CM-values of p-adic Theta-functions

Daas, M.A.

CHAPTER 1

The work of Gross and Zagier

Let $E/\mathbb{Q}$ an elliptic curve and let r_{alg} denote the rank of the group $E(\mathbb{Q})$, which is finite by the Mordell-Weil theorem. We may associate to E an L-function

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

which converges as soon as $\text{Re}(s) > 3/2$ and which by the modularity theorem, proved by Wiles and Taylor, allows an analytic continuation to the whole complex plane. The *Conjecture of Birch and Swinnerton-Dyer* predicts that the order of vanishing r_{an} of $L(E,s)$ at $s=1$, often referred to as the *analytic rank* of E, is equal to the *algebraic rank* r_{alg}. More precisely, it relates the non-zero value of the r_{an}-th derivative $L^{(r_{\text{an}})}(E,1)$ to various arithmetic invariants associated with the elliptic curve $E/\mathbb{Q}$.

In its complete generality, this *BSD-conjecture*, as it has come to be known, is still open. In fact, it is listed as one of the *Millennium Problems* by the Clay Mathematics Institute and is widely recognised as one of the most important and influencial conjectures in all of modern mathematics. As of today, almost all the partial progress towards the conjecture has been achieved for curves with rank at most 1.

The work of Gross, Kohnen and Zagier in [GZ86, GKZ87] constitutes a rare instance of such progress on this notoriously difficult open problem. The former gave a relation between the heights of Heegner divisor classes on the Jacobian of modular curves and the first derivatives at $s=1$ of the L-series of certain modular forms. The latter computed the height pairings of two distinct Heegner divisor classes to show that related quantities can be suitably combined to form the Fourier coefficients of a Jacobi form.

More concretely, using the theory of Heegner points, Theorem 7.4 in [GZ86] shows the following for elliptic curves $E/\mathbb{Q}$ with $L(E,1)=0$. If Ω_E denotes the real period of a regular differential on E, then for the explicitly computable $\alpha \in \mathbb{Q}$ as predicted by the BSD-conjecture and for some $P \in E(\mathbb{Q})$, it holds that

$$L'(E,1) = \alpha \cdot \Omega_E \cdot \langle P, P \rangle,$$

where $\langle -,- \rangle$ denotes the canonical global height pairing on $E(\mathbb{Q})$. In particular, this proves that, if $r_{\text{an}} = 1$, then we must have $r_{\text{alg}} \geq 1$.

Later, by varying one of the discriminants instead, the heights of Heegner cycles were also shown in [KRY04] to be connected to the derivative of a weight $3/2$ Eisenstein series for $\text{SL}_2(\mathbb{Z})$. The *Kudla program* aims to study the arithmetic properties of the first derivative of certain Eisenstein series and to connect these with a specific class of arithmetic

cycles and the special values of certain L-functions. Another relevant instance of a result in this direction can be found in [Sch09].

This thesis aims to generalise the collaborative work [GZ84] by Gross and Zagier that precedes the results of [GZ86, GKZ87] described above. In view of these results, the setting in [GZ84] can be regarded as the $X_0(1)$-case of the work done in [GZ86] and [GKZ87], the height pairing on whose Jacobian vanishes by virtue of the curve being of genus zero. Similarly, our main theorems will reflect the results in [GZ84] and we explain in Remark 2.3.1 how these results are to be interpreted in a more general framework as is done above.

This first introductory chapter contains very little original work and its purpose is mainly to provide the reader with the necessary background information to fully appreciate the context within which the main results of this thesis are best viewed. In particular, we investigate the main results of [GZ84] and interpret both its statement and its proofs to justify the ways in which this thesis aims to generalise them.

1.1 Classical CM-theory

The formulation of *class field theory* in the 20th century has been one of the greatest achievements in the field of algebraic number theory, describing the structure of all abelian extensions of a number field in terms of the arithmetic inside this field. In particular, it promises for every number field K an abelian extension called the *Hilbert class field* H_K which is unramified at every prime and maximal for this property. Even though its existence is known, its explicit construction and that of other class fields in complete generality has been a long standing open problem, known both as Kronecker's *Jugendtraum* and as Hilbert's 12th Problem. At the International Congress of Mathematicians in the year 1900, Hilbert called this problem "one of the most profound and far reaching in the theory of numbers and of functions".

All abelian extensions of $\mathbb{Q}$ are described by the Kronecker-Weber Theorem, which produces these extensions as generated by values of the function $r \mapsto e^{i\pi r}$ for $r \in \mathbb{Q}$; also known as roots of unity. The most natural next step would be to consider the class fields associated with quadratic extensions of $\mathbb{Q}$ and to attempt to find a function similar to the one above that mimics this striking property.

For *imaginary* quadratic fields, such results were obtained through study of Klein's j-function, given by

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

where $\mathbf{q} = e^{i\pi\tau}$ and $\tau \in \mathcal{H}$. This function is also integral to the study of isomorphism classes of elliptic curves, as it yields an isomorphism

$$j : \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H} \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}).$$

This work does not introduce the concept of elliptic curves; we assume the reader to be familiar with these objects. For a comprehensive introduction to elliptic curves, we refer the reader to Silverman's excellent *The Arithmetic of Elliptic Curves* [Sil09].

Throughout this section, K will be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. One may compute for instance that

$$j(\sqrt{-5}) = 2^6 \cdot 5 \cdot (1975 + 884\sqrt{5}).$$

One may then observe that $H = K(\sqrt{5})$ is in fact the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$, the field over which the input is defined. One of the key results of classical CM theory is that this is no coincidence, and in fact holds very generally. Until recently, the case of CM-fields were the only class of number fields for which explicit class field theory had been provably realised, though large breakthroughs have been made recently by Dasgupta and Kakde in their works [DK23a] and [DK23b]. The CM-values of the j-function are often called *singular moduli*.

To explain the results from CM theory most conceptually, we opt to approach the classical theory of complex multiplication in a modern adèlic language that will allow for swift and intuitive generalisations to the setting of Shimura curves in Chapter 2, as will be the focus of this thesis. Let $\widehat{\mathbb{Z}}$ denote the profinite integers and let $\mathcal{K} \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be a compact open subgroup. Examples of $\mathcal{K}$ include the closures of congruence subgroups of $\mathrm{GL}_2(\mathbb{Z})$ inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For each such $\mathcal{K}$, we may define the open modular curve $Y_{\mathcal{K}}$ through the following adèlic description:

$$Y_{\mathcal{K}}(\mathbb{C}) = (\mathcal{K} \cap \mathrm{SL}_2(\mathbb{Z})) \setminus \mathcal{H} \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Q}) \setminus \left(\mathcal{H}^{\pm} \times \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})/\ \mathcal{K}\right),$$

where $\mathcal{H}^{\pm} = \mathbb{C} \setminus \mathbb{R}$ denotes the union of the two half planes. This isomorphism sends $\tau \in \mathcal{H}$ to the object $\mathrm{GL}_2(\mathbb{Q})\,(\tau, 1 \cdot \mathcal{K})$.

We will fix an embedding $\alpha : \mathcal{O}_K \to M_2(\mathbb{Z})$ and we let $\tau \in \mathcal{H}$ denote the unique fixed point of the image of α under its action on $\mathcal{H}^{\pm}$. Then $\tau \in \mathcal{H}$ denotes a choice of a *CM-point* in the upper half plane. Since $K^{\times}$ is a dense subgroup of $\mathbf{A}_K^{\mathrm{fin},\times}$, by continuity α extends uniquely to an embedding $\mathbf{A}_K^{\mathrm{fin},\times} \to \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})$, which we will by slight abuse of notation also denote by α. Then we obtain a natural map

$$K^{\times} \setminus \mathbf{A}_K^{\mathrm{fin},\times} \to \mathrm{GL}_2(\mathbb{Q}) \setminus \left(\mathcal{H}^{\pm} \times \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})\right),$$

which sends some idèle $s \in \mathbf{A}_K^{\mathrm{fin},\times}$ to the pair $(\tau, \alpha(s))$. Note that this is well-defined, as the image of $K^\times$ fixes τ by definition. We stress that $K^\times \setminus \mathbf{A}_K^{\mathrm{fin},\times} = K^\times \mathbb{C}^\times \setminus \mathbf{A}_K^\times$, and thus by global class field theory this is isomorphic to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ using the Artin map, denoted by $[-, K]$. The following theorem is often referred to as the *Main Theorem of Complex Multiplication*, see Theorem 4.19 in [Del71].

Theorem 1.1.1. *Consider the following commutative diagram:*

$$\begin{array}{ccc} K^\times \setminus \mathbf{A}_K^{\mathrm{fin},\times} & \longrightarrow & \mathrm{GL}_2(\mathbb{Q}) \setminus \left(\mathcal{H}^\pm \times \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})\right) \\ {\scriptstyle [-,K]}\downarrow & & \downarrow{\scriptstyle /\ \mathcal{K}} \\ \mathrm{Gal}(K^{\mathrm{ab}}/K) & \overset{\eta}{\dashrightarrow} & Y_{\mathcal{K}}(\mathbb{C}). \end{array}$$

Then the image of η is contained in $Y_{\mathcal{K}}(\overline{\mathbb{Q}})$ and η is Galois-equivariant.

We illustrate its power by deducing from this an adèlic version of *Shimura reciprocity*, specialising to the CM-points on the curve $Y_0(1)$. Recall that every left-ideal in $M_2(\mathbb{Z})$ is principal.

Corollary 1.1.2. *Let $\tau \in \mathcal{H}$ be the CM-point associated with the embedding $\alpha : \mathcal{O}_K \to M_2(\mathbb{Z})$. Then it holds that $j(\tau) \in H$. Further, let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal and let $x \in M_2(\mathbb{Z})$ be such that $\alpha(\mathfrak{a})M_2(\mathbb{Z}) = x \cdot M_2(\mathbb{Z})$. Then it holds that*

$$j(\tau)^{[\mathfrak{a}, H_K/K]} = j(x^{-1} \cdot \tau),$$

where $x^{-1} \cdot \tau \in \mathcal{H}$ is a CM-point for the embedding $x^{-1}\alpha(-)x$.

Proof. We apply Theorem 1.1.1 in that case that $\mathcal{K} = \mathrm{GL}_2(\widehat{\mathbb{Z}})$. For $s \in \mathbf{A}_K^{\mathrm{fin},\times}$, the map η from Theorem 1.1.1 is given by

$$\eta([s, K]) = \mathrm{GL}_2(\mathbb{Q}) \left(\tau, \alpha(s)\mathrm{GL}_2(\widehat{\mathbb{Z}})\right).$$

To work out which point on the modular curve this corresponds to, we recall the easy to check equality of groups $\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}} = \mathbb{Q}\widehat{\mathbb{Z}}$, and using strong approximation results, one can deduce from this that also

$$\mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}}) = \mathrm{GL}_2(\mathbb{Q})\mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

We may then decompose

$$\alpha(s) = xy \quad \text{with} \quad x \in \mathrm{GL}_2(\mathbb{Q}) \quad \text{and} \quad y \in \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

We then find that

$$\begin{aligned}\mathrm{GL}_2(\mathbb{Q})\left(\tau, \alpha(s)\mathrm{GL}_2(\widehat{\mathbb{Z}})\right) &= \mathrm{GL}_2(\mathbb{Q})\left(\tau, xy\mathrm{GL}_2(\widehat{\mathbb{Z}})\right)\\ &= \mathrm{GL}_2(\mathbb{Q})\left(x^{-1}\tau, 1\cdot \mathrm{GL}_2(\widehat{\mathbb{Z}})\right).\end{aligned}$$

In other words, we may describe the map $\eta : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to Y_0(1)(\overline{\mathbb{Q}})$ by the formula

$$\eta([s,K]) = x^{-1}\tau \in \mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H};$$

this is well-defined because the ambiguity in the choices of x and y is measured by $\mathrm{GL}_2(\mathbb{Q})\cap\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \mathrm{GL}_2(\mathbb{Z})$. Set $U = \prod_v \mathcal{O}_v^\times$, where the product is taken over all finite places v of K. If $s \in U$, then by continuity it follows that $\alpha(s) \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and therefore we may take $x = 1$. This shows once again that the CM-point τ is defined over the Hilbert class field H of K.

To refine this, we must consider more general $s \in \mathbf{A}_K^{\mathrm{fin},\times}$ such that $[s,K]|_H = [\mathfrak{a}, H/K]$. We claim that the $M_2(\mathbb{Z})$-ideal generated by the image $\alpha(\mathfrak{a})$ is equal to $x\cdot M_2(\mathbb{Z})$ with x as defined above. To see this, we recall that the quotient

$$\mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})/\mathrm{GL}_2(\widehat{\mathbb{Z}})$$

is in bijection with set of fractional $M_2(\mathbb{Z})$-ideals inside $M_2(\mathbb{Q})$. Indeed, any such class can be represented by an element from $\mathrm{GL}_2(\mathbb{Q})$, which defines a fractional $M_2(\mathbb{Z})$-ideal inside $M_2(\mathbb{Q})$ as this element is well-defined up to an element from $\mathrm{GL}_2(\mathbb{Z})$, which does not affect the resulting $M_2(\mathbb{Z})$-ideal. This shows that indeed $\alpha(s)$ induces the ideal $x\cdot M_2(\mathbb{Z})$ and thus so will $\alpha(\mathfrak{a})$ by virtue of our choice of s. □

1.2 Singular moduli

In their paper [GZ84], Gross and Zagier studied the differences between singular moduli. For example,

$$j\left(\frac{1+\sqrt{-43}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) = 2^{19}\cdot 3^6\cdot 5^3\cdot 7^3\cdot 37\cdot 433. \tag{1.1}$$

Aside from this number being rather smooth, one may observe that all its prime divisors are inert in both $\mathbb{Q}(\sqrt{-43})$ and $\mathbb{Q}(\sqrt{-163})$. More precisely, all of these primes occur as the factor of a number of the form $43\cdot 163 - x^2$ for some $|x| < \sqrt{43\cdot 163}$, as the equality $43\cdot 163 - 9^2 = 16\cdot 433$

exemplifies. These patterns persist when repeating the experiment with other, possibly non-rational singular moduli if one takes the norm down to $\mathbb{Q}$. This thesis aims to study factorisation phenomena that display a parallel with the observations made and subsequently explained by Gross and Zagier in [GZ84].

Before stating the factorisation formulas, we require some notation. Suppose that m is an integer supported at primes that are not inert in $F/\mathbb{Q}$. Assume that there is a unique prime ℓ both dividing m an odd number of times, say $2k+1$ times, with the additional property that any prime ideal $\mathfrak{l}$ of F above ℓ satisfies $\chi(\mathfrak{l}) = -1$. We will call such primes the *special* primes of the integer m; terminology that we will use again in Chapter 6. Further, let $\{c_i\}$ be the set of exponents of primes dividing m with the property that all primes of F lying above them split in L/F. Then we set

$$F(m) := \ell^X \quad \text{where} \quad X = (k+1)\prod(c_i+1),$$

and simply $F(m) = 1$ for all other $m \in \mathbb{Q}$. Finally, let $\tau_1, \tau_2 \in \mathcal{H}$ be CM-points of discriminants D_1 and D_2 respectively. Then Gross and Zagier proved the following in [GZ84].

Theorem 1.2.1. *With all notation from above, it holds that*

$$\mathrm{Nm}_{\mathbb{Q}}\big(j(\tau_1) - j(\tau_2)\big)^{\frac{8}{w_1 w_2}} = \pm \prod_{\substack{x^2 < D \\ x^2 \equiv D \bmod 4}} F\left(\frac{D-x^2}{4}\right).$$

We illustrate this theorem in a few simple cases for discriminants of class number 1. We record here the following CM curves:

$$E_7 : y^2 + xy = x^3 - x^2 - 2x - 1 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right];$$

$$E_{11} : y^2 + y = x^3 - x^2 - 7x + 10 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right];$$

$$E_{19} : y^2 + y = x^3 - 38x + 90 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right];$$

$$E_{43} : y^2 + y = x^3 - 860x + 9707 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right].$$

One computes from this the quantities

$$j(E_7) = -3^3 5^3; \quad j(E_{11}) = -2^{15};$$
$$j(E_{19}) = -2^{15} 3^3; \quad j(E_{43}) = -2^{18} 3^3 5^3.$$

Example 1.2.2. Let us first choose $D_1 = -7$ and $D_2 = -11$. Then $D = D_1 D_2 = 77$, and so we make the following table.

x	± 1	± 3	± 5	± 7
$\frac{D-x^2}{4}$	19	17	13	7
$F(\frac{D-x^2}{4})$	19	17	13	7

Indeed, one computes that

$$j(E_7) - j(E_{11}) = -3^3 5^3 + 2^{15} = 29393 = 7 \cdot 13 \cdot 17 \cdot 19,$$

as predicted by Theorem 1.2.1. Note here that the norm of the rational invariant down to $\mathbb{Q}$ is just the identity, and the exponent $8/(w_1 w_2) = 2$ corresponds to the fact that we double count each entry in our table by virtue of $\pm x$ giving the same outcome.

Example 1.2.3. Let us now choose $D_1 = -7$ and $D_2 = -19$. Then $D = D_1 D_2 = 171$, and so we make the following table.

x	± 1	± 3	± 5	± 7	± 9	± 11
$\frac{D-x^2}{4}$	$3 \cdot 11$	31	3^3	$3 \cdot 7$	13	3
$F(\frac{D-x^2}{4})$	3^2	31	3^2	3^2	13	3

One might enjoy verifying that

$$j(E_7) - j(E_{19}) = -3^3 5^3 + 2^{15} 3^3 = 881361 = 3^7 \cdot 13 \cdot 31,$$

which agrees with Theorem 1.2.1.

Example 1.2.4. Finally, we choose $D_1 = -7$ and $D_2 = -43$. Then $D = D_1 D_2 = 301$, and so we make the following table.

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3
$F(\frac{D-x^2}{4})$	3	73	3^2	7	5^2	5	3^2	19	3

We leave it to the reader to check that indeed,

$$j(E_7) - j(E_{43}) = -3^3 5^3 + 2^{18} 3^3 5^3 = 884732625 = 3^6 \cdot 5^3 \cdot 7 \cdot 19 \cdot 73,$$

in perfect accordance with Theorem 1.2.1.

Gross and Zagier in [GZ84] gave two proofs of this formula, and the dissimilarities between these proofs cannot be overstated. In this section we briefly discuss their first proof, and leave a discussion of the second to Section 1.6. The idea of this first proof is to count and compare the prime factors of both sides of the equality proposed by Theorem 1.2.1. As the right hand side is already expressed in fairly elementary terms, the difficulty comes from analysing the left hand side. The starting point for this method is Proposition 2.3 in [GZ84], which reads as follows.

Theorem 1.2.5. *Let ℓ be a prime number and let A be the complete discrete valuation ring of a finite field extension of $\mathbb{Q}_\ell^{\mathrm{unr}}$. Let π be a uniformiser and let v be the discrete valuation on A satisfying $v(\pi) = 1$. Let E_1 and E_2 be elliptic curves over A with good reduction and associated j-invariants $j_1, j_2 \in A$. For any positive integer n, let $\mathrm{Iso}_n(E_1, E_2)$ denote the number of isomorphisms from E_1 to E_2 defined over the ring A/π^n. Then*

$$2v(j_1 - j_2) = \sum_{n \geq 1} \mathrm{Iso}_n(E_1, E_2).$$

This formula refines the elementary observation that for elliptic curves $E_1, E_2/\mathbb{Q}$ with good reduction at a rational prime ℓ, it holds that

$$\ell \mid j_1 - j_2 \iff \overline{E}_1 \xrightarrow{\sim} \overline{E}_2 \quad \text{over } \overline{\mathbb{F}}_\ell.$$

According to Theorem II.6.1 in [Sil94], the algebraic numbers j_1 and j_2 are in fact algebraic integers, implying that both E_1 and E_2 have potentially good reduction at the prime ℓ. Therefore, the assumption of good reduction in Theorem 1.2.5 above is not in fact a restriction and may be assumed without loss of generality.

We thus reduce to determining the numbers $\mathrm{Iso}_n(E_1, E_2)$ for each positive integer n. The next key observation is that if E_1 and E_2 have CM by $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively, in case this quantity is non-zero, both $\overline{E}_1 \cong \overline{E}_2/\overline{\mathbb{F}}_\ell$ must have supersingular reduction at ℓ. Indeed, for $i \in \{1, 2\}$, we have an injective map

$$\alpha_i : \mathcal{O}_i \to \mathrm{End}(\overline{E}/\overline{\mathbb{F}}_\ell).$$

If E_1 and E_2 instead had ordinary reduction at ℓ, this endomorphism ring would have been an order in an imaginary quadratic field, and as such would not have been able to receive embeddings from two such orders of different coprime discriminants.

We recall the Deuring correspondence. Let B_ℓ denote the definite rational quaternion algebra ramified only at ℓ and ∞. We fix a maximal order $R_\ell \subset B_\ell$.

Let $E/\overline{\mathbb{F}}_\ell$ be a fixed supersingular elliptic curve equipped with an isomorphism $\eta : \mathrm{End}(E) \xrightarrow{\sim} R_\ell$ which we may $\mathbb{Q}$-linearly extend to an isomorphism $\eta : \mathrm{End}(E)\otimes\mathbb{Q} \xrightarrow{\sim} B_\ell$. For any integral left R_ℓ-ideal $I \subset R_\ell$, one may define the group scheme theoretic intersection

$$E[I] := \bigcap_{\alpha\in I} E[\eta^{-1}(\alpha)] \quad \text{and set} \quad E_I := E/E[I].$$

The elliptic curve E_I is again supersingular and comes with a natural projection morphism $\phi_I : E \to E_I$. Lemma 42.2.7 in [Voi21] states that the map

$$f_I : \mathrm{Hom}(E_I, E) \xrightarrow{\sim} I : \psi \mapsto \eta(\psi\phi_I)$$

is an isomorphism of left R-modules. Now the Deuring correspondence, Theorem 42.3.2 in [Voi21], states the following.

Theorem 1.2.6. *Let $E_0/\overline{\mathbb{F}}_\ell$ be a fixed supersingular elliptic curve with $\mathrm{End}(E_0) \cong R_\ell$. Then the associations*

$$E \mapsto \mathrm{Hom}(E, E_0) \quad \textit{and} \quad E_I \nleftarrow I$$

define an equivalence between the categories of supersingular elliptic curves over $\overline{\mathbb{F}}_\ell$ and the category of invertible left R_ℓ-modules.

This allows us to transpose the problem at hand into a counting problem inside the quaternion algebra B_ℓ. Let $x_2 \in A$ denote a fixed element satisfying a quadratic equation over $\mathbb{Q}$ with discriminant D_2. As is explained in [GZ84], each $f \in \mathrm{Iso}_n(E_1, E_2)$ gives rise, through the association $f \mapsto f^{-1} \circ [x_2] \circ f$, to an endomorphism of E_1 modulo π^n with trace and norm equal to that of x_2, also inducing multiplication by x_2 on $\mathrm{Lie}(E_1)$. To prove this is a bijective correspondence, one requires the following refinement of a theorem by Deuring; this is Proposition 2.7 in [GZ84].

Proposition 1.2.7. *Given any elliptic curve $\widetilde{E}$ over A/π^n and an endomorphism $\widetilde{[x_2]} : \widetilde{E} \to \widetilde{E}$ with the properties above, there exists an elliptic curve E over A and an endomorphism $[x_2]$ of E, unique up to isomorphism, lifting the pair $(\widetilde{E}, \widetilde{[x_2]})$ such that $[x_2]$ induces multiplication by x_2 on $\mathrm{Lie}(E)$.*

This means that, to determine the sizes of the sets

$$\left\{ f^{-1} \circ [x_2] \circ f \;\middle|\; f \in \mathrm{Iso}_n(E_1, E_2) \right\} \subset \mathrm{End}(E_1 \mod \pi^n),$$

we may instead consider the sets

$$S_n := \big\{ g \in \mathrm{End}(E_1 \mod \pi^n) \mid \mathrm{tr}(g) = \mathrm{tr}(x_2), \\ \mathrm{Nm}(g) = \mathrm{Nm}(x_2), \quad g = x_2 \text{ on } \mathrm{Lie}(E_1) \big\}.$$

To determine the cardinalities of these sets, we use the explicit description of $\mathrm{End}(E_1 \mod \pi^n)$ from Lemma 3.5 in [GZ84]. It claims that

$$B_\ell \cong \left\{ \begin{pmatrix} \alpha & \beta \\ -\ell\overline{\beta} & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in K_1 \right\} \subset M_2(K_1),$$

and this isomorphism sends $\mathrm{End}(E_1 \mod \pi^n)$ to those matrices satisfying that $\alpha \in \mathcal{D}_{K_1}^{-1}$, the inverse different of K_1, and $\beta \in \mathcal{D}_{K_1}^{-1}\ell^{n-1}\overline{\mathfrak{a}}/\mathfrak{a}$, further satisfying that $\alpha \equiv \lambda\beta \mod \mathcal{O}_1$. Here λ is such that $\lambda^2 \equiv -\ell \mod \mathcal{D}_{K_1}$ and $\mathfrak{a} \subset K_1$ is a fractional ideal of K_1 determined by the precise prime above ℓ of H_1 we are considering.

Finally, this counting problem is solved in the remainder of Section 3 in [GZ84] for all possible splitting behaviours of the prime ℓ in the fields K_1 and K_2. This allows one to finally compare the result to the right hand side of Theorem 1.2.1, completing the first proof.

1.3 Intersection numbers of embeddings

In this section, we describe an alternative formulation of Theorem 1.2.1 described above. Namely, key to the algebraic proof of Theorem 1.2.1 were the existence of two embeddings

$$\alpha_i : \mathcal{O}_i \to \mathrm{End}(\overline{E}),$$

where the latter ring is a maximal order inside the quaternion algebra B_ℓ. Both to formulate and to prove our generalisations of Theorem 1.2.1, which will be the main focus of this thesis, in the chapters that follow we will also work with such embeddings, so we elaborate on how these concepts occur in the original setting of [GZ84] as well.

Suppose that a prime ℓ is inert in both $\mathcal{O}_1$ and $\mathcal{O}_2$. Fix a set of representative left R_ℓ-ideals $\mathrm{Cl}_L(R) = \{I_1, I_2, \ldots, I_n\}$ for the left-class set of R. Define $R_j := R_{I_j}$ as the associated right order for the ideal I_j for $j \in \{1, \ldots, n\}$, so that all conjugacy classes of maximal orders of B_ℓ occur either once or twice among the R_j.

By Corollary 1.1.2, for $i \in \{1, 2\}$, the elliptic curves E_i with CM by $\mathcal{O}_i$ are a principal homogeneous space for the action of $\mathrm{Pic}(K_i)$. Therefore,

the number of elliptic curves E_i with CM by $\mathcal{O}_i$ is given by h_i, where h_i denotes $\#\mathrm{Pic}(K_i)$.

Let $\alpha_1 : K_1 \to B_\ell$ and $\alpha_2 : K_2 \to B_\ell$ denote embeddings. For $\mathcal{O} \in \{\mathcal{O}_1, \mathcal{O}_2\}$ and $R \subset B_\ell$ a maximal order, define

$$\mathrm{Emb}(\mathcal{O}, R, R^\times) := \{\alpha : \mathcal{O} \to R\}/\sim,$$

where $\alpha \sim \beta$ if and only if $\alpha = \xi\beta\xi^{-1}$ for some $\xi \in R^\times$. Theorem 30.4.7 in [Voi21] states for $i \in \{1, 2\}$ that

$$\sum_{j=1}^{n} \#\mathrm{Emb}(\mathcal{O}_i, R_j, R_j^\times) = 2h_i.$$

Therefore, this set is in bijection with the set of elliptic curves with CM by $\mathcal{O}_i$ as considered above if we identify embeddings if they are equal after applying the involution on B_ℓ. This bijection suggests that $\mathrm{Pic}(K_i)$ acts on this set too and indeed that is so; we explore this further in Section 4.5. We stress here that we count each maximal order separately for each time it occurs as the right order of a left ideal class in the class group of B_ℓ, which can happen either once or twice, as explained in the first two sections of [Gro87].

Let $\mathfrak{l}$ be a prime above the prime number ℓ in the compositum of the fields $\mathbb{Q}(j(E_1))$ and $\mathbb{Q}(j(E_2))$, and let $v_\mathfrak{l}$ denote the $\mathfrak{l}$-adic valuation. Since ℓ is assumed inert in both K_i, it must split completely in the extension H_i/K_i for $i \in \{1, 2\}$. As such, the prime ℓ must split completely in $\mathbb{Q}(j(E_i))/\mathbb{Q}$ as well, and so both the set of primes $\mathfrak{l}$ above ℓ and the set of pairs of CM elliptic curves (E_1, E_2) up to isomorphism are principal homogeneous spaces for the action of $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$.

We may consider both E_1 and E_2 to be defined over $\mathbb{Q}(j(\tau_1), j(\tau_2))$, and we wish to determine

$$v_\mathfrak{l}\big(j_1(E_1) - j_2(E_1)\big).$$

In the previous section, we considered the reductions of E_1 and E_2 modulo $\mathfrak{l}$ and appealed to Theorem 1.2.5. Alternatively, one may note that the reduction maps induce embeddings $\alpha_i : \mathcal{O}_i \to \mathrm{End}(\overline{E}_i) \subset B_\ell$. Varying $\mathfrak{l}$, for both curves we get different reductions over $\overline{\mathbb{F}}_\ell$, which may induce embeddings into different maximal orders.

We write Γ_1 and Γ_2 for the subgroups stabilising the images of α_1 and α_2 respectively. It is easy to show that for $i \in \{1, 2\}$, it holds that $\#\Gamma_i = \#\mathcal{O}_i^\times$. As B_ℓ is a definite quaternion algebra, the group $R^\times$ is finite for any maximal order $R \subset B_\ell$. We will need the following definition, in the style of the PhD thesis of James Rickards [Ric21].

Definition 1.3.1. Let $i, j \in \{1, \dots, n\}$ and let $\alpha_1 : \mathcal{O}_1 \to R_i$ and $\alpha_2 : \mathcal{O}_2 \to R_j$ be two embeddings. If $i = j$, define the *intersection number* $(\alpha_1 \cap \alpha_2)_\ell$ to be the greatest $t \in \mathbb{N}$ for which $\mathrm{im}(\alpha_1)$ and $\mathrm{im}(\alpha_2)$ agree modulo $\ell^{t-1}R_i = \ell^{t-1}R_j$. If $i \neq j$, we set $(\alpha_1 \cap \alpha_2)_\ell = 0$.

It should be noted that embeddings into the same maximal order always have a positive intersection number. However, even if $R_i = R_j$ as sets but $i \neq j$, we still say that embeddings into R_i and R_j do not intersect. We now claim the following theorem.

Theorem 1.3.2. *Let E_1 and E_2 be elliptic curves with complex multiplication by $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively and let ℓ be a rational prime that is inert in both $\mathcal{O}_1$ and $\mathcal{O}_2$. Let $\mathfrak{l}$ be a prime of $\mathbb{Q}(j(E_1), j(E_2))$ above ℓ and let $\alpha_1 : \mathcal{O}_1 \to R_i$ and $\alpha_2 : \mathcal{O}_2 \to R_j$ for some $i, j \in \{1, \dots, n\}$ be the pair of embeddings that corresponds to it. Suppose that both E_1 and E_2 have good reduction at $\mathfrak{l}$. If $i \neq j$, then $\mathfrak{l} \nmid j(E_1) - j(E_2)$. If $i = j$, then*

$$v_{\mathfrak{l}}\big(j(E_1) - j(E_2)\big) = \sum_{\Gamma_1 \backslash R^\times / \Gamma_2} \big(\alpha_1 \cap (u\alpha_2 u^{-1})\big)_\ell,$$

where $R = R_i = R_j$ and $u \in \Gamma_1 \setminus R^\times / \Gamma_2$.

Proof. For the sake of exposition, we assume throughout the proof that $D_i \notin \{-3, -4\}$ for $i \in \{1, 2\}$, so that $\Gamma_1 \setminus R^\times / \Gamma_2 = R^\times / \{\pm 1\}$.

We appeal to Theorem 1.2.5 to reduce to showing that

$$2 \sum_{R^\times / \{\pm 1\}} \big(\alpha_1 \cap (u\alpha_2 u^{-1})\big)_\ell = \sum_{n \geq 1} \mathrm{Iso}_n(E_1, E_2).$$

Clearly both curves are supersingular at $\mathfrak{l}$. Theorem 1.2.6 immediately yields that $\overline{E}_1 \cong \overline{E}_2$ if and only if $i = j$. This proves the result in case $i \neq j$, for $\mathfrak{l} \mid j(E_1) - j(E_2)$ if and only if $\overline{E}_1 \cong \overline{E}_2$.

Now assume that $i = j$, so $\overline{E}_1 \cong \overline{E}_2$ and therefore $\mathrm{Iso}_1(E_1, E_2) \neq \varnothing$. We will prove the theorem by establishing for any n a bijection between $\mathrm{Iso}_n(E_1, E_2)$ and the set of $u \in R^\times / \{\pm 1\}$ such that

$$\big(\alpha_1 \cap (u\alpha_2 u^{-1})\big)_\ell \geq n,$$

from which the desired equality would immediately follow.

Let us first illustrate the simple case of $n = 1$. Then, the isomorphisms from E_1 to E_2 over $\overline{\mathbb{F}}_\ell$ are in bijection with the automorphisms of either $\overline{E}_i$ over that same field, which thus biject with $R^\times$. On the other hand, any $u \in R^\times$ will contribute at least 1 to the sum of intersection numbers on the left hand side. The factor of 2 makes up for our

dividing out by $\{\pm 1\}$. This concludes this case. For $n > 1$, we suppose that $\mathrm{Iso}_n(E_1, E_2) \neq \varnothing$, so there exists some isomorphism $f : E_1 \mod \ell^n \xrightarrow{\sim} E_2 \mod \ell^n$. As explained in the previous section, through the association $f \mapsto g_f := f^{-1} \circ [x_2] \circ f$ we obtain for each element $f \in \mathrm{Iso}_n(E_1, E_2)$ a unique endomorphism $g_f \in \mathrm{End}(E_1 \mod \ell^n)$ that satisfies the same equation as some fixed x_2 with $\mathcal{O}_2 = \mathbb{Z}[x_2]$. First note that $g_f \in \alpha_1(\mathcal{O}_1) \mod \ell^{n-1}R$. Indeed, from the explicit description of $\mathrm{End}(E_1 \mod \ell^n)$ from the previous section, we deduce, using the observation that $\ell^{n-1} \mid \beta$, that

$$\mathrm{End}(E \mod \ell^n) \equiv \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} \right\} = \alpha_1(\mathcal{O}_1) \mod \ell^{n-1}R,$$

where we also used that modulo ℓ^{n-1}, there is no difference between taking α inside $\mathcal{O}_1$ or D_{K_1} by the coprimality of D_1 with ℓ. The element g_f for each $f \in \mathrm{Iso}_n(E_1, E_2)$ defines an embedding $\mathcal{O}_2 \to R$. This embedding must be conjugate to α_2 through an element $u \in R^\times$ and by construction, the images of these embeddings must agree $\mod \ell^{n-1}R$. This element u is only uniquely defined in the group $R^\times/\{\pm 1\}$, so the association we constructed is injective. It remains to show that it is also surjective for each $n \geq 1$. Now suppose that some embedding $\beta_2 = u^{-1}\alpha_2(-)u : \mathcal{O}_2 \to R$ agrees with $\alpha_1 : \mathcal{O}_1 \to R$ modulo $\ell^{n-1}R$. Then in particular, we find that $\beta_2(x_2) \in \alpha_1(\mathcal{O}_1) \mod \ell^{n-1}R$. Using the isomorphism from Lemma 3.5 in [GZ84] as above, we conclude that it even holds that $\beta(x_2) \in \mathrm{End}(E \mod \ell^n)$ with trace, norm and action on $\mathrm{Lie}(E_1)$ identical to the element $x_2 \in \mathcal{O}_2$. As reasoned in the beginning of Section 3 of [GZ84], using their Proposition 2.7, every endomorphism with these properties must be of the form $f^{-1} \circ [x_2] \circ f$ for some $f \in \mathrm{Iso}_n(E_1, E_2)$. This proves surjectivity. □

1.4 Extended example

We illustrate Theorem 1.3.2 using the following singular moduli;

$$\begin{aligned} j\left(\frac{1+\sqrt{-67}}{2}\right) &= -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3; \\ j\left(\frac{1+\sqrt{-163}}{2}\right) &= -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3; \\ j\left(\frac{1+\sqrt{-67}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) &= 2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 139 \cdot 331. \end{aligned}$$

We will verify the formula from Theorem 1.3.2 for various rational primes. Throughout this section, we will for $x, y \in \mathbb{Q}^\times$ adopt the notation $(x,y)_\mathbb{Q}$ for the quaternion algebra over $\mathbb{Q}$ with the explicit $\mathbb{Q}$-basis

$$(x,y)_\mathbb{Q} := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

with the multiplication rules

$$i^2 = x, \quad j^2 = y \quad \text{and} \quad ij = -ji = k.$$

The trace form is given by $\mathrm{tr}(a + bi + cj + dk) = 2a$, and the norm by

$$\mathrm{Nm}(a + bi + cj + dk) = a^2 - xb^2 - yc^2 + xyd^2.$$

The prime $\ell = 2$

The algebra $B_2 = \mathbb{H} = (-1,-1)_\mathbb{Q}$ is that of the *Hamilton quaternions*. Its unique maximal order (up to conjugacy) is given by

$$R_2 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2}.$$

Computing its units of norm 1 is equivalent to solving $a^2+b^2+c^2+d^2 = 1$ in integers, or all half-integers. This yields 24 solutions, so the group of interest $\Gamma_1 \setminus R_2^\times / \Gamma_2$ consists of 12 elements.

To give embeddings of the rings of integers $\mathbb{Z}[(1+\sqrt{-67})/2]$ and $\mathbb{Z}[(1+\sqrt{-163})/2]$ into R_2, we must find quaternions satisfying

$$x^2 - x + 17 = 0 \quad \text{and} \quad x^2 - x + 41 = 0$$

respectively. This means that we are looking for $x \in R_2$ satisfying $\mathrm{tr}(x) = 1$ and $\mathrm{nrd}(x) = 17$ or $\mathrm{nrd}(x) = 41$ respectively. Clearly, the first condition amounts to specifying $a = 1/2$, so all other coefficients are half integers, and we reduce to expressing 67 and 163 as the sum of three odd squares respectively. We find among the solutions

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1 \pm 3i \pm 3j \pm 7k}{2}$$

and

$$\alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{1 \pm 9i \pm 9j \pm k}{2}.$$

Since the images x and $1-x$ are considered to induce the same embedding, one easily finds all 12 embeddings from the above examples for both discriminants.

To examine the formula from Theorem 1.3.2, we note that, since the quaternion algebra has a unique maximal order, by definition each of the 12 terms in the sum contributes at least 1. This already gives us 12 factors of 2, so we are left to justify the remaining $15 - 12 = 3$.

We let α_1 be given by the embedding above with only plus signs and investigate for which choices of α_2 the images of the embeddings agree modulo $2R_2$. One checks that this means that the coefficients in the numerators of the generators must all agree mod 4. This gives us

$$\frac{1-9i-9j-k}{2}, \quad \frac{1-i-9j-9k}{2}, \quad \text{and} \quad \frac{1-9i-j-9k}{2}.$$

One verifies that in each case, these elements do not agree modulo $4R_2$. We have thus found three embeddings for which the intersection number is 2. This brings our final number of factors of 2 in the difference to $9 + 2 \cdot 3 = 15$, as predicted by Theorem 1.3.2.

The prime $\ell = 3$

To analyse the situation at the prime $\ell = 3$, we must introduce $B_3 = (-1, -3)_{\mathbb{Q}}$. It has a maximal order given by

$$R_3 = \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k.$$

This time, we obtain 12 units of norm 1, so after dividing out by ± 1, the group $\Gamma_1 \backslash R_3^{\times} / \Gamma_2$ contains 6 elements. To construct the embeddings α_1 and α_2, we are again looking for elements of norms 17 and 41 respectively, of which the rational part equals 1/2. Similar to before, we find

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1+j}{2} + 2i + 2k.$$

For α_2, all possible images are given by

$$\frac{1 \pm 7j}{2} \pm i \pm k \quad \text{and} \quad \frac{1 \pm 7j}{2} \pm 2i.$$

Again, all of these embeddings contribute at least 1 to the sum of intersection numbers from Theorem 1.3.2, meaning that we have already found at least 6 factors of 3 in the difference between the j-invariants. Now we are left to compare the image of α_1 to the image of every possibility for α_2 modulo $3R_3$. One verifies that only $\frac{1+7j}{2} - i - k$ will do the trick. However, modulo $9R_3$, these images are distinct. This means that we get an intersection number of 2 for one embedding, bringing our final total of factors of 3 to $5 \cdot 1 + 2 = 7$, once more in accordance with our computations.

The prime $\ell = 5$

We once again start by introducing the quaternion algebra $B_5 = (-2, -5)_{\mathbb{Q}}$. Its unique conjugacy class of maximal orders has the representative

$$R_5 = \mathbb{Z}\frac{1+j+k}{2} + \mathbb{Z}\frac{i+2j+k}{4} + \mathbb{Z}j + \mathbb{Z}k.$$

Now we find 6 units in total, so that the group $\Gamma_1 \setminus R_5^\times / \Gamma_2$ consists of 3 elements. Examples of the embeddings are

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{2+3i+5k}{4} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{2+9i+7k}{4}.$$

The only other possibilities for the image of α_2 are

$$\frac{2-9i-7k}{4} \quad \text{and} \quad \frac{1}{2} \pm \left(\frac{11}{4}i - \frac{3}{4}k\right) \pm 2j.$$

We leave it to the reader to check that these are the only choices of signs that produces an element in R_5. There are no congruences to be found this time, yielding 3 factors of 5, as Theorem 1.3.2 predicts.

The prime $\ell = 7$

We continue to study $B_7 = (-1, -7)_{\mathbb{Q}}$. It has the maximal order

$$R_7 = \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k.$$

It is easy to see that in this case, we only have ± 1 and $\pm i$ as units of norm 1, so $\Gamma_1 \setminus R_5^\times / \Gamma_2$ has order 2. As for the embeddings, we find

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1+2i+3j}{2} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{1 \pm 10i \pm 3j}{2}$$

indeed giving us the $4/2 = 2$ embeddings that we expected. One checks that no choice of signs will result in orders that agree modulo $7R_7$. Therefore, both embeddings will only contribute 1 to the sum, giving 2 factors of 7 in total, once more as expected by Theorem 1.3.2.

The primes $\ell = 11$

This example is interesting because it is the smallest prime for which there is not a unique maximal order, but in fact there are two distinct conjugacy classes. We have $B_{11} = (-1, -11)_{\mathbb{Q}}$ and

$$R_{11}^1 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}\frac{1+j}{2}$$

and

$$R_{11}^2 = \mathbb{Z}\frac{1+j+2k}{2} + \mathbb{Z}\frac{i+2j+5k}{4} + \mathbb{Z}j + 2\mathbb{Z}k$$

are two representatives. For the possible embeddings, we only find

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1+13i-3k}{4} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{1+3j}{2} + 4i.$$

We see that α_1 and α_2 embed into different maximal orders of B_{11}, thus giving intersection number zero. Indeed, we did not find any factors of 11 in our difference of j-invariants.

The primes $\ell \geq 13$

For our last small prime that we will check, we record that $B_{13} = (-2,-13)_{\mathbb{Q}}$ and now there is a unique conjugacy class of maximal order again, given by

$$R_{13} = \mathbb{Z}\frac{1+j+k}{2} + \mathbb{Z}\frac{i+2j+k}{4} + \mathbb{Z}j + \mathbb{Z}k.$$

The units of norm 1 are given by ± 1, so that we will get *unique* embeddings α_1 and α_2, given by

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{2 \pm (11i+k)}{4} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{2 \pm (i-5k)}{4}.$$

A moment's inspection now shows that these embeddings do not agree modulo $13R_{13}$, thus giving an intersection number of 1. We therefore get 1 factor of 13 in the difference of j-invariants, as expected from the numbers themselves and Theorem 1.3.2.

For embeddings α_1 and α_2 to exist in the first place, the prime ℓ must be inert in both K_1 and K_2. In our case, this already shows that our difference in j-invariants will have no factors of ℓ for all $13 < \ell < 31$. Using this elementary observation, we may already disregard 75% of all primes from our considerations. Of those that remain, one should find that only for $\ell = 139$ and $\ell = 331$ there will be embeddings that map into the same maximal order; for all other primes, the embeddings will land inside distinct maximal orders. The number of distinct maximal orders grows approximately as $\ell/12$ as ℓ increases; a precise formula can be found in the first chapter of [Gro87]. Therefore, it will become increasingly unlikely that two embeddings will belong to the same maximal order, thus contributing a prime factor to the difference of j-invariants.

1.5 Irrational examples

To illustrate the way in which Theorem 1.3.2 is in some sense more refined than Theorem 1.2.1, we must consider irrational singular moduli. Recall that the field $\mathbb{Q}(\sqrt{-5})$ has class number 2, whereas $\mathbb{Q}(\sqrt{5})$ has class number 1. In this section, we will consider the following values:

$$\begin{aligned} j\left(\sqrt{-5}\right) &= 2^6 \cdot 5 \cdot (1975 + 884\sqrt{5}); \\ j\left(\frac{1+\sqrt{-7}}{2}\right) &= -3^3 \cdot 5^3; \\ j\left(\sqrt{-5}\right) - j\left(\frac{1+\sqrt{-7}}{2}\right) &= (2+\sqrt{5}) \cdot 5\sqrt{5} \cdot 13 \cdot 17 \cdot (8+3\sqrt{5}) \cdot (6+\sqrt{5}). \end{aligned}$$

Note that $\mathrm{Nm}(2+\sqrt{5}) = 2^2 - 5 = -1$, so the first factor is a mere unit. Also, $\mathrm{Nm}(8+3\sqrt{5}) = 8^2 - 5 \cdot 3^2 = 19$ and $\mathrm{Nm}(6+\sqrt{5}) = 6^2 - 5 = 31$, so that the last two factors represent primes above 19 and 31 respectively. These will be the most interesting primes for us.

The case $\ell = 19$

We start by writing $B_{19} = (-1,-19)_{\mathbb{Q}}$, which has two distinct conjugacy classes of maximal orders, given by

$$\begin{aligned} R_{19}^1 &= \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k; \\ R_{19}^2 &= \mathbb{Z}\frac{1+j+2k}{2} + \mathbb{Z}\frac{i+2j+k}{4} + \mathbb{Z}j + 2\mathbb{Z}k. \end{aligned}$$

Using this, it is easy to establish that in R_{19}^1 the units are given by ± 1 and $\pm i$, whereas in R_{19}^2 the only units are given by ± 1. We expect to find two different $R_{19}^{i,\times}$-conjugacy classes of embeddings of $\mathbb{Z}[\sqrt{-5}]$, corresponding to its class number. We are looking for traceless elements of norm 5, and naively one would find $\frac{\pm i \pm j}{2}$ and $\frac{\pm i \pm k}{2}$ as the only possibilities. Only the latter family lands in one of the above two maximal orders. In fact, it is contained in *both* maximal orders, provided we choose the right signs in the case of R_{19}^2. We therefore must interpret the two distinct families of embeddings as

$$\alpha_1^1(\sqrt{-5}) = \frac{i+k}{2} \in R_{19}^1 \quad \text{and} \quad \alpha_1^2(\sqrt{-5}) = \frac{i+k}{2} \in R_{19}^2.$$

The situation for the other seems more familiar, as there we expect and find only the embedding

$$\alpha_2\left(\frac{1+\sqrt{-7}}{2}\right) = \frac{1}{2} \pm \frac{3i-k}{4} \in R_{19}^2.$$

So we are left to interpret these results properly. Each of the two embeddings α_1 corresponds to one of the primes above 19 in the factorisation of the difference between singular moduli. The first embeds into R_{19}^1, and thus when comparing it to the embedding α_2 landing inside R_{19}^2, they have intersection number 0. The second embedding does reach R_{19}^2, so for each of the embeddings α_2, of which there is only one, we get a prime factor. This is the single factor of the prime above 19 that we observe in the factorisation, in perfect accordance with Theorem 1.3.2.

The case $\ell = 31$

To illustrate the arithmetic complexity of the right hand side of Theorem 1.3.2, we conclude this example by analysing the algebra $B_{31} = (-1,-31)_{\mathbb{Q}}$. This has *three* distinct conjugacy classes of maximal orders, representatives of which are given by

$$\begin{aligned} R_{31}^1 &= \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k; \\ R_{31}^2 &= \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i-k}{4} + \mathbb{Z}j + 2\mathbb{Z}k. \\ R_{31}^3 &= \mathbb{Z}\frac{3+i+j-k}{6} + 2k + \mathbb{Z}\frac{i+j-k}{3} + \mathbb{Z}\frac{i+k}{2} + 3\mathbb{Z}k. \end{aligned}$$

The units in R_{31}^1 are ± 1 and $\pm i$, whereas the other two orders only contain ± 1. Searching for the possible embeddings α_1 leaves us with

$$\alpha_1^1(\sqrt{-5}) = \pm\frac{7i+k}{4} \in R_{31}^2 \quad \text{and} \quad \alpha_1^2(\sqrt{-5}) = \pm\frac{5i+2j+k}{6} \in R_{31}^3.$$

For the other we indeed find a single embedding,

$$\alpha_2\left(\frac{1+\sqrt{-7}}{2}\right) = \frac{1}{2} \pm \frac{i+j-k}{6} \in R_{31}^3.$$

We find ourselves in a very similar situation as before. Indeed, the embedding α_1^1 reaches a different maximal order than α_2, and so for one of the two primes above 31 we will not get any factors. For the other, however, the unicity of α_2 gives us via α_1^2 one factor, as expected from Theorem 1.3.2.

Two irrational non-singular moduli

Let us conclude our numerous illustrative examples with one in which both singular moduli are irrational. To be precise, we explore

$$\begin{aligned} j\left(\sqrt{-5}\right) &= 2^6 \cdot 5 \cdot (1975 + 884\sqrt{5}); \\ j\left(\sqrt{-13}\right) &= -2^6 \cdot 3^3 \cdot 5^3 \cdot (15965 + 4428\sqrt{13}); \\ j\left(\sqrt{-5}\right) - j\left(\frac{1+\sqrt{-7}}{2}\right) &= 2^8 \cdot 5 \cdot (2693600 - 221\sqrt{5} + 747225\sqrt{13}). \end{aligned}$$

Factoring this difference is a tad tricky, so for now we will content ourselves with its norm

$$2^{40} \cdot 5^6 \cdot 13^2 \cdot 37^2 \cdot 139 \cdot 179 \cdot 211 \cdot 251.$$

We will focus on the prime $\ell = 37$. Even though the discriminants -20 and -52 are not in fact coprime, one only expects the formula to fail for the shared prime 2, so we are free to consider the prime $\ell = 37$ here. One final time, we introduce $B_{37} = (-2, -37)_{\mathbb{Q}}$, which has three conjugacy classes of maximal orders, of which only two are distinct, which is caused by two of the ideal classes in the quaternion algebra having the same maximal order. This is actually the smallest prime at which this phenomenon occurs. The maximal orders are then given by

$$\begin{aligned} R_{37}^1 &= \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{2-i+k}{4} + \mathbb{Z}\frac{1-i+j}{2}; \\ R_{37}^2 = R_{37}^3 &= \mathbb{Z}\frac{1+j+k}{2} + \mathbb{Z}\frac{i+6j+k}{8} + \mathbb{Z}(j+k) + 2\mathbb{Z}k. \end{aligned}$$

All orders only have the numbers ± 1 as units. For the possible images of $\sqrt{-5}$ we find

$$\alpha_1(\sqrt{-5}) = \pm\frac{7i+2j-k}{8} \in R_{37}^2 = R_{37}^3.$$

For the images of $\sqrt{-13}$, we establish

$$\alpha_2(\sqrt{-13}) = \pm\frac{3i+2j+3k}{8} \in R_{37}^2 = R_{37}^3.$$

We reiterate that the order $R_{37}^2 = R_{37}^3$ is to be considered twice; once for each ideal class. Namely, in doing so, for each of the two (identical) embeddings α_1, we find that only one of the two (identical) embeddings α_2 lands in the *same* order, hence contributing a factor of some prime above 37. Hence we have explained the two factors of 37 in the above norm, which is what we sought to do.

1.6 Analytic proof

Whereas the first proof of Theorem 1.2.1 in [GZ84], outlined in Section 1.2, made use of CM-theory, the other analysed a family of Hilbert Eisenstein series. More precisely, the second strategy employed by Gross and Zagier in [GZ84] was to consider a family $E_{1,\chi}(s)$ of non-holomorphic parallel weight 1 Hilbert Eisenstein series, indexed by a complex parameter s. Some of the properties of its $s = 0$-specialisation $E_{1,\chi}$ are described in Section A.2 in Appendix A. For the ideal class of the inverse different $\mathcal{D}_F^{-1}$, this specialisation vanishes, which implies that the first derivative of this family with respect to the weight parameter s, is a meaningful object to study.

Gross and Zagier in [GZ84] studied the *diagonal restriction*, denoted by Δ below, of this first derivative with respect to the weight-parameter s, which must be a real analytic modular form of weight 2 for $\mathrm{SL}_2(\mathbb{Z})$. One then applies the *holomorphic projection* operator e^{hol} to find

$$e^{\mathrm{hol}}\left(\Delta \frac{d}{ds} E_{1,\chi}(s)\Big|_{s=0}\right) \in M_2(\Gamma_0(1)) = \{0\}. \tag{1.2}$$

Most of the effort that goes into this analytic proof of Theorem 1.2.1 is to compute the Fourier coefficients of the expression on the left hand side, without appealing to its eventual vanishing as found above. With careful analysis to circumvent convergence issues, one finds that the first of these coefficients splits up in two terms; one equal to the logarithm of the norm of $j(\tau_1) - j(\tau_2)$, and the other to the logarithm of the explicit formula that was to be proved. It is crucial to note that this proof does not use any CM-theory whatsoever. It is a p-adic analogue of this proof that will be the main focus of this thesis.

To understand this approach in greater detail, we would need to explain why both the difference between the two j-invariants occurs as a result of these operations, as well as the finite elementary formula from Theorem 1.2.1. Let us start with the difference between j-invariants.

Roughly, a *Green's function* $G(x, y)$ on a Riemann surface X with a distinguished point ∞ is a symmetric function with the property that for fixed $y \in X$, the function $G(-, y)$ is harmonic on $X \setminus \{y, \infty\}$, having a log-pole at the removed points. If such a function exists, it must be unique up to a constant and this function can then be used to define an archimedean height pairing between certain divisors on X. On $\mathbb{P}^1$, there is an obvious choice for such a function: $G(x, y) = \log|x - y|^2$. Therefore, the function

$$\log|j(\tau_1) - j(\tau_2)|^2 : (\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H})^2 \to \mathbb{C}$$

is a natural Green's function on $\mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H}$. There are general strategies to construct Green's functions on modular curves, however. To this end, we define the weight 0 Eisenstein series

$$E(\tau,s) := \frac{1}{2}\sum_{\substack{c,d\in\mathbb{Z}\\ \gcd(c,d)=1}} \frac{\mathrm{im}(\tau)^s}{|c\tau+d|^{2s}}.$$

Next, one constructs a function $G_s(x,y)$ using an average over $\mathrm{SL}_2(\mathbb{Z})$ of functions built from a Legendre function Q_{s-1} of the second type. One may then show that

$$\lim_{s\to 1} G_s(\tau_1,\tau_2) + 4\pi E(\tau_1,s) + 4\pi E(\tau_2,s) - 4\pi\varphi(s) - 24,$$

describes another Green's function on $\mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H}$, where φ is a function expressed in elementary terms. Comparing their asymptotics, it follows that it must equal $\log|j(\tau_1)-j(\tau_2)|^2$. Next, one proves the expression

$$\frac{4}{w_1w_2}G_s(\tau_1,\tau_2) = -2\sum_{\substack{n>\sqrt{D}\\ n\equiv D \bmod 2}} \mu(n)Q_{s-1}\left(n/\sqrt{D}\right), \tag{1.3}$$

where the numbers $\mu(n)$ are integers related to a certain counting problem for integral binary quadratic forms. These numbers can be shown to be linked to the explicit formula that appears in Theorem 1.2.1.

The non-holomorphic Hilbert Eisenstein series $E_{1,\chi}(z,z',s)$ introduced by Hecke of weight 1 for $\mathrm{SL}_2(\mathcal{O}_F)$ is defined by

$$\sum_{[\mathfrak{a}]\in\mathrm{Pic}(F)^+}\chi(\mathfrak{a})\mathrm{Nm}(\mathfrak{a})^{1+2s}\sum_{\substack{(m,n)\in\mathfrak{a}^2/\{\pm1\}\\ (m,n)\neq(0,0)}}\frac{y^sy'^s|mz+n|^{-2s}|m'z'+n'|^{-2s}}{(mz+n)(m'z'+n')},$$

where $z=x+iy$ and $z'=x'+iy'$, which specialises to the Hilbert Eisenstein series $E_{1,\chi}$ for $s=0$. The Fourier expansion of this object is known, and this allows one to compute the diagonal restriction of the derivative

$$\frac{d}{ds}E_{1,\chi}(z,z,s)|_{s=0}.$$

By construction, this function on $\mathcal{H}$ transforms like a modular form of weight 2 under the action of $\mathrm{SL}_2(\mathbb{Z})$ and is asymptotically given by $A\log(y)+B+O(y^{-\epsilon})$ for some $A,B\in\mathbb{C}$ and $\epsilon>0$. We can write this function as a Fourier expansion of the form

$$\sum_{m=-\infty}^{\infty} a_m(y)e^{2\pi imz}.$$

A result of Sturm then allows us to compute the *holomorphic projection*, the first coefficient of which is defined by

$$\lim_{s\to 0}\left(4\pi\int_0^\infty a_1(y)e^{-4\pi y}y^s\ dy+\frac{24A}{s}\right).$$

This result must vanish, since the computed object is now contained in $M_2(\Gamma_0(1))=\{0\}$. Performing the computation, we find the same terms appearing as in Equation 1.3, establishing an equality and ultimately the result of Theorem 1.2.1.

The results of [GZ84] and [GKZ87] show that the outcome of this procedure for a family of Hilbert Eisenstein series, consisting of taking a diagonal restriction, a derivative and a holomorphic projection, is very generally related to the height pairing of certain divisors on the relevant modular curves. Since these height pairings are given by Green's functions and $\log|j(\tau_1)-j(\tau_2)|^2$ describes such a Green's function, the appearance of the difference between singular moduli in the result of this computation, need not be surprising. In fact, it is the vanishing of this height pairing, by virtue of the genus of the curve $Y_0(1)=\mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H}$ being zero, that ensures the algebraicity of this difference, as opposed to its transcendence.

We conclude this section by sketching a more direct connection between the logarithm of the explicit elementary formula that occurs in Theorem 1.2.1 and the diagonal restriction of the derivative with respect to the weight parameter of a family of Hilbert modular forms specialising to $E_{1,\chi}$. Recall that an ideal $\mathfrak{m}\subset\mathcal{O}_F$ is said to be *primitive* if it is not divisible by any rational prime. We need the following result.

Proposition 1.6.1. *Let $\mathfrak{m}\subset\mathcal{O}_F$ be a primitive ideal with at least one special prime. Then*

$$\log(F(\mathrm{Nm}(\mathfrak{m})))=-\sum_{I|\mathfrak{m}}\chi(I)\log(\mathrm{Nm}(I)).$$

Proof. Let us abbreviate the equality and conditions from the proposition to saying that $(*)$ holds. We use implicit induction to extend the set of ideals $\mathfrak{m}$ for which we know that $(*)$ holds until we have reached the full set of primitive integral ideals with $\chi(\mathfrak{m})=-1$.

Throughout, we let r be a rational prime that is not inert in $F/\mathbb{Q}$ and we let $\mathfrak{r}\subset\mathcal{O}_F$ be a prime above it. We assume that $r\nmid\mathrm{Nm}(\mathfrak{m})$.

First suppose that $\chi(\mathfrak{r}) = -1$. We will show that $(*)$ holds for $\mathfrak{r}^{2k+1}$ for any non-negative integer k. Indeed, we compute that

$$\sum_{I|\mathfrak{r}^{2k+1}} \chi(I)\log(\mathrm{Nm}(I)) = \log(r)\sum_{n=0}^{2k+1}(-1)^n n = -(k+1)\log(r);$$

which by definition equals $-\log(F(r^{2k+1}))$.

Suppose now that $(*)$ holds for $\mathfrak{m}$ and suppose that $\chi(\mathfrak{r}) = 1$. We claim that $(*)$ also holds for $\mathfrak{m}\mathfrak{r}^k$ for any $k > 0$. We compute that

$$\begin{aligned}\sum_{I|\mathfrak{m}\mathfrak{r}^k} \chi(I)\log(\mathrm{Nm}(I)) &= \sum_{n=0}^{k}\sum_{I|\mathfrak{m}} \chi(I\mathfrak{r}^n)\log(\mathrm{Nm}(I\mathfrak{r}^n)) \\ &= (k+1)\sum_{I|\mathfrak{m}}\chi(I)\log(\mathrm{Nm}(I)) + \sum_{n=0}^{k} n\log(r)\sum_{I|\mathfrak{m}}\chi(I) \\ &= -(k+1)\log(F(\mathrm{Nm}(\mathfrak{m})) = -\log(F(\mathrm{Nm}(\mathfrak{m}\mathfrak{r}^k))\end{aligned}$$

where we used Lemma A.2.10 and the observation that having a special prime means that $\rho(\mathfrak{m}) = 0$, as follows from its proof.

Suppose now that $(*)$ holds for $\mathfrak{m}$ and suppose that $\chi(\mathfrak{r}) = -1$. We claim that $(*)$ also holds for $\mathfrak{m}\mathfrak{r}^k$ for any $k > 0$. We compute that

$$\begin{aligned}\sum_{I|\mathfrak{m}\mathfrak{r}^k} \chi(I)\log(\mathrm{Nm}(I)) &= \sum_{n=0}^{k}\sum_{I|\mathfrak{m}} \chi(I\mathfrak{r}^n)\log(\mathrm{Nm}(I\mathfrak{r}^n)) \\ &= \sum_{n=0}^{k}(-1)^n\sum_{I|\mathfrak{m}}\chi(I)\log(\mathrm{Nm}(I)) + \sum_{n=0}^{k}(-1)^n n\log(r)\sum_{I|\mathfrak{m}}\chi(I) \\ &= \begin{cases} -\log(F(\mathrm{Nm}(\mathfrak{m})) & \text{if } k \text{ is even;} \\ 0 & \text{if } k \text{ is odd.}\end{cases}\end{aligned}$$

Here we again used Lemma A.2.10 in view of the information that $\mathfrak{m}$ has at least one special prime. If k is even, then by definition, $F(\mathrm{Nm}(\mathfrak{m})) = F(\mathrm{Nm}(\mathfrak{m}\mathfrak{r}^k))$, so the desired conclusion follows. If k is odd, then the ideal $\mathfrak{m}\mathfrak{r}^k$ would have more than 1 special prime. By definition, this causes the F-value of its norm to vanish, completing the proof of this case too. □

What follows is mostly heuristic, but it will hint at something profound. By Proposition 2.1 in [DDP11], for each positive integer k, there

exists a parallel weight k Hilbert modular form $E_{1,\chi}(k)$ with normalised Fourier coefficients $\mathfrak{m} \subset \mathcal{O}_F$ given by

$$a(\mathfrak{m}, E_{1,\chi}(k)) = \sum_{I|\mathfrak{m}} \chi(I)\mathrm{Nm}(I)^{k-1},$$

of which the object from Proposition A.2.9 is the $k = 1$-specialisation. Of course, the parameter k is discrete, so naively taking a derivative with respect to this weight parameter, is mathematically unsound. Disregarding this and formally doing so anyway, we would obtain

$$\frac{d}{dk} a(\mathfrak{m}, E_{1,\chi}(k)) = \sum_{I|\mathfrak{m}} \chi(I)\log(\mathrm{Nm}(I))\mathrm{Nm}(I)^{k-1}.$$

As such, specialising at $k = 1$ would yield

$$\frac{d}{dk} a(\mathfrak{m}, E_{1,\chi}(k))|_{k=1} = \sum_{I|\mathfrak{m}} \chi(I)\log(\mathrm{Nm}(I)),$$

which is the same quantity as appears in Proposition 1.6.1. We now consider the diagonal restriction of this hypothetical object for the ideal class $\mathcal{D}_F^{-1}$. The nth Fourier coefficient of the result will introduce a sum over all elements $\nu \in \mathcal{D}_F^{-1,+}$ of fixed trace n. It is easy to check that these elements are precisely those integral elements of the form $\nu = (x + n\sqrt{D})/2\sqrt{D}$ where $x^2 < n^2 D$. Putting all these observations together, we obtain for the first coefficient of the result the expression

$$\sum_{\nu \in \mathcal{D}_F^{-1,+}} \sum_{I|\nu\mathcal{D}_F} \chi(I)\log(\mathrm{Nm}(I)) = \sum_{\substack{x^2<D \\ x^2 \equiv D \bmod 4}} \log F\left(\frac{D-x^2}{4}\right);$$

this is the right hand side of Theorem 1.2.1.

Even though this argument is heuristic and not rigorous, it still illustrates why the precise order of operations as carried out by Gross and Zagier in [GZ84] might lead to an explicit formula as it appears in Theorem 1.2.1. Indeed, taking a derivative with respect to the weight parameter and subsequently a diagonal restriction seems to produce the terms that we are after. As we will explain in the next chapter, this deep phenomenon seems to allow itself for various generalisations, of which this thesis is but one example. However, this still leaves much to be explored in the future.