive integer. In this section we will construct a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, use it to define the modular curve $X^+_{ns}(n)$, and relate it to the class number one problem. This is the approach presented in Serre [14] (and Chen [5] and Baran [3]).

Let $R = \{1, \alpha\}$ be an order in an imaginary quadratic field. Let the minimal polynomial for α be $x^2 - ux + v \in \mathbb{Z}[x]$. R/pR is either $\mathbb{F}_{p^2}$ or $\mathbb{F}_p \times \mathbb{F}_p$ depending on whether the prime $p \in \mathbb{Z}$ splits in R. Let $A = R/nR$. Note that $\{1, \alpha\}$ is a basis for A over $\mathbb{Z}/n\mathbb{Z}$.

Definition 45. A Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is the image of $A^\times$ acting on A by multiplication. If A is not split at p for every prime dividing n, then this subgroup is called a non-split Cartan subgroup. Denote it by $C_{ns}(n)$.

Although Serre gives a more general definition [14], all non-split Cartan subgroups turn out to be conjugate so nothing is lost.

For every prime p that divides n, let $r = v_p(n)$ and consider the ring automorphism σ_p of order 2 that acts as

$$\sigma_p(\alpha) \equiv \overline{\alpha} \mod p^r \quad \text{and} \quad \sigma_p(\alpha) \equiv \alpha \mod n/p^r.$$

(It exists by the Chinese remainder theorem.) Using the basis, it gives a matrix S_p in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. It is clear that for different primes the matrices commute.

Next we consider the normalizer of $C_{ns}(n)$.

Lemma 46. *Denote the normalizer of $C_{ns}(n)$ in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ by $C_{ns}^+(n)$. It is generated by $C_{ns}(n)$ and the elements S_p for $p|n$. In particular, if v is the number of prime divisors of n the size of the normalizer is*

$$n^2 2^v \prod_{p|n} (1 - \frac{1}{p^2}).$$

Proof. The proof follows Baran [3]. The first step is to deal with the case $n = p^r$ and determine the normalizer. If k is in the normalizer of $C_{ns}(p^r)$, it acts by conjugation on $C_{ns}(p^r)$ giving a map $t_k : C_{ns}(p^r) \to C_{ns}(p^r)$. Identifying $C_{ns}(p^r)$ with $A^\times$, t_k extends to a ring automorphism of A. Since any such ring automorphism will preserve the minimal polynomial of α (reduced modulo p^r), either $t_k(\alpha) = \alpha$ or $u - \alpha$. Thus as a linear transformation $t_k(z) = z$ or $t_k(z) = \sigma_p(z)$ for $z \in A$. For $Z \in C_{ns}(p^r)$ corresponding to multiplying by z, this implies

$$kZk^{-1} = Z \quad \text{or} \quad kZk^{-1} = S_p Z S_p$$

as the linear transformation $S_p Z S_p$ corresponds to multiplying by $\sigma_p(z)$. As S_p has order 2, either k or $S_p k$ commutes with $C_{ns}(p^r)$. Linear algebra shows the centralizer of $C_{ns}(p^r)$ is itself, so $k \in C_{ns}(p^r)$ or $k \in S_p C_{ns}(p^r)$. Thus the normalizer of $C_{ns}(p^r)$ is generated by S_p and $C_{ns}(p^r)$ as claimed. For composite n the result follows through the Chinese remainder theorem as S_p and $S_{p'}$ commute for $p \neq p'$.

The size of this group is the product of the size of $C_{ns}(n) = |A^\times| = n^2 \prod\limits_{p|n} \left(1 - \frac{1}{p^2}\right)$ and the group generated by the S_p. The latter has size 2^r since the S_p are of order 2 and commute with each other. □

Next we will check that $\det : C_{ns}^+(n) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is a surjection.[5]

Proof. Given an integer r relatively prime to n, we first need to find an $\alpha \in R$ such that $N_{K/\mathbb{Q}}(\alpha) \equiv \pm r \mod p^m$. Recall the norm of α is the determinant of the transformation multiplication by α. Let p be a prime dividing n. By hypothesis, it is inert in K, so K_p is a quadratic extension of $\mathbb{Q}_p$. By the elementary properties of the Hilbert symbol for local fields (see Serre [13] Chapter III), we know that $\mathbb{Q}_p^\times / N_{K_p/\mathbb{Q}_p}(K_p^\times)$ is a group of order 2. Thus there exists an $\alpha \in K_p^\times$ such that $N_{K_p/\mathbb{Q}_p}(\alpha) = \pm r$. It is easy to see $\alpha \in R_p$. Now pick an $\alpha_{\mathfrak{p}} \in R$ with $\alpha_p \equiv \alpha \mod p^m$. Note this implies $N_{K/\mathbb{Q}}(\alpha_p) \equiv \pm r \mod p^m$.

Do this for each prime divisor p of n. Use the weak approximation theorem to pick $\beta \in R$ such that $b \equiv \alpha_p \mod p^m$ for all $p^m | n$. But then $N_{K/\mathbb{Q}}(\beta) = \beta\overline{\beta} \equiv \alpha_p \overline{\alpha_p} \equiv \pm r \mod p^m$. Since S_p has determinant -1 when viewed as transformation modulo p^m and determinant 1 for the other primes, we can multiply to obtain a transformation with determinant $r \mod p^m$ for each prime p. Thus it has determinant r modulo n. □

Now define $\Gamma_{C_{ns}^+(n)} \subset \mathrm{SL}_2(\mathbb{Z})$ to be the subgroup that reduces modulo N to elements of $C_{ns}^+(n)$. Because $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, the index of $\Gamma_{C_{ns}^+(n)}$ in $\mathrm{SL}_2(\mathbb{Z})$ is the index of $C_{ns}^+(n) \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. The size of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is $n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right)$, and the index of $C_{ns}^+(n) \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ in $C_{ns}^+(n)$ is $\phi(n)$ as the determinant map is surjective. Thus $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_{C_{ns}^+(n)}]$ is $\frac{n\phi(n)}{2^v}$ where v is the number of primes dividing n.

Combined with the theory from the previous section, this implies there is a modular curve $X_{ns}^+(n)$ with the following properties:

[5] In any particular case this is simple to check, so this argument is unnecessary for specific uses of $C_{ns}^+(n)$.

- $X_{ns}^+(n)$ parametrizes equivalence classes of (E,φ) where E is an elliptic curve and φ is an isomorphism $E[n] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Two pairs are equivalent if $E = E'$ and $\varphi \circ \varphi^{-1} \in C_{ns}^+(n) \subset \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Note that the cusps are not part of this identification.
- This is isomorphic to $\Gamma_{C_{ns}^+(n)} \backslash \mathcal{H}^\times$ and is an algebraic curve over $\mathbb{Q}$.
- There is a projection $X_{ns}^+(n) \to X(1)$ given by mapping $(E,\varphi) \to E$. The degree is just the index of $\Gamma_{C_{ns}^+(n)}$ in $\mathrm{SL}_2(\mathbb{Z})$ which has already been calculated to be $\frac{n\phi(n)}{2^v}$.

Information about the rational points on this curve will let us solve the class number one problem. The reductions used in Heegner's proof allow us to only consider maximal orders.

Theorem 47. *Let K be an imaginary quadratic field with class number one, and n be an integer such that all primes dividing n are inert in K. Any elliptic curve E with complex multiplication by K gives rise to a unique rational point on $X_{ns}^+(n)$ with integral j invariant.*

Proof. Let K be an imaginary quadratic field of class number one with ring of integers $\mathcal{O}_K$. The set of elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$ (up to complex isomorphism) are in bijection with the class group by viewing the curve as a lattice (see C.11 of Silverman [15]). Since the class number is one, all curves with complex multiplication by $\mathcal{O}_K$ are isomorphic over $\mathbb{C}$, they all have $j-$invariant $j(\mathcal{O}_K)$. It must be rational as it is fixed by $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$.[6] Since an elliptic curve over any algebraically closed field of characteristic 0 is uniquely determined by its $j-$invariant, there is a unique elliptic curve E defined over $\overline{\mathbb{Q}}$ with this j-invariant. Now pick an identification $\varphi : E[n] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$, so we get a homomorphism

$$\rho_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

We will show that the image lies in the subgroup $C_{ns}^+(n)$. Assuming this, let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We know that $E^\sigma = E$ and $\varphi \circ \rho_n(\sigma) \circ \varphi^{-1} \in C_{ns}^+(n)$ so $(E,\varphi) = (E,\varphi)^\sigma$ is a rational point on $X_{ns}^+(n)$. Therefore $\mathcal{O}_K$ gives rise to a unique rational point (E,φ) with $j(E) = j(\mathcal{O}_K) \in \mathbb{Z}$.

It remains to prove the claim about the image of ρ_n. The map $\mathcal{O}_K \to \mathrm{End}(E[n])$ coming from complex multiplication factors through $n\mathcal{O}_K$ as $n\,\mathrm{End}(E[n]) = 0$. Identifying $\mathrm{Aut}(E[n])$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ via φ, we see that the image of $(\mathcal{O}_K/n\mathcal{O}_K)^\times$ is a non-split Cartan subgroup $C_{ns}(n)$. The image of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ will commute with $C_{ns}(n)$ since it fixes $\mathcal{O}_K$. The image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ will not. Since $C_{ns}(n)$ is its own centralizer, $\rho_n(\mathrm{Gal}(\overline{\mathbb{Q}}/K)) \subset C_{ns}(n)$. K is an imaginary quadratic field, so $\rho_n(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ will normalize $\rho_n(\mathrm{Gal}(\overline{\mathbb{Q}}/K))$, thus $\rho_n(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is contained in $C_{ns}^+(n)$. □

If K is an imaginary quadratic field of discriminant d and class number 1, then all primes less that $\frac{1+|d|}{4}$ are inert (Proposition 2). If p is the largest prime dividing n, then every imaginary quadratic field with class number 1 and discriminant greater than or equal to $4p$ will give a rational point with integral j-invariant on $X_{ns}^+(n)$. For special values of n, it is feasible to find all such points. For example, Chen [5] and Baran [2], [3] do this for a variety of small n including $n = 9, 15, 16, 20$, and 21.

9. The Class Number One Problem and $X_{ns}^+(24)$

Serre writes that for "$N = 24$ an elliptic curve is obtained. This is the level considered in effect by Heegner." He provides no details, and Heegner's approach seems to have nothing

[6] Alternately, use Proposition 35 (or the stronger Theorem 34).

to do with $X_{ns}^+(24)$. In this section we will find the rational points with integral j-invariant on $X_{ns}^+(24)$ by looking at $X_{ns}^+(8)$ and $X_{ns}^+(3)$. Any such point on $X_{ns}^+(24)$ naturally maps to rational points on $X_{ns}^+(8)$ and $X_{ns}^+(3)$. These are nicer because they turn out to have genus 0.

9.1. Computing the Ramification of $X_{ns}^+(n)$ over $X(1)$.

The map from $X_{ns}^+(n) \to X(1)$ is a map of degree $n\phi(n)/2^v$. That means the generic fibre is $n\phi(n)/2^v$ points. The only places where this fails to happen are the cusps and the elliptic points of $X(1)$, $\rho = \frac{-1+\sqrt{-3}}{2}$ and i. Let $H = \Gamma_{C_{ns}^+(n)}$, so $X_{ns}^+(n) = H\backslash X(1)$. We have the following computational result.

Proposition 48. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ contain ± 1. For $z' \in \Gamma\backslash\mathcal{H}^*$ above $z \in X(1)$, the ramification index at z' is $[\mathrm{SL}_2(\mathbb{Z})_z : \Gamma_{z'}]$ where the subscripts denote stabilizers. If $\sigma \in \mathrm{SL}_2(\mathbb{Z})/\Gamma$ and $\sigma(z) = z'$, the ramification index can also be computed by $[\mathrm{SL}_2(\mathbb{Z})_z : \sigma^{-1}\Gamma\sigma \cap \Gamma_z]$.*

All of this material is standard in the theory of modular forms, and found for example in Diamond and Shurman [8].

Therefore, if we have a set of coset representatives for H in $\mathrm{SL}_2(\mathbb{Z})$ it is a mechanical calculation with finite groups to find the ramification indices. There are general results about the ramification in Baran [3], including formulas for the genus and number of elliptic fixed points. We only need results for $n = 3, 8$ so it is much simple to do it by hand.

We only consider the case $n = p^r$. For every $m \in (\mathbb{Z}/p^r\mathbb{Z})^\times/\{\pm 1\}$, choose a $y_m \in (\mathbb{Z}/p^r\mathbb{Z})[\alpha]^\times$ with $N(y_m) = m$. Let the set of all y_m be denoted by $Y(p^r)$.

Lemma 49. *A set of coset representatives for $C_{ns}^+(p^r) \cap \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ are given by the linear maps that transform the basis $\{1, \alpha\}$ of A as*

$$1 \to y^{-1} \quad \textit{and} \quad \alpha \to \overline{y}(\alpha + x)$$

where $x \in \mathbb{Z}/p^r\mathbb{Z}$ and $y \in Y(p^r)$.

Proof. We know the index of $C_{ns}^+(p^r) \cap \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ is $p^r\phi(p^r)/2$. There are $p^r \cdot \phi(p^r)/2$ elements listed above. It suffices to show they all lie in distinct cosets.

Now unwinding definitions shows $C_{ns}^+(p^r) \cap \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ consists of the transformation of the form

$$1 \to y \quad \text{and} \quad \alpha \to y\alpha, \quad N(y) = 1$$

and transformations of the form

$$1 \to \overline{y} \quad \text{and} \quad \alpha \to \overline{y\alpha}, \quad N(y) = -1$$

The latter is multiplication by y followed by σ_p, which is complex conjugation as p^r has only one prime divisor.

If two pair (x, y), $(x', y') \in (\mathbb{Z}/p^r\mathbb{Z}) \times Y(p^r)$ lie in the same coset, then there is a $\beta \in (\mathbb{Z}/p^r\mathbb{Z})[\alpha]^\times$ with $N(\beta) = 1$ such that multiplying by β relates the two maps, or $N(\beta) = -1$ and multiplying by β and then conjugating relates the two. Thus comparing what the transformations do to 1,

$$y^{-1} = (y')^{-1}\beta \quad \text{or} \quad y^{-1} = \overline{y'^{-1}\beta}.$$

It follows $N(y) = \pm N(y')$, so $y = y'$ as both are in $Y(p^r)$. Looking at what the transformations do to α, it follows $x \equiv x' \mod p^r$. Thus all of the coset representatives are distinct. □

Through the isomorphism $\mathrm{SL}_2(\mathbb{Z})/\Gamma(p^r) \to \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$, these cosets representatives lift to give cosets for $\Gamma_{C^+_{ns}(p^r)}$ in $\mathrm{SL}_2(\mathbb{Z})$.

It is now completely elementary to compute the ramification of $X^+_{ns}(8)$ above $X(1)$ and of $X^+_{ns}(3)$ above $X(1)$ using Proposition 48. The results are that:

- $X^+_{ns}(3)$ is degree 3 over $X(1)$. It is ramified above ρ and ∞ with index 3, while there are three unramified (elliptic) points above i.
- $X_{ns}(4)$ is degree 4 over $X(1)$. It is ramified with index 4 above ∞. There are three points above i, one ramified of index 2 and the other two σ_1 and σ_2 elliptic. There are two points above ρ, ρ_1 being elliptic and ρ_2 being ramified of index 3.
- $X_{ns}(8)$ is degree 4 over $X_{ns}(4)$. There are two points above ∞ each with index 2. There are three points above each of σ_1 and σ_2, one ramified of index 2 and the other two elliptic. There are two points above ρ_1, one ramified of index 3 and the other elliptic. All of the remaining points are unramified.

To compute the genus, we will look at how the Riemann surfaces branch over $X(1)$ and the standard result that if μ is the index of a congruence subgroup, e_i is the number of elliptic fixed points of order i, and e_∞ is the number of cusps, then

$$g = 1 + \frac{\mu}{12} - \frac{e_2}{4} - \frac{e_3}{3} - \frac{e_\infty}{2}.$$

In particular, $X^+_{ns}(3)$, $X^+_{ns}(4)$, and $X^+_{ns}(8)$ are genus 0. $X^+_{ns}(24)$ has genus 1. Baran [3] calculates the genus more generally.

9.2. **Computing Uniformizers.** Because they are genus 0 and defined over $\mathbb{Q}$, we will look for an identification $X^+_{ns}(n) \to \mathbb{P}^1$ that is defined over $\mathbb{Q}$. This is called a uniformizer. The $j-$function is a uniformizer for $X(1)$. We will compute the following relations between uniformizers.

Theorem 50. *There exists a uniformizer $s : X^+_{ns}(3) \to \mathbb{P}^1$ defined over $\mathbb{Q}$ such that $j = s^3$.*

In particular, for any imaginary quadratic field giving a rational point on $X^+_{ns}(3)$, the j invariant will be a cube of a rational number. Since the j invariant is an algebraic integer, its cube root is an integer. This gives the promised proof of the piece of Theorem 36 we needed.

Theorem 51. *There exists a uniformizer $t : X^+_{ns}(4) \to \mathbb{P}^1$ such that*

$$j = -2^{14}t(t-1)^3.$$

Furthermore, $t(\sigma_1) = \frac{5}{4} + \frac{\sqrt{-2}}{4}$ and $t(\sigma_2) = \frac{5}{4} - \frac{\sqrt{-2}}{4}$.

Theorem 52. *There exists a uniformizer $u : X^+_{ns}(8) \to \mathbb{P}^1$ such that*

$$t = \frac{-16u}{(4u^2+4u-1)^2}.$$

Putting the second and third together, we obtain

Corollary 53. *There exists a uniformizer $w : X^+_{ns}(8) \to \mathbb{P}^1$ such that*

$$j = -\frac{2^{18}w(16w+(4w^2+4w-1)^2)^3}{(4w^2+4w-1)^8}.$$

By picking a different uniformizer the denominator takes on a nicer form.

Corollary 54. *There exists a uniformizer* $v : X_{ns}^+(8) \to \mathbb{P}^1$ *such that*

$$j = -\frac{2^{17}(v+1)^3\left(8(v+1)^3 + (v^2-2)^2\right)^3}{(v^2-2)^8}.$$

Proof. This follows from setting $w = \dfrac{1}{2v+2}$ and simplifying algebraically. □

All of the theorems about uniformizers are proven using the ramification data, following Chen [5] and Baran [3]. Suppose u is a uniformizer for $X_{ns}^+(N)$, and j the uniformizer for $X(1)$. Since $j(\rho) = 0$ and $j(\infty) = \infty$, by working over $\mathbb{C}$ and comparing poles and zeroes there is a relation

$$j = \lambda \frac{\displaystyle\prod_{z \text{ above } \rho} (u - u(z))^{e(z)}}{\displaystyle\prod_{z \text{ above } \infty} (u - u(z))^{e(z)}} \tag{12}$$

where λ is a constant and $e(z)$ is the ramification index of z over ρ or ∞. Since u can be varied using the automorphisms of $\mathbb{P}^1$, by appropriately selecting u the constants can be made rational giving the desired uniformizer.

For a warm up, we will compute the uniformizer for $X_{ns}^+(3)$. First, note that the (unique) points P and Q above ∞ and ρ will be rational. To see this, note that $j(\infty)$ and $j(\rho)$ lie in $\mathbb{P}^1_{\mathbb{Q}}$ and that the uniformizer is a rational function. This implies that acting by any element of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $X_{ns}([)3$ sends P and Q to points above ∞ and ρ since the j value is unchanged. But these are the unique points above ∞ and ρ, so P and Q are rational.

Now using an automorphism of $\mathbb{P}^1_{\mathbb{Q}}$, we may assume that our uniformizer s satisfies $s(\infty) = \infty$ and $s(\rho) = 0$. These conditions determine s up to scaling. Then (12) combined with the ramification data from the last section says that

$$j = \lambda s^3.$$

Now λ will be a rational cube (evaluate on a point corresponding to a class number one field, where we have calculated j to be a cube), so by rescaling s we get $j = s^3$.

The uniformizers for $X_{ns}^+(4)$ and $X_{ns}^+(8)$ use the same idea, but involve more work. If t is a uniformizer for $X_{ns}^+(4)$, note that $t(\rho_1)$, $t(\rho_2)$, and $t(\infty)$ are rational since ∞ is the unique point above ∞, and ρ_1 and ρ_2 are the unique points above ρ with ramification index 1 and 3. Use an automorphism of $\mathbb{P}^1_{\mathbb{Q}}$ so that $t(\infty) = \infty$, $u(\rho_1) = 1$ and $t(\rho_2) = 0$. Then (12) says

$$j = \lambda t(t-1)^3.$$

To compute λ, note that we have additional ramification data over i. There are three points above i, which means that if we evaluate the right side of equation at i, getting 1728, there must be a double root. Thus there should exist A, B, C such that

$$\lambda t(t-1)^3 - 1728 = \lambda(t^2 + At + B)(t - C)^2.$$

Expand this and note that it must be the zero polynomial. Thus all of the coefficients are zero, so we obtain a system of equations

$$\begin{aligned} -B^2C\lambda - 1728 &= 0 \\ -AC^2\lambda + 2BC\lambda - \lambda &= 0 \\ 2AC\lambda - C^2\lambda - B\lambda + 3\lambda &= 0 \\ -A\lambda + 2C\lambda - 3\lambda &= 0 \end{aligned}$$

Solving the system gives $\lambda = -2^{14}$, $A = -\frac{5}{2}$ and $B = \frac{27}{16}$. We also need to evaluate $t(\sigma_1)$ and $t(\sigma_2)$. They have ramification index 1, so are the roots of $t^2 + At + B = 0$. Thus $t(\sigma_1) = \frac{5}{4} + \frac{\sqrt{-2}}{4}$ and $t(\sigma_2) = \frac{5}{4} - \frac{\sqrt{-2}}{4}$.

The uniformizer for $X_{ns}^+(8)$ over $X_{ns}^+(4)$ is similar but much nastier. There are only two rational points that help, the two points over ρ_1. Choose w so that the elliptic point is sent to 0 and the ramified point is sent to infinity. Since $t(\rho_1) = 0$, the uniformizer satisfies

$$t = \lambda \frac{w}{(Aw^2 + Bw - 1)^2} \tag{13}$$

as there are two points, ramified of order 2, above ∞. We need to specify λ. Unfortunately, it is only clear in hindsight to pick $\lambda = \frac{-1}{2}$, so we choose λ later. The other data we have is that

$$\lambda \frac{w}{(Aw^2 + Bw - 1)^2} - t(\sigma_1) = 0$$

has a double root and likewise for $t(\sigma_2)$. This gives systems of equations, but they are more complicated than is pleasant to solve by hand. Sage [11] can be used to solve them with some effort.[7] Of course, given the solution it is easy to verify it has the required properties. This establishes all of the required relations between uniformizers.

9.3. **Solving the Class Number One Problem.** To solve the class number one problem, we are looking for rational points on $X_{ns}^+(24)$ with integral j invariant. Such a point projects to rational points on $X_{ns}^+(8)$ and $X_{ns}^+(3)$. In order for the j invariant to be integral, it is clear that the uniformizer t must be an integer, while v is (only) rational. Thus we need to find all rational v and integer s such that

$$s^3 = -\frac{2^{17}(v+1)^3\left(8(v+1)^3 + (v^2-2)^2\right)^3}{(v^2-2)^8}. \tag{14}$$

Theorem 55. *The only solutions (v, s) to (14) are*

$$(\infty, 0), \quad (-2, -32) \quad (0. -96) \quad (-3, -960) \quad (2, -5280) \quad (3, -640320)).$$

[7] To do this, rewrite the denominator as $w^2 + A'w + B'$ and let $\lambda = 2$. Then let $\alpha = t(\sigma_1)$, $\overline{\alpha} = t(\sigma_2)$, and write down the double root condition for $t(\sigma_1)$. This gives 4 equations, three of them multiples of α. Solve these for the roots, keeping A' and B' as free variables. This is possibly but nasty as it involves square roots. Then change variables so one of the variables is the square root. There are two families of solutions, one of which makes the fourth equation (the one not a multiple of α) impossible. Now do the same for $t(\sigma_2)$. The two remaining equations are too nasty to be solved exactly but can be solved numerically. However, if $\lambda = 1$ (the obvious first choice) the numerical equation solver doesn't find the correct solution. $\lambda = 2$ works. This gives a solution with A' and B' not rational. However rescaling w finally gives the stated uniformizer with rational coefficients. If we pick the correct value of λ, -1 with the denominator we're using, the system of two equations that could only be solved numerically, which are two cubics, turn out to have integer solutions.

These correspond to the imaginary quadratic fields

$$\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \textit{ and } \mathbb{Q}(\sqrt{-163})$$

Proof. Let $v = \frac{x}{y}$ where x and y are relatively prime, and let $t = -s$. We obtain that

$$t^3 = \frac{2^{17} y (x+y)^3 \left(8(x+y)^3 y + (x^2 - 2y^2)^2\right)^3}{(x^2-2y^2)^8}. \tag{15}$$

Suppose a prime p divides $x^2 - 2y^2$. Then if $p \neq 2$, if $p | x$ is must also divide y, contradicting the fact that x and y are relatively prime. Likewise p does not divide y. If $x + y \equiv 0 \mod p$, then $x = -y \mod p$ so $x^2 - 2y^2 = -x^2 \neq 0 \mod p$, a contradiction. Thus it follows that $v_p(y)$, $v_p(x+y)$, and $v_p(8(x+y)^3 y + (x^2-2y^2)^2)$ are all 0. This implies $v_p(t) < 0$. But $t \in \mathbb{Z}$, so the only prime dividing $x^2 - 2y^2$ is 2. If $2 | x^2 - 2y^2$, then x must be even. Since x and y are relatively prime, y is odd and hence two exactly divides $x^2 - 2y^2$. Therefore it suffices to find all (x, y) such that $x^2 - 2y^2 = \pm 1$ or $x^2 - 2y^2 = \pm 2$ and t is an integer. The amazing thing is that these equations reduce to the same four Diophantine equations in Lemma 40 that solved the class number one problem in Heegner's method.

If $x^2 - 2y^2 = \pm 1$, for t to be an integer we need the right side of (15) to be a cube. The only terms which are not cubes are $2^{17} y$. Thus we see that $y = 2z^3$ for some integer z. Then $x^2 = 2(2z^3)^2 \pm 1$. Writing $w := 2z^2$, we obtain $x^2 = w^3 \pm 1$. Both of these equations are solved by Lemma 40.

If $x^2 - 2y^2 = \pm 2$, then for t to be an integer the right side of (15) must be a cube. The denominator is 2^8, so the only non-cube term is y. Thus $y = z^3$ for some integer z and we have $x^2 = 2z^6 \pm 2$. It is clear x is even. Writing $x = 2x_2$, we see that $4x_2^2 = 2z^6 \pm 2$, so $2x_2^2 = z^6 \pm 1$. The positive case is covered in Lemma 40. In the negative case, letting $w = z^2$ and multiplying the equation by -1 gives $-2x_2^2 = (-w)^3 + 1$, the last equation in Lemma 40.

Using the changes of variables to find $v = \frac{x}{y}$, only some of these correspond to integer solutions to the original equations $x^2 - 2y^2 = \pm 1, \pm 2$. For those that do, the table lists the value of v and t. Since any two imaginary quadratic fields with the same class number are the same, we identify all the sufficiently large imaginary quadratic fields of class number one using Table 1. This completes the second proof of the class number one theorem. □

Table 2. Integral Points and the Quadratic Fields of Class Number 1

Equation	Solutions	v	t	Quadratic Field
$x^2 = w^3 + 1$	$(-1, 0)$	none		
	$(0, \pm 1)$	∞	0	$\mathbb{Q}(\sqrt{-3})$
	$(2, \pm 3)$	± 3	-640320, -960	$\mathbb{Q}(\sqrt{-163})$, $\mathbb{Q}(\sqrt{-43})$
$x^2 = w^3 - 1$	$(1, 0)$	none		
$z^6 + 1 = 2x_2^2$	$(\pm 1, \pm 1)$	± 2	-5280, -32	$\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-11})$
$(-w)^3 + 1 = -2x_2^2$	$(1, 0)$	0	-96	$\mathbb{Q}(\sqrt{-19})$

Serre wrote that for "$N = 24$, an elliptic curve is obtained." The above argument produces 4 elliptic curves as subsidiary results, but the main equation does not seem to be an elliptic curve. However, looking back at equation (14) we see that t will be rational whenever $\frac{4}{(v^2-2)^2}$ is a cube. as the remaining terms are cubes. This is the same as $4(v^2 - 2)$ being a cube.

Thus t is rational whenever v is a rational solution to

$$u^3 = 4v^2 - 8 \qquad \Longrightarrow \qquad (v')^2 = u^3 + 8$$

where $v' = 2v$. This is an elliptic curve of rank 1, so there are infinitely many rational solutions. Since t must also be an integer only finitely many of these are relevant, but the argument presented above is easier than trying to find which rational points on the curve give integral values of t directly.

Finally, note that $\mathbb{Q}(\sqrt{-7})$ is missing from this list. This is because 2 is split. The class number one condition only implied that primes less than $\frac{1+7}{4} = 2$ are inert, so this is not a problem. But every imaginary quadratic field with discriminant at least 12 does appear as predicted.

9.4. **The Relationship with Heegner's Argument.** The fact that this solution reduced to the same Diophantine equations as Heegner's method suggests they are closely related. Essentially, what happened is that the modular functions in Heegner's proof are explicit descriptions of functions on $X^+_{ns}(n)$. The connection between γ_2 and the uniformizer s for $X^+_{ns}(3)$ is simplest, so we will start with that.

Section 3.1 showed that $\gamma_2(z)$ was a modular function on

$$H \backslash \mathcal{H}^*$$

where H was found to be

$$H := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 0 \mod 3 \quad \text{or} \quad b \equiv c \mod 3 \right\}.$$

However, we can also write down $\Gamma_{C^+_{ns}(3)}$ using explicitly $R = \mathbb{Z}[i]$ and the description of $C^+_{ns}(3)$ in Lemma 49. They are exactly the matrices of H. Thus γ_2 is the uniformizer for $X^+_{ns}(3)$ over $X(1)$. Using the analytic formula $j = \gamma_2^3$, we immediately get Theorem 50 without thinking about ramification.

So what happens for $X^+_{ns}(24)$? Even the uniformizer for $X^+_{ns}(8)$ looks vastly more complicated than anything appearing in Heegner's proof. On the other hand, Theorem 23 looks like the relation between two uniformizers. One of the uniformizers is γ_2, the other would be one for a curve above $X^+_{ns}(3)$. It can't be one for $X^+_{ns}(24)$ over $X^+_{ns}(3)$ since $X^+_{ns}(24)$ has genus 1. So instead of thinking of uniformizers, it is better to think of minimal polynomials. Theorem 23 can be interpreted as giving the minimal polynomial $\mathfrak{f}_2^2$ over $\mathbb{C}(X^+_{ns}(3)) = \mathbb{C}(\gamma_2)$.

The next question is for which congruence subgroup is $\mathfrak{f}_2^2$ a modular function. By Proposition 33, we know it has level 24. We also have a description of $C^+_{ns}(24)$. We can lift each element (or find generators and lift them), write the result in terms of the generators of $\mathrm{SL}_2(\mathbb{Z})$, and use Proposition 31 to see if $\mathfrak{f}_2^2$ is invariant under $C^+_{ns}(24)$. It is easy to verify with a computer that of the 192 elements of $C^+_{ns}(24)$, $\mathfrak{f}_2^2$ is invariant under 64. Thus it is a modular function on a curve X that admits a degree 3 map to $X^+_{ns}(24)$. Choose this map so it is rational, and let f be a modular function on X defined over $\mathbb{Q}$. If $P \in X^+_{ns}(24)$ is a rational point, then the three points Q_i above P are permuted among themselves by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This forces $f(Q_i)$ to be an algebraic number of degree 3. This is exactly the situation we see in Heegner's proof, as α^2 is an algebraic integer of degree 3 whenever the quadratic field has class number one. So in some sense Heenger's argument finds the rational points on $X^+_{ns}(24)$ by looking at an even larger curve.

The resulting Diophantine equation is much nicer than the one obtained from combining $X^+_{ns}(8)$ and $X^+_{ns}(3)$ because $\mathfrak{f}_2^2$ is invariant under more than the 64 elements of $\mathrm{SL}_2(\mathbb{Z}/24\mathbb{Z})$

in $C_{ns}^{+}(24)$ found above. A computer search on $\mathrm{SL}_2(\mathbb{Z}/24\mathbb{Z})$ finds it is invariant under 256 elements (for example, it is invariant under $\begin{pmatrix} 1 & 1 \\ 22 & 23 \end{pmatrix}$ which is not in $C_{ns}^{+}(24)$). Let Y be the corresponding curve. By comparing sizes of subgroups of $\mathrm{SL}_2(\mathbb{Z}/24\mathbb{Z})$, it follows that the projection $Y \to X_{ns}^{+}(3)$ is of degree 12, which matches the explicit polynomial for $\mathfrak{f}_2^2$ produced in Theorem 23. Thus Heegner's approach really is essentially the same as Serre's approach with $N = 24$, but is cleaner because it works on a related modular curve to simplify the relations between the modular functions.

References

1. Alan Baker, *Linear forms in logarithms of algebraic numbers*, Mathematika (1966), 204–216.
2. Burcu Baran, *A modular curve of level 9 and the class number one problem*, Journal of Number Theory (2009), 715–728.
3. ______, *Normalizers of non-split cartan subgroups, modular curves and the class number one problem*, Journal of Number Theory (2010), 2753–2772.
4. B. J. Birch, *Weber's class invariants*, Mathematika (1969), 283–294.
5. Imin Chen, *On siegel's modular curve of level 5 and the class number one problem*, Journal of Number Theory (1999), 278–297.
6. Henri Cohen, *Number theory vol i: Tools and diophantine equations*, Springer, 2007.
7. David A. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley and Sons, 1989.
8. Fred Diamond and Jerry Shurman, *A first course in modular forms*, Springer, 2005.
9. Kurt Heegner, *Diophantische analysis und modulfunktionen*, Math. Zeit. (1952), 227–253.
10. Serge Lang, *Elliptic functions*, Springer-Verlag, 1987.
11. *SAGE mathematics software, version 4.6.2*, http://www.sagemath.org.
12. Reinhard Schertz, *Complex multiplication*, Cambridge University Press, 2010.
13. Jean-Pierre Serre, *A course in arithmetic*, Springer, 1973.
14. ______, *Lectures on the mordell-weil theorem*, ch. Appendix: The Class Number 1 Problem and Integral Points on Modular Curves, Vieweg, 1989.
15. Joseph Silverman, *The arithmetic of elliptic curves*, Springer, 2009.
16. H. M. Stark, *A complete determination of the complex quadratic fields of class number one*, Michigan Mathematics Journal (1967), 1–27.
17. H. M. Stark, *On the "gap" in a theorem of heegner*, Journal of Number Theory (1969), 16–27.
18. H. Weber, *Lehrbuch der algebra*, vol. 3, Chelsea, 1961.