CM-values of p-adic Theta-functions

Daas, M.A.

CHAPTER 2

Main results

Ever since the conception of Theorem 1.2.1 by Gross and Zagier in [GZ84], people have searched for generalisations of these kinds of factorisation phenomena. One place for such investigations has been the arithmetic of Shimura curves; the main results of this thesis will be such generalisations. Major contributions to the field in this setting were previously achieved by Shou-Wu Zhang in [Zha01, YZZ13], vastly generalising the work of [GZ86, GKZ87] on modular curves to the Shimura curve setting. This thesis, however, will venture in a slightly direction.

2.1 Shimura curves over $\mathbb{C}$

To motivate the definition of Shimura curves, we recall that the open modular curve $Y_0(1)$ is defined as

$$Y_0(1) := \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}.$$

If $X_0(1)$ denotes its compactification by adding the cusp at infinity, the j-function exhibits an isomorphism

$$j : X_0(1) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}).$$

The group $\mathrm{SL}_2(\mathbb{Z})$ can be viewed as an index 2 subgroup of the unit group $\mathrm{GL}_2(\mathbb{Z})$ of the ring $M_2(\mathbb{Z})$, which in turn is a maximal order in the split quaternion algebra $M_2(\mathbb{Q})$. If we regard the determinant form $\det : M_2(\mathbb{Q}) \to \mathbb{Q}$ as the natural *norm* on the algebra $M_2(\mathbb{Q})$, then one may obtain the group $\mathrm{SL}_2(\mathbb{Z})$ from this quaternion algebra by first choosing a maximal order and subsequently considering the subgroup of units of norm 1. It is the generalisation of this procedure that defines the family of Shimura curves over $\mathbb{C}$ as we will consider them in this thesis.

Let N be a squarefree positive integer divisible by an even number of primes. Now let B_N denote the quaternion algebra over $\mathbb{Q}$ with discriminant N; that is, it is ramified at all primes dividing N, and is split at all other places. Since it is indefinite, it has a maximal order R_N that is unique up to conjugation and B_N can be embedded into $M_2(\mathbb{R})$. Choosing such a splitting, the subgroup $R_{N,1}^\times \subset R_N^\times$ consisting of all elements of unit norm can be regarded as acting on the complex upper half plane $\mathcal{H}$. In view of the above discussion, we now consider the quotient

$$X_N := R_{N,1}^\times \setminus \mathcal{H}.$$

This is called the *Shimura curve* of level N. In contrast to the case of $X_1 = X_0(1)$, if $N > 1$, we need not add any cusps, as one can show that

this quotient is already compact. Furthermore, as is the case for modular curves, X_N is an algebraic curve and in fact has a model defined over $\mathbb{Q}$.

Next, we observe that each element of the normaliser

$$\mathcal{N}(R_{N,1}^\times) = \left\{ b \in B_N^\times \mid bR_{N,1}^\times = R_{N,1}^\times b \right\}$$

induces an automorphism of the curve X_N. Indeed, the left-multiplication by b-map $\mathbb{C} \to \mathbb{C}$ decends to a map $X_N \to X_N$, as

$$b \cdot \left(R_{N,1}^\times z \right) = R_{N,1}^\times (b \cdot z) .$$

Clearly $\mathbb{Q}^\times R_{N,1}^\times \subset \mathcal{N}(R_{N,1}^\times)$, but all of these elements induce trivial automorphisms of X_N. The following lemma classifies what remains after this realisation.

Lemma 2.1.1. *The normaliser $\mathcal{N}(R_{N,1}^\times)$ satisfies*

$$\mathcal{N}(R_{N,1}^\times)/\mathbb{Q}^\times R_{N,1}^\times = \{ w_d \mid d > 0, \quad d \mid N \} \cong \prod_{r \mid N} \mathbb{Z}/2\mathbb{Z},$$

where the product $r \mid N$ is taken over all prime divisors r of N.

Proof. This is stated early in Chapter 43 of [Voi21]. □

This group is called the *Atkin-Lehner group* and is typically denoted by W_N. As the lemma above suggests, it is generated by commuting involutions w_r for every rational prime $r \mid N$. Note that for the modular curve $X_0(1)$ the Atkin-Lehner group is trivial, as $X_0(1)$ can be regarded as the $N = 1$-case of the construction above.

The following result is crucial for us, which will be a special case of Proposition 2.1 in [Pad23], which was originally proved by Ogg in [Ogg83].

Proposition 2.1.2. *Let φ denote the Euler totient function. Then the algebraic curve X_N has genus equal to*

$$g(X_N) = 1 + \frac{\varphi(N)}{12} - \frac{\epsilon_4(N)}{4} - \frac{\epsilon_3(N)}{3},$$

where for $k \in \mathbb{Z}$,

$$\epsilon_k(N) := \prod_{p \mid N} \left(1 - \left(\frac{-k}{p} \right) \right).$$

Corollary 2.1.3. *The Shimura curve X_N is of genus 0 if and only if*

$$N \in \{1, 6, 10, 22\}.$$

Proof. Clearly $g(X_1) = g(X_0(1)) = 0$. Let $N \in \mathbb{N}$ be such that $g(X_N) = 0$ and let $\tau(N)$ denote the number of primes dividing N. Suppose that we can find $\alpha, \beta, \gamma > 0$ such that

$$\varphi(N) \geq \alpha 2^{\tau(N)}\sqrt{N}, \quad \epsilon_4(N) \leq \beta 2^{\tau(N)} \quad \text{and} \quad \epsilon_3(N) \leq \gamma 2^{\tau(N)}.$$

Then it follows from Proposition 2.1.2 that

$$g(X_N) \geq 1 + 2^{\tau(N)}\frac{\alpha\sqrt{N} - 3\beta - 4\gamma}{12}, \text{ so } g(X_N) \geq 1 \text{ if } N \geq \left(\frac{3\beta + 4\gamma}{\alpha}\right)^2.$$

More sharply, if $\tau(N) = 2$, we even have that

$$g(X_N) \geq 1 + \frac{\alpha\sqrt{N} - 3\beta - 4\gamma}{3}, \text{ so } g(X_N) > 0 \text{ if } N > \left(\frac{3\beta + 4\gamma - 3}{\alpha}\right)^2.$$

To compute α, we note that

$$\frac{\varphi(N)}{2^{\tau(N)}\sqrt{N}} = \prod_{p|N}\frac{p-1}{2\sqrt{p}}, \quad \text{and} \quad \frac{p-1}{2\sqrt{p}} > 1 \quad \text{if} \quad p \geq 7.$$

If N is odd, then we may take $\alpha = 1/2$ and trivially $\beta = \gamma = 1$ to find that $g(X_N) \geq 1$ as soon as $N \geq 196$. Since $2 \cdot 3 \cdot 5 \cdot 7 > 196$, it follows that $\tau(N) = 2$, and therefore $g(X_N) > 0$ as soon as $N > 64$. If N contains a prime factor $p > 3$ that is not $-1 \mod 12$, then either $\epsilon_4(N) = 0$ or $\epsilon_3(N) = 0$ and we may take either $\beta = 0$ or $\gamma = 0$, to find $g(X_N) > 0$ always. This only leaves the curve X_{33}, but one checks that $g(X_{33}) = 1$.

Therefore N must be even, so henceforth we may take $\beta \leq 1/2$.

Suppose that N is not divisible by 3. Noting that indeed $g(X_{10}) = 0$ but $g(X_{14}) = 1$, we may assume that N contains a prime factor $p \geq 11$. We may then again take $\alpha = 1/2$, $\beta = 1/2$ and $\gamma = 1$ to find that $g(X_N) \geq 1$ as soon as $N \geq 121$. Thus again $\tau(N) = 2$ and we find $g(X_N) > 0$ as soon as $N > 25$. This leaves only the curve X_{22}, which indeed satisfies $g(X_{22}) = 0$.

It remains to study the case that $6 \mid N$, when we may also take $\gamma \leq 1/2$. Checking that $g(X_6) = 0$, we may assume that $\tau(N) \geq 4$. We may then take $\alpha = 1/5$, $\beta = \gamma = 1/2$ to find that $g(X_N) \geq 1$ as soon as $N > 306$. Since $2 \cdot 3 \cdot 5 \cdot 11 > 306$, this leaves only the curve X_{210}. But one checks that $g(X_{210}) = 5$, so the proof is complete. □

We assume throughout the rest of this thesis that $N \in \{6, 10, 22\}$. Then X_N admits an isomorphism

$$j_N : X_N \xrightarrow{\sim} \mathbb{P}^1,$$

which yields a generator j_N of the function field of X_N. However, in contrast to the modular curve case, we now longer have a cusp that we may use to normalise j_N in a natural way, as was done with Klein's j-function. As such, there is no canonical choice for this function j_N and it is so far defined only up to automorphism of $\mathbb{P}^1$. Recall that

$$\mathrm{Aut}(\mathbb{P}^1) \cong \mathrm{PGL}_2 \quad \text{through} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} [z_1 : z_2] := [az_1 + bz_2, cz_1 + dz_2].$$

If all primes dividing N are inert in some imaginary quadratic field K, we can find an embedding $\alpha : \mathcal{O}_K \to R_N$ and for each such embedding, there is a unique point $P \in \mathcal{H}$ fixed by the action of the image of the embeddings under the fixed splitting $B_N \to M_2(\mathbb{R})$. Then P is called the *CM-point* associated with the embedding α.

By Shimura's reciprocity law, as explained on the first pages of [Shi67], if j_N is chosen appropriately, the value $j_N(P)$ for a point $P \in X_N$ with complex multiplication by $\mathcal{O}_K$ is defined over the Hilbert class field H of the field K. In fact, this is a natural consequence of the adèlic *Main Theorem of Complex Multiplication* in the setting of Shimura curves, again see Theorem 4.19 in [Del71]. It requires only minimal adjustments compared to Theorem 1.1.1, illustrating the power of this formulation. For the sake of exposition, we specialise to the maximal compact open subgroup case.

Theorem 2.1.4. *Let $B_N/\mathbb{Q}$ be an indefinite quaternion algebra and let $N \in \mathbb{N}$ be its discriminant. Consider the following commutative diagram:*

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

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

As a result we have the following corollary; a version of Shimura reciprocity that we will need later.

Corollary 2.1.5. *For a CM point $P \in X_N$ associated with the embedding $\alpha : \mathcal{O}_K \to R_N$, it holds that $P \in X_N(H)$. Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal and let $x \in R_N$ be such that $\alpha(\mathfrak{a})R_N = xR_N$. Then*

$$P^{[\mathfrak{a},H_K/K]} = x^{-1} \cdot P \in X_N,$$

where $x^{-1} \cdot P$ is a CM-point for the embedding $x^{-1}\alpha(-)x : \mathcal{O}_K \to R_N$.

Proof. The power of the formulation of Theorem 2.1.4 lies in the fact that one may deduce Corollary 2.1.5 from it very similariy as to how we deduced Corollary 1.1.2 from Theorem 1.1.1. One merely needs to replace the algebraic group GL_2 by the algebraic group $B_N^\times$ and all arguments will go through without difficulty. □

With these algebraicity results known, and their strong analogy with the $X_0(1)$-setting from the previous chapter, one may wonder about a generalisation of Theorem 1.2.1 as proved by Gross and Zagier in [GZ84].

Elkies in [Elk98] numerically computed the CM-values for certain choices of a generator of the function field of certain *Atkin-Lehner quotients* of X_N, but not all values could be proved. However, the apparent smoothness of the resulting numbers did not go unnoticed. Using the theory of Borcherds lifts, Errthum in [Err11] was able to prove the correctness of many of Elkies's computations, but no conjectures as to the general structure of the values were posed. Some further explicit computations for particular choices of the generator of the function field can be found in [Voi09] and more general rational points on Atkin-Lehner quotients are studied in [Cla03].

Instead of choosing a function j_N, one may observe that the cross-ratio of its values is well-defined and independent of any choices. We recall that for any distinct x, y, z, w in some field, the cross-ratio is defined as

$$[x, y, z, w] := \frac{z - x}{z - y} \cdot \frac{w - y}{w - x}.$$

We invite the reader to check that if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then indeed} \quad [Ax, Ay, Az, Aw] = [x, y, z, w].$$

In 2022, Sofia Giampietro and Henri Darmon in [GD22], as part of the first author's master thesis, chose a prime $p \mid N$ and conducted extensive numerical computations with the quantities

$$\frac{j_N(P_1) - j_N(P_2)}{j_N(P_1') - j_N(P_2)} \cdot \frac{j_N(P_1') - j_N(P_2')}{j_N(P_1) - j_N(P_2')},$$

where for a CM-point P on the curve X_N, we write $P' := w_p(\mathrm{Frob}_p(P))$ where Frob_p denotes Frobenius at p in the CM-field of definition for P. The definition of P' may seem very little intuitive at first, but the logic behind this construction will become apparent in the next section.

As an example of these computations, Section 5 in [GD22] elaborates on the case of $N = 6$, $D_1 = -43$ and $D_2 = -163$, computing that

$$\mathrm{Nm}_{\mathbb{Q}}^{F}\left[\frac{j_N(P_1)-j_N(P_2)}{j_N(P_1')-j_N(P_2)}\cdot\frac{j_N(P_1')-j_N(P_2')}{j_N(P_1)-j_N(P_2')}\right]=\left(\frac{2\cdot 29\cdot 257\cdot 277}{73\cdot 137\cdot 241}\right)^2.$$

In parallel with Equation 1.1, one can check that all primes that occur on the right hand side are inert in both K_1 and K_2. More strongly, they are even prime divisors of a number of the form $43\cdot 163 - x^2$ for some $|x| < \sqrt{43\cdot 163}$, as the equality $43\cdot 163 - 19^2 = 24\cdot 277$ exemplifies. In fact, in this case, the authors did conjecture a general formula for this quantity. If we let $\{a, -a, b, -b\}$ denote the four square roots of $D = D_1D_2$ modulo $2N$, and define

$$\delta(x) = \begin{cases} +1 & \text{if } x \equiv \pm a \mod 2N; \\ -1 & \text{if } x \equiv \pm b \mod 2N, \end{cases} \tag{2.1}$$

then the following was conjectured in [GD22]. Its proof will be one of the main focusses of this thesis and can be found in Chapter 3.

Theorem A. *Let $N \in \{6, 10, 22\}$. For any pair of points P_1 and P_2 on X_N with CM by $\mathcal{O}_i$, the norm*

$$\mathrm{Nm}_{\mathbb{Q}}^{H_1H_2}\left[\frac{j_N(P_1)-j_N(P_2)}{j_N(P_1')-j_N(P_2)}\cdot\frac{j_N(P_1')-j_N(P_2')}{j_N(P_1)-j_N(P_2')}\right]^{\frac{\pm 2}{w_1w_2}}$$

is equal to the finite product

$$\pm\prod_{\substack{x^2<D\\ x^2\equiv D \bmod 4N}} F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}.$$

The similarity with Theorem 1.2.1 is apparent, even though, as our explicit examples show, the changed argument of the F-function causes most of the primes occurring in the two factorisations to be different. Finally, it is worth noting that in the concluding section of [GD22], the computations from [Err11] are shown to all be in accordance with the above result, giving strong validity to the statement above.

The statement of this theorem seems to suggest a resolution in the language of CM abelian varieties over the complex numbers $\mathbb{C}$, and in Chapter 3, we will carry out such a proof. However, following the treatment in [GD22], we also opt to approach this problem over the p-adics instead, for reasons we will explain in Section 2.3. The next section outlines how several powerful results combine to facilitate this.

2.2 The p-adic point of view

Using the p-adic uniformisation of Shimura curves, the authors of [GD22] related the quantity from Theorem A to one of a p-adic nature as follows. Recall that $N \in \{6, 10, 22\}$ and write $N = pq$ in such a way that $q \in \{2, 3, 5\}$, so as to ensure that B_q contains a unique maximal order R_q. We let $\mathcal{H}_p = \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$ denote Drinfeld's p-adic upper half plane. By choosing a splitting $B_q \to M_2(\mathbb{Q}_p)$, we obtain an action of B_q on $\mathcal{H}_p$. Furthermore, we let $R_q[1/p]$ be a maximal $\mathbb{Z}[1/p]$-order in B_q and by $R_q[1/p]_1^\times$ we will denote its units of unit norm. This group is infinite, and the quotient $R_q[1/p]_1^\times \setminus \mathcal{H}_p$ is a compact curve over $\mathbb{C}_p$.

A priori, it is not clear that this quotient should be related to the curve X_N in any way, since these objects are constructed using different quaternion algebras. Therefore, all the more surprising becomes the following celebrated theorem of Čerednik and Drinfeld, originally proved in [Čer76, Dri76] and well explained in [BC91].

Theorem 2.2.1. *The quotient $R_q[1/p]_1^\times \setminus \mathcal{H}_p$ is isomorphic to X_N over $\mathbb{C}_p$, with the isomorphism itself being defined over $\mathbb{Q}_{p^2}$, the unique quadratic unramified extension of $\mathbb{Q}_p$. The Čerednik-Drinfeld isomorphism*

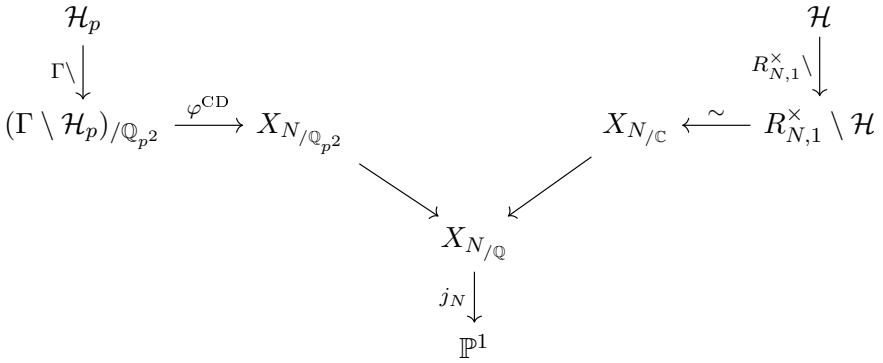
$$\varphi^{\mathrm{CD}} : R_q[1/p]_1^\times \setminus \mathcal{H}_p \xrightarrow{\sim} X_N(\mathbb{C}_p),$$

satisfies the property that for any $\tau \in R_q[1/p]_1^\times \setminus \mathcal{H}_p$ and $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, it holds that

$$\varphi^{\mathrm{CD}}(\delta(\tau)) = \begin{cases} \delta(\varphi^{\mathrm{CD}}(\tau)) & \text{if } \delta \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^2}); \\ w_p \cdot \delta(\varphi^{\mathrm{CD}}(\tau)) & \text{if } \delta \notin \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^2}). \end{cases}$$

This is a deep result, and we refrain from commenting on its proof. We relate the two stories told above by summarising everything in the single diagram below, where we wrote $\Gamma = R_q[1/p]_1^\times$ for clarity.

One of the advantages of this p-adic viewpoint is that the function $j_N : X_N(\mathbb{C}_p) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}_p)$ enjoys a more explicit description after appealing to the isomorphism from Theorem 2.2.1. Namely, the function



fields of such curves are generated by the titular p-adic Θ-functions. For a comprehensive treatment of these objects, we refer to Section 2.2 of [GvdP06]. We recall their definitions and main properties. We define for any $w_1, w_2 \in \mathcal{H}_p$ the infinite p-adic product

$$\Theta(w_1, w_2; z) := \prod_{\gamma \in R_q[1/p]_1^{\times}} \frac{z - \gamma w_1}{z - \gamma w_2}. \tag{2.2}$$

As shown in Section 2.2 of [GvdP06], this product converges for any value of $z \in \mathcal{H}_p$ as long as the denominator never vanishes. This function satisfies for any $\gamma \in R_q[1/p]_1^{\times}$ the relation

$$\Theta(w_1, w_2; \gamma z) = c(\gamma)\Theta(w_1, w_2; z)$$

for a certain factor of automorphy $c(\gamma) \in \mathbb{C}_p^{\times}$. As explained in Section 3 of [GD22], if X_N is of genus 0, as we are assuming, this factor of automorphy vanishes and as such, the expression above describes a rational function on the quotient $R_q[1/p]_1^{\times} \setminus \mathcal{H}_p$ with divisor $2(w_1) - 2(w_2)$. The factor of 2 here is caused by the trivially acting element $-1 \in R_q[1/p]_1^{\times}$, which is the only such element other than the identity itself.

Recall that for $i \in \{1, 2\}$, we fixed embeddings $\alpha_i : \mathcal{O}_i \to R_q$ and that for its image inside $M_2(\mathbb{Q}_p)$, there now exist two Galois conjugate common fixed CM-points in $\mathcal{H}_p$. It follows from Theorem 2.2.1 that if the CM-point $\tau_i \in \mathcal{H}_p$ maps to the CM-point $P_i \in X_N$ under the Čerednik-Drinfeld isomorphism φ^{CD}, then τ_i' will map to $P_i' = w_p(\mathrm{Frob}_p(P))$, explaining the perhaps somewhat non-obvious definition of the point P_i' from the previous section.

Comparing divisors, we obtain the equality

$$\Theta(w_1, w_2; z) = c(w_1, w_2) \left(\frac{j_N \circ \varphi^{\mathrm{CD}}(z) - j_N \circ \varphi^{\mathrm{CD}}(w_1)}{j_N \circ \varphi^{\mathrm{CD}}(z) - j_N \circ \varphi^{\mathrm{CD}}(w_2)} \right)^2,$$

where $c(w_1, w_2) \in \mathbb{C}_p^\times$ is some unknown constant. This constant seemingly prevents us from relating the precise norms of the expressions on both sides of this equation to achieve a p-adic analogue of Theorem A. However, a simple trick allows us to circumvent these concerns. Indeed, we may evaluate the above expression at two different values z_1 and z_2, and subsequently divide out the constant $c(w_1, w_2)$ to find the unconditional equality

$$\frac{\Theta(w_1, w_2; z_1)}{\Theta(w_1, w_2; z_2)} = \big[j_N \circ \varphi^{\mathrm{CD}}(z_1), j_N \circ \varphi^{\mathrm{CD}}(z_2), j_N \circ \varphi^{\mathrm{CD}}(w_1), j_N \circ \varphi^{\mathrm{CD}}(w_2)\big]^2.$$

In fact, a cross-ratio also appears on the right hand side, as

$$\begin{aligned}\frac{\Theta(w_1, w_2; z_1)}{\Theta(w_1, w_2; z_2)} &= \prod_{\gamma \in R_q[1/p]_1^\times} \frac{z_1 - \gamma w_1}{z_2 - \gamma w_2} \frac{z_2 - \gamma w_2}{z_2 - \gamma w_1} \\ &= \prod_{\gamma \in R_q[1/p]_1^\times} [z_1, z_2, \gamma w_1, \gamma w_2].\end{aligned}$$

In view of Theorem A, it should now be natural to set $z_1 = \tau_1$, $z_2 = \tau_1'$, $w_1 = \tau_2$ and $w_2 = \tau_2'$. If we let P_i be the image of τ_i for $i \in \{1, 2\}$ under the isomorphism φ^{CD}, then we obtain the equality

$$\prod_{\gamma \in R_q[1/p]_1^\times} [\tau_1, \tau_1', \gamma\tau_2, \gamma\tau_2'] = [j_N(P_1), j_N(P_1'), j_N(P_2), j_N(P_2')]^2.$$

In Section 4.5, we will define an action of the class group $\mathrm{Pic}(K_i)$ on the set of embeddings $\mathcal{O}_i \to R_q$ and as such, also on the set of CM-points for the orders $\mathcal{O}_i$ for $i \in \{1, 2\}$. A product over $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ then corresponds to taking the norm of the p-adic quantities above, which should conjecturally be algebraic and contained in the field H_1H_2, down to the field L. However, these algebraic numbers are in fact always contained in a degree $2h_1h_2$ subfield of H_1H_2, which will cause this norm to L to always be contained in the real quadratic field F.

To algebraically describe the final step down to $\mathbb{Q}$, we let $\pi \in R_q$ denote any quaternion with $\mathrm{Nm}(\pi) = p$. We now define

$$\Theta(D_1, D_2) := \prod_{[c_1], [c_2]} \frac{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \tau_2\big)}{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \tau_2'\big)}$$

and

$$\Theta_p(D_1, D_2) := \prod_{[c_1], [c_2]} \frac{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \pi\tau_2\big)}{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \pi\tau_2'\big)},$$

where the products are taken over all $[c_1] \in \mathrm{Pic}(K_1)$ and $[c_2] \in \mathrm{Pic}(K_2)$. We then also claim the following p-adic version of Theorem A, the proof of which will be the main focus of this thesis.

Theorem B. *It holds that*

$$\left(\frac{\Theta(D_1,D_2)}{\Theta_p(D_1,D_2)}\right)^{\frac{\pm 2}{w_1 w_2}} = \pm \prod_{\substack{x^2<D \\ x^2 \equiv D \bmod 4N}} F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}.$$

Clearly, Theorem A and Theorem B are equivalent.

We conclude this section by recording a proposition that aims to relate the result from Theorem 1.3.2 to the differences between the fixed points associated with the embeddings $\alpha_i : \mathcal{O}_i \to R_q$. It illustrates that these fixed points contain a lot of arithmetic information about the pair of embeddings that defined them.

Since we expect only primes ℓ that are inert in both K_1 and K_2 to contribute to the eventual norm of the algebraic quantities we are considering in Theorems A and B, we will restrict ourselves to this class of primes when formulating and proving the following result, once more strengthening the ties between our results and Theorem 1.2.1. Finally, we remark that, even though the following proposition is formulated in terms of the matrix algebra $M_2(\mathbb{Z}_\ell)$, by choosing a splitting it is actually applicable to every rational quaternion algebra B_M as long as $\ell \nmid M$.

Proposition 2.2.2. *Let ℓ be a rational prime that is inert in both K_1 and K_2. Let $\alpha_1 : \mathcal{O}_1 \to M_2(\mathbb{Z}_\ell)$ and $\alpha_2 : \mathcal{O}_2 \to M_2(\mathbb{Z}_\ell)$ be embeddings with associated fixed points $\tau_1 \in \mathbb{Z}_{\ell^2}$ and $\tau_2 \in \mathbb{Z}_{\ell^2}$. Then $v_\ell(\tau_1 - \tau_2)$ is equal to the largest $k \in \mathbb{Z}_{\geq 0}$ such that the images of α_1 and α_2 coincide modulo $\ell^k M_2(\mathbb{Z}_\ell)$.*

Proof. Let us suppose that the image $\alpha_1(\sqrt{D_1})$ is given by

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \quad \text{with fixed point} \quad \tau_1 = \frac{a+\sqrt{D_1}}{c},$$

where $D_1 = a^2 + bc$ is one of the discriminants in question. Further suppose that the image $\alpha_2(\sqrt{D_2})$ is given by

$$\begin{pmatrix} x & y \\ z & -x \end{pmatrix} \quad \text{with fixed point} \quad \tau_2 = \frac{x+\sqrt{D_2}}{z},$$

where $D_2 = x^2 + yz$ is the other discriminant. First, we claim that $b, c, y, z \in \mathbb{Z}_\ell^\times$. Indeed, if this were not the case, then $D_1 \equiv a^2 \mod \ell$ and $D_2 \equiv x^2 \mod \ell$. However, then the prime ℓ would not have been inert in the fields K_1 and K_2; a contradiction. Therefore we find that

$$\tau_1 - \tau_2 \in \ell^k \mathbb{Z}_{\ell^2} \iff z(a + \sqrt{D_1}) - c(x + \sqrt{D_2}) \in \mathbb{Z}_{\ell^2}.$$

Now note that we can write $\mathbb{Z}_{\ell^2} = \mathbb{Z}_\ell + \mathbb{Z}_\ell \sqrt{D_1}$. Therefore, we find that

$$\tau_1 - \tau_2 \in \ell^k \mathbb{Z}_{\ell^2} \iff za - cx \in \ell^k \mathbb{Z}_\ell \quad \text{and} \quad zD_1 - c\sqrt{D} \in \ell^k \mathbb{Z}_\ell.$$

Suppose that these congruences hold for some value of k. Then

$$zD_1 \equiv c\sqrt{D} \mod \ell^k \mathbb{Z}_\ell \implies z^2 D_1^2 \equiv c^2 D_1 D_2 \mod \ell^k \mathbb{Z}_\ell.$$

We continue to compute that

$$z^2 D_1 \equiv c^2 D_2 \mod \ell^k \mathbb{Z}_\ell \implies z^2(a^2 + bc) \equiv c^2(x^2 + yz) \mod \ell^k \mathbb{Z}_\ell.$$

Using that $za \equiv cx \mod \ell^k \mathbb{Z}_\ell$, we conclude that $z^2 bc \equiv c^2 yz \mod \ell^k \mathbb{Z}_\ell$, and so $zb \equiv cy \mod \ell^k \mathbb{Z}_\ell$. Now define $t \in \mathbb{Z}_\ell^\times$ to solve the equation $z = tc$. Then we find that $tca \equiv cx \mod \ell^k \mathbb{Z}_\ell$, and as such, $ta \equiv c \mod \ell^k \mathbb{Z}_\ell$. Furthermore, we find that $tcb \equiv cy \mod \ell^k \mathbb{Z}_\ell$, and as such $tb \equiv y \mod \ell^k \mathbb{Z}_\ell$. This means that

$$\begin{pmatrix} x & y \\ z & -x \end{pmatrix} \equiv t \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \mod \ell^k M_2(\mathbb{Z}_\ell).$$

As the images $\alpha_1(\sqrt{D_1})$ and $\alpha_2(\sqrt{D_2})$ are both traceless, this is equivalent to the images of the embeddings agreeing modulo $\ell^k \mathbb{Z}_\ell$.

Conversely, suppose that the above matrix congruence holds true for some $t \in \mathbb{Z}_\ell^\times$. Then we find that $za \equiv tca \equiv cx \mod \ell^k \mathbb{Z}_\ell$, and similarly, as now $D_2 \equiv t^2 D_1 \mod \ell^k \mathbb{Z}_\ell$, we find that $zD_1 \equiv tcD_1 \equiv c\sqrt{D} \mod \ell^k \mathbb{Z}_\ell$, proving the other direction too. □

2.3 Parallels with RM-theory

In the spirit of the original paper by Gross and Zagier [GZ84], our approach to proving Theorem A and Theorem B is two-fold. First we present a direct proof of Theorem A using CM-theory, which one could say is the standard approach for problems of this nature. It is not surprising that such a proof exists, and in fact, using the results from Phillips's thesis [Phi15], the proof is rather straightforward.

Much more interesting is our second proof, which proves Theorem B directly, not relying on any CM-theory whatsoever and is done purely by studying the infinitesimal p-adic deformation theory of the Galois representation associated with an appropriate p-stabilisation of the parallel weight 1 Hilbert Eisenstein series $E_{1,\chi}$ described in Section A.2 and studied in Section 1.6. Captured in one equation, letting Δ once again denote the diagonal restriction, Theorem B will be a consequence of the claim that the first Fourier coefficient of the ordinary projection

$$e^{\mathrm{ord}}\left(\Delta\frac{d}{d\epsilon}E_{1,\chi}^{(p)}(\epsilon)\right)\in S_2(\Gamma_0(N)),$$

must vanish, once more strengthening the parallels with the analytic proof in [GZ84] that we sketched in Section 1.6 and which we similarly captured succinctly in Equation 1.2.

Our main motivation for this second proof, which constitutes the focus of this manuscript, originates from the recent advancements in the theory of real multiplication, as we will now explain.

A most naive attempt at using the j-function also to generate abelian extensions of *real* quadratic fields to mimic the results of Corollary 1.1.2 is complicated by the observation that the real line $\mathbb{R}$ is not contained in the field of definition $\mathcal{H}$ of j. A more conceptual way of phrasing this obstruction, is that the infinite place of a real quadratic field is split, whereas it is not for imaginary quadratic fields. As $\mathcal{H}_p=\mathbb{P}^1(\mathbb{C}_p)\backslash\mathbb{P}^1(\mathbb{Q}_p)$ and all p-adic embeddings of a number field land inside $\mathbb{Q}_p$ if and only if p splits completely, a real quadratic field *does have points* inside the p-adic upper half plane as soon as p does *not* split.

Building upon this insight and influences from the theory of linking numbers of modular knots, in [DV21], Darmon and Vonk proposed a p-adic real quadratic analogue of the differences between singular moduli as studied in [GZ84]; a certain *rigid meromorphic cocycle* for the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$, whose RM-values conjecturally often generate the appropriate Hilbert class fields for real quadratic fields. Certain cases of these conjectures have recently been proved and while this emerging theory should be well connected with many other areas of mathematics, notable among these the theory of Borcherds products and their ostensible connections to both p-adic heights and intersection numbers of geodesics on Shimura curves, many aspects remain to be explored.

The RM-values of the rigid meromorphic cocycles introduced in [DV21] in many ways behave like a p-adic real quadratic analogue of the differences between singular moduli as studied in [GZ84], as these RM-values conjecturally display factorisations of an intricacy similar to those

claimed by Theorem 1.2.1. More recently, these constructions were generalised to different quaternion algebras than the matrix algebra in [Geh20, GMX21], reflecting the step from modular curves to Shimura curves as outlined earlier in this chapter, and to more general orthogonal groups in [DGL23].

Historically, the study of CM-theory has largely been facilitated by its connection to the geometry of abelian varieties and the moduli spaces that govern them. The development of an analogous RM-theory is complicated by the lack of such obvious connections to geometry. It is for this reason that the analytic proof in [GZ84] is of particular interest, as its independence from CM-theory contrasted strongly with the other, more algebraic, proof.

Darmon, Pozzi and Vonk used similar ideas in [DPV21, DPV23], studying the ordinary projection of the diagonal restriction of the first derivative with respect to the weight parameter of a p-adic family of Hilbert modular Eisenstein series attached to more general odd characters of the narrow class group of a real quadratic field. They computed its Fourier coefficients and these quantities proved to be related to both Stark-Heegner points and Gross-Stark units, enriching the analogy between the classical theory of complex multiplication and its extension to real quadratic fields.

In a similar spirit, Dasgupta and Kakde in [DK23a, DK23b] recently proved the Brumer-Stark conjecture away from 2 and used these ideas to prove the p-part of the integral Gross-Stark conjecture for the Brumer-Stark p-units in CM abelian extensions of a totally real field using the theory of group ring valued Hilbert modular forms. Another recent breakthrough towards Hilbert's 12th problem was recently established in [BCG23], highlighting the buzzing research activity surrounding the ideas and techniques that drive the main concepts explored in this thesis.

The p-adic nature of these advancements in the RM setting raises the question of the applicability of some of these techniques in the CM setting, where the theory is much more understood and other methods than those employed in this thesis are also available. The main motivation for this manuscript is to answer this question in one particular setting, proving the same theorem both using the geometric moduli interpretation of the Shimura curve X_N, and not using this interpretation at all, and instead relying purely on the newly developed techniques from modern RM theory. This is especially interesting in view of the presently still unknown geometric framework within which the modern developments in RM-theory should best be described. Finally, we remark that

the present work serves as a direct p-adic transposition of the analytic proof by Gross and Zagier in [GZ84] because we study an appropriate p-stabilisation of the exact same Hilbert Eisenstein series $E_{1,\chi}$, but using p-adic instead of archimedean methods.

Additionally, our work hints at an occurrence of a non-archimedean instance of the Kudla program, which is presently being investigated more intensively than ever. Even though it has classically been mostly studied in an archimedean context, recent years have seen some instances of similar results in non-archimedean settings. Examples of this include the results from [DPV21, DPV23], but also for instance the works [DT08] and [LN19]. This emerging "p-adic Kudla program" still leaves much to be explored in the forthcoming years. It is also for this reason that in the present work, we do not explore the possibly third approach using Borcherds lifts in a similar style of [Err11] when proving the CM-values from [Elk98], even though the success of such an approach should be expected as well.

Remark 2.3.1. If we relax the condition that the Shimura curve X_N be of genus zero, then the quotient $\Theta(D_1, D_2)/\Theta_p(D_1, D_2)$ from Theorem B can no longer be expected to be algebraic and indeed it generally will not be, for it will consist of both an algebraic part, determined above, and a transcendental part given by an appropriate p-adic height pairing on the Jacobian of the Shimura curve X_N, which vanishes in the genus zero case. Define for $i \in \{1, 2\}$ the divisors on X_N by the formulas

$$\mathcal{D}_i = \sum_{[c_i] \in \mathrm{Pic}(K_i)} [c_i] \cdot (P_i - P_i').$$

Let T_m denote the natural Hecke correspondence on the Jacobian of X_N and let $(-,-)_p$ denote the p-adic Schneider height pairing as computed in [Gro86, Wer96]. Even though Werner's result in [Wer96] only pertains to the quotient by Schottky groups, using the results from Section 4 of [vdP92], one expects this to be extendable to quotients by groups such as $R_q[1/p]_1^\times$. One may conjecture an equality of the form

$$e^{\mathrm{ord}}\left(\Delta \frac{d}{d\epsilon} E_{1,\chi}^{(p)}(\epsilon)\right) = \sum_{m \geq 1} (\mathcal{D}_1, T_m \mathcal{D}_2)_p \; q^m \in S_2(\Gamma_0(N)).$$

This p-adic instance of the Kudla program would bear strong resemblance to various previous works in an archimedean setting; most notably to Theorem V.1 in [GKZ87]. It would also resemble some of the results by Zhang in [Zha01, YZZ13].

2.4 Outline of the thesis

In Chapter 3, we describe an approach that mirrors the ideas behind Gross and Zagier's original algebraic proof in [GZ84], exploiting the moduli interpretation of the Shimura curve X_N and the theory of complex multiplication. We appeal to the main result of the PhD thesis of Andrew Phillips [Phi15], which computes the intersection numbers of certain substacks of the full moduli stack that parametrise CM abelian varieties, following ideas of Howard and Yang in [HY12]. Using these results, the proof of Theorem A is rather straightforward.

The weight of this thesis is concentrated in our proof of Theorem B. For this, we follow the general strategy of the main arguments presented in [DPV23]. The core idea is to deform $E_{1,\chi}^{(p)}$ as a p-adic *cusp form*. To obtain such a family of deformations, we first deform a rigidification ρ_η of the decomposable representation $\rho = \mathbb{1} \oplus \chi$ associated with $E_{1,\chi}^{(p)}$. We then justify that these representations come from modular forms by means of proving a so-called $R = T$-theorem. With this family of modular forms in hand, we finish the proof through a computation.

Our second proof can thus be divided into three distinct steps.

Step 1: In Chapter 4, we describe an F-quadratic form $\det_F$ on B_q refining the quaternion norm to F. Together with a construction that associates to a quaternion an $\mathcal{O}_L$-ideal, we derive a bijection between the elements of R_q with a fixed $\det_F$-value and the set of $\mathcal{O}_L$-ideals of a certain norm. In Section 6.1, we use this to rewrite the left hand side of Theorem B in a more useful form.

Step 2: Chapter 5 proves an $R = T$ theorem using similar methods as in Pozzi's thesis [Poz19] and the works [BDP22, BD16, BDS20, BC06], using fundamental results from Hida in [Hid89b, Hid89a]. This is done by constructing a lift of ρ_η to Hida's cuspidal nearly ordinary Hecke algebra and comparing the dimensions of this Hecke algebra T and the nearly ordinary deformation ring R. This is used in Section 6.2.

Step 3: In Chapter 6, we consider one particular deformation and, supported by the result of Chapter 5, compute the infinitesimal family of deformations of $E_{1,\chi}^{(p)}$ that corresponds to it. After taking its diagonal restriction, its derivative with respect to the weight parameter and applying the ordinary projection operator, we argue why the result must vanish identically. Ultimately, we conclude the proof of Theorem B by computing explicitly the Fourier coefficients and equating the first of these coefficients to zero.