A p-adic approach to singular moduli on Shimura curves

Sofia Giampietro
Henri Darmon

Abstract

This paper defines a rational invariant $\mathcal{J}_N(D_1, D_2)$ associated to singular moduli of discriminants D_1 and D_2 on the genus-zero Shimura curves of discriminant $N = 6, 10$ or 22. An algorithm is devised to compute this invariant p-adically using the Cerednik-Drinfeld uniformisation of Shimura curves, following the approach described in the thesis of I. Negrini [10]. A formula for the factorization of this invariant is proposed, similar to the formula of Gross and Zagier for differences of classical singular moduli.

2010 Mathematics Subject Classification: 14G35, 11G15, 11G18

Keywords: Singular moduli on Shimura curves, p-adic uniformisation

1 Introduction

In [8], Gross and Zagier give an explicit formula for the factorisation of the norm of differences of singular moduli. Given two negative coprime fundamental discriminants D_1 and D_2 and their associated imaginary quadratic fields $K_i = \mathbb{Q}(\sqrt{D_i})$ with ring of integers $\mathcal{O}_{D_i}$, let τ_1 and τ_2 be two points on the upper half plane with complex multiplication by $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$ respectively. Consider the elliptic modular function j on the upper half plane which has a Fourier expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots ,$$

where $q = e^{2\pi i\tau}$. Then the norm of $j(\tau_1) - j(\tau_2)$ is a highly divisible integer, and Gross and Zagier prove the following:

Theorem 1 (Gross, Zagier)**.** *Let D_1 and D_2 be coprime fundamental discriminants and*

$$J(D_1, D_2) = \prod_{\substack{[\tau_1],[\tau_2] \\ disc\tau_i = D_i}} (j(\tau_1) - j(\tau_2))^{\frac{4}{w_1 w_2}}$$

where w_i is the order of the group of units of $\mathcal{O}_{D_i}$ for $i = 1, 2$. For $D_i \leq -4$ this quantity denotes the norm of the difference of two singular moduli of these *discriminants. Let $D = D_1 D_2$. For primes l with $\left(\frac{D}{l}\right) \neq -1$, define*

$$\epsilon(l) = \begin{cases} \left(\frac{D_1}{l}\right) & \text{if } (l, D_1) = 1, \\ \left(\frac{D_2}{l}\right) & \text{if } (l, D_2) = 1. \end{cases}$$

If $n = \prod l_i^{a_i}$ with $\left(\frac{D}{l_i}\right) \neq -1$ for all i, define $\epsilon(n) = \prod \epsilon(l_i)^{a_i}$. Then

$$J(D_1, D_2)^2 = \pm \prod_{\substack{x^2 < D \\ x^2 \equiv D (mod\ 4)}} F\Big(\frac{D - x^2}{4}\Big),$$

where

$$F(m) = \prod_{\substack{nn'=m \\ n,n'>0}} n^{\epsilon(n')}. \tag{1}$$

Gross and Zagier observe that $F(m)$ is either 1 or is a power of a single prime. Indeed, write

$$m = l_1^{2a_1+1} \cdots l_s^{2a_s+1} d_1^{2b_1} \cdots d_r^{2b_r} q_1^{c_1} \cdots q_t^{c_t},$$

where for all i, $\epsilon(l_i) = \epsilon(d_i) = -1$ and $\epsilon(q_i) = +1$. Then $F(m) = 1$ if $s > 1$, otherwise

$$F(m) = l_1^{(a_1+1)(c_1+1)\cdots(c_t+1)}.$$

This article defines a similar invariant, on Shimura curves of genus 0. Let $N = 6, 10$ or 22. Let X_N be the genus zero Shimura curve of discriminant N. As in the case of the usual modular curve, one can develop a theory of complex multiplication (CM) points on Shimura curves. In particular the value of a uniformizing function j_N of X_N at CM points has similar properties to those of the classical singular moduli. However computing a uniformizing function j_N for the Shimura curve X_N is more subtle than in the classical case as the lack of cusps on X_N gives no natural choice of a point at infinity and prevents the use of Fourier series expansion. For that reason we use p-adic methods instead.

This paper is inspired by the recent work of Rickards [11], and Guitart, Masdeu and Xarles [9]. In particular the invariants computed in this article can be seen as the complex counterpart to those involving modular geodesics on Shimura curves defined in [3].

Let p be a prime dividing N exactly and write $N = pN'$ with $(p, N') = 1$. Let B be the definite rational quaternion algebra of discriminant N', so that we may consider an embedding $\iota : B \hookrightarrow M_2(\mathbb{Q}_p)$. Let R be a maximal $\mathbb{Z}[\frac{1}{p}]$ order in B and let $\Gamma_N^{(p)} = \iota(R^*_{\text{norm}=1}) \subseteq SL_2(\mathbb{Q}_p)$ be the image of its norm 1 elements. By Cerednik-Drinfeld's theorem, the quotient $\Gamma_N^{(p)} \backslash \mathcal{H}_p$, where $\mathcal{H}_p$ denotes the p-adic upper half plane, is isomorphic to $X_N(\mathbb{C}_p)$. Again, one can consider complex multiplication points on the p-adic uniformisation of the Shimura curve, corresponding to optimal embeddings of imaginary quadratic orders into the

quaternion order R.
Fix two negative discriminants D_1, D_2 and consider the corresponding imaginary quadratic orders $\mathcal{O}_{D_1}$ and $\mathcal{O}_{D_2}$. For $i = 1, 2$ a choice of an embedding $\mathcal{O}_{D_i} \hookrightarrow R$ gives rise to two p-adic conjugate complex multiplication points $\{\tau_i, \tau_i'\}$.

Let $[a, b, c, d] = \frac{c-a}{c-b} \cdot \frac{d-b}{d-a}$ denote the cross ratio of four numbers. The p-adic quantity we are interested in is:

$$J_N^{(p)}(\tau_1, \tau_2) := \prod_{\gamma \in \Gamma_N^{(p)}} [\gamma\tau_1, \gamma\tau_1', \tau_2, \tau_2']. \tag{2}$$

This infinite product converges p-adically and this paper presents a simple algorithm to compute it in the case when the underlying quaternion algebra is of class number one. This is the case for $N' = 2, 3$ and 5, so we only exclude the case in which $N = 22$, $p = 2$ and $N' = 11$.

By Cerednik-Drinfeld, for $i = 1, 2$ the CM points $\{\tau_i, \tau_i'\}$ on the p-adic quotient $\Gamma_N^{(p)} \backslash \mathcal{H}_p$ correspond to some CM points on the curve X_N and by abuse of notation denote these points again by $\{\tau_i, \tau_i'\}$. If $j_N : X_N \to \mathbb{P}^1$ is a generator over $\mathbb{Q}$ of the function field, the invariant may then be rewritten as the cross ratio of these singular moduli:

$$\begin{aligned} J_N^{(p)}(\tau_1, \tau_2) &= [j_N(\tau_1), j_N(\tau_1'), j_N(\tau_2), j_N(\tau_2')] \\ &= \frac{j_N(\tau_2) - j_N(\tau_1)}{j_N(\tau_2) - j_N(\tau_1')} \frac{j_N(\tau_2') - j_N(\tau_1')}{j_N(\tau_2') - j_N(\tau_1)}. \end{aligned} \tag{3}$$

Since the value of j_N at CM points is algebraic, expression (3), and hence also the p-adic quantity (2), is algebraic over $\mathbb{Q}$.
Different methods to compute singular moduli on Shimura curves have already been used. For example [5] uses explicit calculations of involutions on these curves while [6] uses the theory of Borcherds forms. Our approach to compute the quantity (3) will instead be that of using the p-adic expression (2).

The p-adic quantity $J_N^{(p)}(\tau_1, \tau_2)$ depends on the choice of the prime p dividing N and on the choice of embeddings that give τ_1 and τ_2. However, the obtained results suggest that the *norm* of this quantity, seen as an algebraic number over $\mathbb{Q}$, is independent of any choice, up to inversion in the multiplicative group. This motivates the following definition.

Definition 2. Let $N = 6, 10, 22$, let D_1, D_2 be two imaginary discriminants and let H_1 and H_2 be their associated ring class fields. For any prime p dividing N, let τ_1 and τ_2 be arbitrary complex multiplication points on $\mathcal{H}_p$ of discriminant D_1 and D_2 respectively. Define:

$$\mathcal{J}_N(D_1, D_2) = \mathrm{Norm}_{H_1 H_2/\mathbb{Q}}(J_N^{(p)}(\tau_1, \tau_2)).$$

It can be proved that this expression does not depend on the choice of point τ_1 and τ_2 by Shimura's reciprocity law.

Results suggest that they enjoy similar factorizations as in the work of Gross and Zagier.

There are four square roots of D mod $2N$, say $\{a, -a, b, -b\}$. Define

$$\delta(x) = \begin{cases} +1 & \text{if } x \equiv \pm a \pmod{2N}, \\ -1 & \text{if } x \equiv \pm b \pmod{2N}. \end{cases} \tag{4}$$

Conjecture 3. *With the same notation as in Theorem 1,*

$$\mathcal{J}_N(D_1, D_2)^{\pm\frac{4}{w_1 w_2}} = \pm \prod_{\substack{x^2 < D \\ x^2 \equiv D (mod\ 4N)}} F\Big(\frac{D - x^2}{4N}\Big)^{2\delta(x)},$$

where $D = D_1 D_2, w_1, w_2$ and the function F are as in Theorem 1, and $\delta(x)$ is defined above.

This conjecture is extensively supported by the data collected and reported on in this paper, which is organised as follows. Section 2 briefly recalls the theory of Shimura curves and their complex multiplication points. Section 3 defines and studies the p-adic $J_N^{(p)}$ quantity. The fourth, fifth and sixth section present an algorithm to compute it and discuss obtained results. The final section compares this work with what has already been computed by Errthum in [6] in the case of $N = 6$.

Acknowledgements. This article is the outcome of a research project carried out by the first author while she was an undergraduate at the the EPFL. It was completed under the supervision of the second author, during a visit to McGill University in the first months of 2020, and, after her stay was cut short by the pandemic, during the ensuing lockdown. The first author is grateful for the material support of the EPFL which made her visit possible. The research of the second author is supported through an NSERC Discovery grant.

2 Shimura curves

Throughout the paper let $N = 6, 10$ or 22. Let B_N be the quaternion algebra over $\mathbb{Q}$ with discriminant N and denote by R_N its (unique up to conjugation) maximal $\mathbb{Z}$-order. The algebra B_N admits a basis $\{1, i, j, k\}$ such that

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k,$$

for some $a, b \in \mathbb{Q}$ with $a > 0$, and it can always be embedded into $M_2(\mathbb{R})$, for example by the following map:

$$\iota : A + Bi + Cj + Dk \mapsto \begin{pmatrix} A + B\sqrt{a} & b(C + D\sqrt{a}) \\ C - D\sqrt{a} & A - B\sqrt{a} \end{pmatrix}. \tag{5}$$

Let R_1^* be the group of elements of R_N^* of norm 1. The action of $\Gamma_N := \iota(R_1^*)/\langle \pm 1 \rangle$ on the upper half plane yields a compact Riemann surface, $\Gamma_N \backslash \mathcal{H}$, denoted by X_N which is of genus zero. Shimura has shown that X_N has a canonical model defined over $\mathbb{Q}$.

Fix a negative discriminant $D < 0$, and let $K = \mathbb{Q}(\sqrt{D})$ be the imaginary quadratic field of discriminant D, and $\mathcal{O}_D$ the maximal order in K.
If all prime divisors of N are inert in K, then there exists an *optimal* embedding ϕ of $\mathcal{O}_D$ into the quaternionic order R_N. In this case the image $\iota(\phi(\mathcal{O}_D)) \subseteq \iota(R_N) \subseteq SL_2(\mathbb{R})$ has a unique fixed point in $\mathcal{H}$. A complex multiplication (CM) point of the curve X_N is the Γ_N orbit of such a point and the discriminant of such a point is the field discriminant of K.
If X_N is of genus zero and $j_N : X_N \to \mathbb{P}^1$ denotes a generator of the function field, just as in the case of the classical modular function, if properly normalised, the value of j_N at a CM point is algebraic over $\mathbb{Q}$.

The Atkin-Lehner group is the subgroup of automorphisms of X_N,

$$\mathcal{W} = \text{Normalizer}_{B_N^*}(R_1^*)/\mathbb{Q}^* R_1^* = \{ \ w_m \ : \ m|N \ \} \cong \prod_{p|N} \mathbb{Z}/2\mathbb{Z}.$$

and let $\text{Pic}(\mathcal{O}_D)$ be the class group of $\mathcal{O}_D$. Then it is well known that these involutions and $\text{Pic}(\mathcal{O}_D)$ act on the set of CM points of a given discriminant D (see Section 5 of chapter III of [12]). Furthermore we have the following result.

Proposition 4 ([2], Lemma 2.5)**.** *Let h_D denote the class number of $\mathcal{O}_D$ and let $\omega(\cdot)$ be the number of prime divisors function. Then there are $h_D \cdot 2^{\omega(N)}$ complex multiplication points of discriminant D on the Shimura curve X_N.*

2.1 The p-adic uniformisation of Shimura curves

Let p denote a prime dividing N so that $N = pN'$. Denote by $\mathbb{C}_p$ the completion with respect to the p-adic norm of the algebraic closure of $\mathbb{Q}_p$ and let

$$\mathcal{H}_p = \mathrm{P}^1(\mathbb{C}_p) - \mathrm{P}^1(\mathbb{Q}_p)$$

be Drinfeld's p-adic upper half plane.
Let B be the definite quaternion algebra over $\mathbb{Q}$ ramified at N' and at ∞. Again it has a basis $\{1, i, j, k\}$ such that

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k,$$

for some $a, b \in \mathbb{Q}$ now with $a, b < 0$. Since B is split at p, there exists $Z_1, Z_2 \in \mathbb{Q}_p$ such that $Z_1^2 - aZ_2^2 = b$ and we may fix an embedding $\iota : B \hookrightarrow M_2(\mathbb{Q}_p)$:

$$\iota : A + Bi + Cj + Dk \ \mapsto \begin{pmatrix} A + Z_1C - aZ_2D & aB + aZ_2C - aZ_1D \\ B - Z_2C + Z_1D & A - Z_1C + aZ_2D \end{pmatrix}. \tag{6}$$

Let $R[\frac{1}{p}]$ be the maximal $\mathbb{Z}[\frac{1}{p}]$ order of B, and consider $(R[\frac{1}{p}])_1^*$, the subgroup of its units of norm 1. The group $\Gamma_N^{(p)} := \iota((R[\frac{1}{p}])_1^*) \subseteq SL_2(\mathbb{Q}_p)$ is a discrete subgroup acting on $\mathcal{H}_p$ whose quotient $\Gamma_N^{(p)}\backslash\mathcal{H}_p$ is compact and its points again correspond to the $\mathbb{C}_p$ points of an algebraic curve over $\mathbb{Q}$, the Shimura curve X_N.

Theorem 5 (Cerednik-Drinfeld). *The quotient $\Gamma_N^{(p)}\backslash\mathcal{H}_p$ is isomorphic as a p-adic rigid analytic space to $X_N(\mathbb{C}_p)$, where X_N is the algebraic curve over $\mathbb{Q}$ whose complex points are identified with the Riemann surface $\Gamma_N\backslash\mathcal{H}$.*

The identification $\varphi : \Gamma_N^{(p)}\backslash\mathcal{H}_p \to X_N(\mathbb{C}_p)$ is defined over the quadratic extension $\mathbb{Q}_{p^2}$ of $\mathbb{Q}_p$ so that for any $\tau \in \Gamma_N^{(p)}\backslash\mathcal{H}_p(\overline{\mathbb{Q}_p})$ and any $\delta \in Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$,

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

where w_p it the Atkin-Lehner involution in p.

Again, let $K = \mathbb{Q}(\sqrt{D})$ with maximal order $\mathcal{O}_D$ and let H denote its ring class field, if p and N' are inert in K, then there exists an optimal embedding φ of $\mathcal{O}_D$ into the quaternionic order $R_N[\frac{1}{p}]$. In this setting, there are *two* conjugate fixed points for the action of $\iota(\phi(\mathcal{O}_D))$ in $\mathcal{H}_p$, hence two p-adic conjugate CM points. Cerednik-Drinfeld's theorem implies that these two points $\tau, \tau' \in \mathcal{H}_p$ correspond to two CM points of discriminant D on the Shimura curve $X_N = \Gamma_N\backslash\mathcal{H}$. If we let P denote the point of $X_N(H)$ corresponding to τ via the choice of an embedding $H \hookrightarrow \overline{\mathbb{Q}_p}$, then by the above, τ' corresponds to the point $w_p(P')$ where P' denotes the image of P by the Frobenius automorphism arising from such embedding.

3 A p-adic cross ratio

Fix once and for all $N = pq$ for primes p, q. We use the same notation as above, only for simplicity denote $\Gamma := \Gamma_N^{(p)}$. Fix two points $w_1, w_2 \in \mathcal{H}_p$. The theta function (see [7]) associated to Γ is defined as

$$\Theta(w_1, w_2; z) = \prod_{\gamma\in\Gamma} \frac{(z - \gamma w_1)}{(z - \gamma w_2)}.$$

It is known (again see [7]) that $\Theta(w_1, w_2; z)$ converges for all z in $\mathcal{H}_p$ and is a rigid analytic meromorphic function so that

$$\Theta(w_1, w_2; \gamma z) = c(\gamma) \cdot \Theta(w_1, w_2; z) \quad \text{for any } \gamma \in \Gamma_N^{(p)}.$$

The automorphy factor from $\Gamma_N^{(p)}$ to $\mathbb{C}_p^*$ given by $\gamma \mapsto c(\gamma)$ measures the obstruction to the divisor $(w_1) - (w_2)$ being principal. If the curve is of genus zero this obstruction is trivial and Θ defines, up to a constant, a rational function on X_N. Hence if w_1 and w_2 correspond to algebraic points on X_N, the ratio $\Theta(w_1, w_2; \tau_1)/\Theta(w_1, w_2; \tau_2)$, for some other algebraic points τ_1 and τ_2, is also algebraic. In particular, this is the case for CM points.

Let D_1 and D_2 be two negative different discriminants such that p and N' are inert in both $\mathbb{Q}(\sqrt{D_i})$, for $i = 1, 2$. Fix embeddings $\phi_1 : \mathcal{O}_{D_1} \hookrightarrow R$ and $\phi_2 : \mathcal{O}_{D_2} \hookrightarrow R$. For $i = 1, 2$, let $\{\tau_i, \tau_i'\} \in \mathcal{H}_p$ be the two fixed CM points of $\iota(\phi_i(\mathcal{O}_{D_i}))$ respectively.

Definition 6.

$$J_N^{(p)}(\tau_1, \tau_2) := \frac{\Theta(\tau_1, \tau_1'; \tau_2)}{\Theta(\tau_1, \tau_1'; \tau_2')} = \prod_{\gamma \in \Gamma_N^{(p)}} [\gamma\tau_1, \gamma\tau_1', \tau_2, \tau_2'],$$

where $[\tau_1, \tau_1', \tau_2, \tau_2']$ denotes the cross-ratio of the four numbers..

Since for $i = 1, 2$ the points τ_i, τ_i' on X_N have coefficients in H_i, the ring class field associated to $\mathbb{Q}(\sqrt{D_i})$, it follows that as an algebraic number this quantity belongs to $H := H_1 H_2$.

Since the curve X_N is of genus 0, there exists a generator j_N of the function field. Considering X_N as the complex quotient $\Gamma_N \backslash \mathcal{H}$, again denote by $\tau_1, \tau_1' \in \mathcal{H}$ the corresponding points. $\Theta(\tau_1, \tau_1', z)$ is a scalar multiple of a rational function defined over $\overline{\mathbb{Q}}$ and hence may be written as

$$\Theta(\tau_1, \tau_1'; z) = \lambda \frac{j_N(z) - j_N(\tau_1)}{j_N(z) - j_N(\tau_1')}.$$

for some constant $\lambda \in \mathbb{C}_p$. We then the following simple expression:

$$J_N^{(p)}(\tau_1, \tau_2) = [j_N(\tau_1), j_N(\tau_1'), j_N(\tau_2), j_N(\tau_2')].$$

The superscript (p) is now only indicating how τ_i and τ_i' relate for $i = 1, 2$.

Suppose that D_1 and D_2 are both of class number one. This implies there are only $\omega(N) = 4$ CM points for each discriminant on the genus-zero Shimura curve, given by the Atkin-Lehner orbit of one such point $P_i \in X_N(H)$, for $i = 1, 2$, so that we may denote by $\{P_i, w_p(P_i), w_q(P_i), w_N(P_i)\}$ the points of discriminant D_i. Let $(\tau_i) \in \Gamma_N^{(p)} \backslash \mathcal{H}_p$ be the point corresponding to P_i. As mentioned in section 2.1, τ_i' is then identified to $w_p(P_i')$, where P_i' is the image of P_i by the Frobenius arising from a chosen embedding $H \hookrightarrow \overline{\mathbb{Q}_p}$, so that we may rewrite the above expression as

$$J_N^{(p)}(\tau_1, \tau_2) = [j_N(P_1), j_N(w_p(P_1')), j_N(P_2), j_N(w_p(P_2'))].$$

This implies that in this case, the cross-ratio itself is invariant to the choice of the embeddings of the quadratic orders into the quaternion algebra. Indeed, fix an $i = 1, 2$ and suppose we change the embedding giving τ_i. Any such other embedding corresponds to a point in $\{P_i, w_p(P_i), w_q(P_i), w_N(P_i)\}$. Observe that

$$w_q(P_i) = w_p(P_i'), \quad w_N(P_i) = P_i',$$

and hence up to Galois conjugation and up to inverses, the quantity $J_N^{(p)}(\tau_1, \tau_2) \in \mathbb{Q}_p$ does **not** depend on the choice of the embeddings τ_1 and τ_2. It does however depend on the choice of p, as for the other prime q dividing N,

$$J_N^{(q)}(\tau_1, \tau_2) = [j_N(P_1), j_N(w_q(P_1')), j_N(P_2), j_N(w_q(P_2'))].$$

When the discriminants of τ_1 and τ_2 have class number different from one, the study of the individual expressions $J_N^{(q)}(\tau_1, \tau_2)$ is more subtle, and they satisfy no simple Shimura reciprocity law. Their norms to the biquadratic field $\mathbb{Q}(\tau_1, \tau_2)$, however, continue to be independent of the choice of τ_1 and τ_2.

3.1 The norm invariant

Obtained results suggest that in all cases the *norm* of this quantity is independent, up to multiplicative inverse, of these choices. It is hence natural to define the following invariant, already mentioned in Definition 2 of the introduction.

Definition 7. Let $N = 6, 10, 22$ and let D_1, D_2 be two imaginary discriminants and let H_1 and H_2 be their associated ring class fields. For any prime p dividing N let τ_1,$\tau_2 \in \mathcal{H}_p$ be arbitrary complex multiplication points of discriminant D_1 and D_2 respectively. Define:

$$\mathcal{J}_N(D_1, D_2) = \mathrm{Norm}_{H_1 H_2/\mathbb{Q}}(J_N^{(p)}(\tau_1, \tau_2))$$

In Section 5 we will propose a formula for its factorisation.

4 Algorithm

In this section we present a simple recursive algorithm to compute $J_N^{(p)}$ as defined in Definiton 6, largely inspired by [10] and [4]. Fix N and p so that we may write $J(\tau_1, \tau_2)$ instead.

Let R_n denote the elements in R whose denominator is divisible exactly by p^n,

$$R_n = \{x \in (R[\tfrac{1}{p}])_{\mathrm{norm}=1} \ : \ x = \tfrac{a+bi+cj+dk}{p^n}, \ gcd(a, b, c, d, p) = 1\}.$$

Define $\Gamma_n = \iota(R_n)$ so that $\Gamma = \bigsqcup_{n=0}^{\infty} \Gamma_n$ and

$$J(\tau_1, \tau_2) = \prod_{\gamma \in \Gamma} [\gamma\tau_1, \gamma\tau_1', \tau_2, \tau_2'] = \prod_n \prod_{\gamma \in \Gamma_n} [\gamma\tau_1, \gamma\tau_1', \tau_2, \tau_2'].$$

Let $M_i \in GL_2(\mathbb{Z}_p)$ be the matrix given by $\iota(\phi_i(\sqrt{D_i}))$.

Lemma 8 (Remark 5.1.5 of [11]). *Set* $t = \frac{1}{2} tr(M_1 M_2)$. *Then*

$$[\tau_1, \tau_1', \tau_2, \tau_2'] = \frac{t - \sqrt{D_1 D_2}}{t + \sqrt{D_1 D_2}}.$$

Proof. The proof follows from direct computations. □

Denoting $t(\phi_1, \phi_1) := \frac{1}{2}\mathrm{tr}(\phi_1(\sqrt{D_1})\phi_2(\sqrt{D_2}))$, and observing that $\gamma\tau_2$ is a fixed point of $\gamma\phi_2\gamma^{-1}$, one may write:

$$J(\tau_1, \tau_2) = \prod_{\gamma\in\Gamma} \frac{t(\phi_1, \gamma\phi_2\gamma^{-1}) - \sqrt{D_1D_2}}{t(\phi_1, \gamma\phi_2\gamma^{-1}) + \sqrt{D_1D_2}}. \quad (7)$$

If $\gamma \in \Gamma_n$, then for $t = t(\phi_1, \gamma\phi_2\gamma^{-1})$, $t \in p^{-2n}\mathbb{Z}_p^\times$, see Proposition 6.5.7 of [11]. Hence for $\gamma \in \Gamma_n$, writing $t(\phi_1, \gamma\phi_2\gamma^{-1}) = \frac{x}{p^{2n}}$,

$$\frac{t(\phi_1, \gamma\phi_2\gamma^{-1}) - \sqrt{D_1D_2}}{t(\phi_1, \gamma\phi_2\gamma^{-1}) + \sqrt{D_1D_2}} = \frac{x - p^{2n}\sqrt{D_1D_2}}{x + p^{2n}\sqrt{D_1D_2}}. \quad (8)$$

Then the expression (8) is congruent to 1 modulo p^{2n}. This implies that to approximate $J(\tau_1, \tau_2)$ up to M digits of precision, it suffices to compute $\prod_{n=0}^{M/2}\prod_{\gamma\in\Gamma_n}[\gamma\tau_1, \gamma\tau_1', \tau_2, \tau_2']$. Denote this *finite* approximation by

$$J_M(\tau_1, \tau_2) := \prod_{n\leq M/2}\prod_{\gamma\in\Gamma_n}[\gamma\tau_1, \gamma\tau_1', \tau_2, \tau_2'].$$

The cardinality of Γ_n being exponential, enumerating all of its elements is not a feasible option. This paper computes these finite products recursively instead, in the case where the underlying quaternion algebra is of class number one (i.e. every left ideal for a maximal order is principal) as this ensures that there is a unique factorisation among quaternions. For the rest of the paper suppose that this is the case. The rational quaternion algebras of discriminants 2, 3 and 5 are all of class number one, so we only exclude the algebra of discriminant 11.
For a more detailed account of unique factorization in quaternion algebras and the proofs of Theorem 10 and Lemmas 12 and 13, see [10].

Definition 9. A quaternion is said to be *primitive* if it cannot be written as $q = nq'$ for n an integer. Otherwise the quaternion is said to be *nonprimitive*.

The following unique factorization theorem holds. The proof relies on the fact that the left ideal of every maximal order is principal.

Theorem 10. *If q is a primitive quaternion and $nrd(q) = p_1...p_n$ is a fixed factorization of $nrd(q)$ as a product of prime numbers, then q can be written as $q = q_1, ...q_n$ where $q_i \in R$ have norm $nrd(q_i) = p_i$ and these factors are unique up to multiplication by units.*

Define

$$Q_n^{pr} = \{x \in B \ : \ nrd(x) = p^n \text{ and } x \text{ is primitive } \},$$

and observe that

$$\Gamma_n = \{\tfrac{\iota(x)}{p^n} \ : \ x \in Q_{2n}^{pr}\}.$$

Definition 11. Define an equivalence relation between (primitive) norm 1 quaternion as follows: $q \sim q'$ iff $q = q'\epsilon$ for ϵ a unit. Let $T = \{r_1, .., r_k\} \subset Q_1^{pr}$ be a set of representatives of the equivalence classes, and denote by $T_i := \{r_i\epsilon \ : \ \epsilon \text{ a unit } \}$ the respective equivalence classes. For each i, denote by T_{i^*} the equivalence class of $\overline{r_i}$.

Lemma 12.

$$|T| = p + 1.$$

By unique factorization we can write any $q \in Q_n^{pr}$ as a product $q = q_1 q_2 ... q_n$, where each quaternion q_i has norm p (in a unique way up to units). Then clearly

$$Q_n^{pr} = \bigsqcup_{r_i \in T} \{q = q_1..q_n \ : \ q_1 \in T_{r_i}\}.$$

Denote by $r_i(Q_n^{pr}) := \{q = q_1..q_n \ \in Q_n^{pr} : \ q_1 \in T_{r_i}\}$. The main result we will need is the following recursive formula for the sets Q_n^{pr}:

Lemma 13. *For $n \geq 2$,*

$$Q_n^{pr} = \bigsqcup_{r_i \in T} \bigsqcup_{r_j \notin T_{i^*}} r_i r_j (Q_{n-1}^{pr}).$$

Fix once and for all τ_1 and its conjugate τ_1'. Define:

$$\theta_n(z) := \prod_{q \in Q_n^{pr}} \frac{z - \iota(q)\tau_1}{z - \iota(q)\tau_1'}.$$

Since Mobius transformations are equal up to multiplication by constants,

$$\Theta(\tau_1, \tau_1'; z) = \prod_{n=0}^{\infty} \theta_{2n}(z).$$

Following what is done in [4], we represent $\theta_n(z)$ as power series in certain disks.

By definition $\tau_1 = \frac{A+\sqrt{D}}{C}$ with $A, C \in \mathbb{Z}_p$, and for $q \in Q_n^{pr}$, $\iota(q)\tau_1 = \frac{A'+p^n\sqrt{D}}{C'}$, for some other $A', C' \in \mathbb{Z}_p$. Classify the q in Q_n^{pr}, for $n \geq 1$ according to the residue of $\iota(q)\tau_1 \mod p\mathbb{O}_{\mathbb{C}_p}$. Observe that this classification is the same if instead of τ_1 we take its conjugate τ_1', as the residue of $\iota(q)\tau_1' = \frac{A'-p^n\sqrt{D}}{C'}$ is also $\frac{A'}{C'}$. Define, for $a = 0, 1, ..., p-1, \infty$, the classes

$$Q_n^a = \{ \ q \in Q_n^{pr} \ : \ \iota(q)\tau_1 \in a + p\mathcal{O}_{\mathbb{C}_p} \ \},$$

and the functions

$$\theta_n^{(a)}(z) := \prod_{q \in Q_n^a} \frac{z - \iota(q)\tau_1}{z - \iota(q)\tau_1'}.$$

Lemma 14. *For all $i \in \{ 0, .., p-1, \infty \}$ there is one index $j_i \in \{0, .., p-1, \infty\}$ such that for all $j \in \{0, .., p-1, \infty\}$ if $j \neq j_i$ then,*

$$\iota(r_i)j \equiv a_{r_i},$$

where $a_{r_i} \in \{ 0, .., p-1, \infty \}$ is a constant independent of j.

Proof. Let $\iota(r_i) = \left(\begin{smallmatrix} R_1 & R_2 \\ R_3 & R_4 \end{smallmatrix}\right)$ be the embedding of r_i into $M_2(\mathbb{Z}_p)$. Then:

$$\iota(r_i)j = \tfrac{R_1 j + R_2}{R_3 j + R_4}.$$

If $R_3 j + R_4 \in p\mathcal{O}_{\mathbb{C}_p}$, then $\iota(r_i)j \equiv \infty$. This happens when $j = j_i \equiv -\frac{R_4}{R_3}$.

In all other cases we can compute that $\iota(r_i)j \equiv \frac{R_1}{R_3}$. □

In general for any $r \in Q_1^{pr}$, we will denote by $a_r \in \{ 0, .., p-1, \infty \}$ the value such that $\iota(r)j = a_r$ for all $j \in \{0, .., p-1, \infty\}$ except one.

Lemma 15. *If $i \neq j$, then $a_{r_i} \neq a_{r_j}$.*

Proof. As before, this follows from direct calculations. Let $\iota(r_i) = \left(\begin{smallmatrix} R_1 & R_2 \\ R_3 & R_4 \end{smallmatrix}\right)$ and $\iota(r_j) = \left(\begin{smallmatrix} T_1 & T_2 \\ T_3 & T_4 \end{smallmatrix}\right)$. By Lemma 14, $a_{r_i} \equiv \frac{R_1}{R_3}$ and $a_{r_j} \equiv \frac{T_1}{T_3}$. If $a_{r_i} = a_{r_j}$, then $\frac{R_1}{R_3} \equiv \frac{T_1}{T_3} \equiv \frac{T_2}{T_4} \equiv \frac{R_2}{R_4} \pmod p$. Then each entry of the matrix $\iota(\overline{r_i})\iota(r_j) = \left(\begin{smallmatrix} R_4 & -R_2 \\ -R_3 & R_1 \end{smallmatrix}\right)\left(\begin{smallmatrix} T_1 & T_2 \\ T_3 & T_4 \end{smallmatrix}\right)$ has positive p-adic valuation and hence $r_i^{-1} r_j = \frac{1}{p}\overline{r_i} r_j = \epsilon$ is a unit. But $r_j = r_i \epsilon$ contradicts the fact that r_i and r_j are representatives of different equivalence classes. □

The previous lemmas imply that the set $\{a_{r_i}\}_{r_i \in T}$ is the set $\{0, 1, ..., p-1, \infty\}$ and each set $r_i(Q_1^{pr}) = \{q \ \in Q_1^{pr} \ : \ q \in T_{r_i}\}$ defined in the previous section corresponds to the set $Q_1^{a_{r_i}}$.

Lemma 16. *The index j_i such that $\iota(r_i)j \neq a_{r_i}$ verifies*

$$j_i = a_{\overline{r_i}}.$$

Proof. If $\iota(r_i) = \left(\begin{smallmatrix} R_1 & R_2 \\ R_3 & R_4 \end{smallmatrix}\right)$, then $\iota(\overline{r_i}) = \left(\begin{smallmatrix} R_4 & -R_2 \\ -R_3 & R_1 \end{smallmatrix}\right)$. By Lemma 14, the j such that $t_{i,j} \neq a_i$, is $j \equiv -\frac{R_4}{R_3}$, and again by the same lemma, this is exactly $a_{\overline{r_i}}$. □

Combining Lemmas 13, 14, 15 and 16 we obtain:

Lemma 17. *For all $a \in \{0, .., p-1, \infty\}$ and all $n > 1$:*

$$Q_n^{(a)} = \bigsqcup_{\substack{i,j \ : \ a_{r_i} = a \\ j \neq a_{\overline{r_i}}}} \{ \ r_i q \ : \ q \in Q_{n-1}^{(j)} \ \}.$$

Hence

$$\theta_n^{(a)}(z) = \prod_{\substack{i,j\ :\ a_{r_i}=a \\ j\neq a_{\overline{r_i}}}} \prod_{q\in Q_{n-1}^j} \frac{z-\iota(r_i)\iota(q)\tau_1}{z-\iota(r_i)\iota(q)\tau_1'}.$$

Since two rational functions with the same divisor are equal up to a constant:

$$\begin{aligned}\theta_n^{(a)}(z) &= c \prod_{\substack{i,j\ :\ a_{r_i}=a \\ j\neq a_{\overline{r_i}}}} \prod_{q\in Q_{n-1}^j} \frac{\iota(r_i)^{-1}z-\iota(q)\tau_1}{\iota(r_i)^{-1}z-\iota(q)\tau_1'} \\ &= c \prod_{\substack{i,j\ :\ a_{r_i}=a \\ j\neq a_{\overline{r_i}}}} \theta_{n-1}^{(j)}(\iota(r_i)^{-1}z), \qquad (9)\end{aligned}$$

for some $c \in \mathbb{C}_p$.

To compute the constant, again following [4], we approximate each $\theta_n^{(a)}$ as a power series in $x_a = \frac{1}{z-a}$, instead of in z, for $a = 0, .., p-1$ and $x_a = z$ for $a = \infty$. In this way:

$$\theta_n^{(a)} \in 1 + p\mathcal{O}_{\mathbb{C}_p}\langle x_a\rangle.$$

Hence by normalizing at each recursion the right hand side of (9) one implicitly finds the correct constant.

Algorithm 1 below summarizes how to compute all $\theta_n^a(z)$ for $n \leq M$, where M is a given precision.

Algorithm 1 Algorithm to compute $\theta_k^{(a)}$ for $k \leq M$ for a given M.

- Compute $\theta_0(z)$, for example by enumerating Γ_0 (Γ_0 has at most 24 elements).
- **For** $a = 0, ..., p-1$:
  Compute the power series $\theta_1^{(a)}$ in variable $x = \frac{1}{z-a}$ given by: $\theta_1^{(a)} = \prod_{q \in Q_1^a} \frac{z-\iota(q)w}{z-\iota(q)w'}$.
- Compute the power series $\theta_1^{(\infty)}$ in variable $x = z$ given by: $\theta_1^{(\infty)} = \prod_{q \in Q_1^\infty} \frac{1/z-1/\iota(q)w}{1/z-1/\iota(q)w'}$.

  These two steps will again require us to enumerate Γ_1.
- Compute the indexes a_{r_i}, for $i = 1, .., p+1$.
- Compute the indices $a_{\overline{r_i}}$, for $i = 0, 1, .., p+1$.
- **For** $n = 2, ..., M$:
  For each $a = 0, ..., p-1, \infty$, compute $\theta_n^{(a)}$ recursively using (9) in the variable $x = \frac{1}{z-a}$ (or $x = z$ if $a = \infty$) and normalizing so the constant term is one.

One can easily recover $J_M(\phi_1, \phi_2)$ from the functions $\theta_{2n}^{(a)}(z)$:

$$J_M(\phi_1, \phi_2) = \prod_{n=0}^{M/2} \prod_a \frac{\theta_{2n}^{(a)}(\tau_2)}{\theta_{2n}^{(a)}(\tau_2')}.$$

All constants and all elements of $\mathbb{Q}_p$ used in above algorithm are always computed with M digits of p-adic precision.

Observe that if instead of $\Gamma_{\leq M}^p$, we would like to take $\Gamma_{\leq M}^p / \langle \pm 1 \rangle$, it suffices to take the square root of the result. Results reported in the following section are for the group $\Gamma_{\leq M}^p / \langle \pm 1 \rangle$.

The algorithm was implemented using Sage and the code can be found in the appendix.

5 Results and discussion

This section discusses results for the invariant $J_N^{(p)}(\tau_1, \tau_2)$ for the pairs N, p such that the quaternion algebra ramified at $N' = N/p$ has class number one. The possible pairs are: $(6, 3)$, $(6, 2)$, $(10, 2)$, $(10, 5)$, $(22, 11)$. We only exclude the 2-adic uniformisation of the Shimura curve of discriminant 22.
The result returned by the algorithm described in the previous section is a p-adic number. To recognize it as an algebraic integer GP/PARI's `algdep` function

was used. For each pair (N, p), the invariant $J_N^{(p)}(\tau_1, \tau_2)$ is computed for all discriminants D_1 and D_2 of class number one that are both inert with respect to N, see tables 3 to 6. Discriminants of higher class numbers (D_1 of class number 3 or 5) are also computed and reported in tables 8 to 10. The reason only few discriminants of higher class number have been computed is that PARI's `algdep` function requires large precision to recognise higher degree polynomials, making calculations extremely slow.
In table 1 we indicate for each $q = 2, 3, 5$ the choice of quaternion algebra split at q, ∞ and of the respective maximal order used for computations. The embeddings into the matrix algebras used are those given by (5) or (6). Tables of results are reported in the following section.

q	B	R
2	$\left(\frac{-1,-1}{\mathbb{Q}}\right)$	$\mathbb{Z}[i, j, k\frac{1+i+j+k}{2}]$
3	$\left(\frac{-1,-3}{\mathbb{Q}}\right)$	$\mathbb{Z}[1, i, \frac{1+j}{2}, \frac{i+k}{2}]$
5	$\left(\frac{-2,-5}{\mathbb{Q}}\right)$	$\mathbb{Z}[1, j, \frac{1+j+k}{2}, \frac{i+2j+k}{4}]$

Table 1: Choice of quaternion algebras and their maximal orders.

Results suggest that $J_N^{(p)}(\tau_1, \tau_2)$ seems to satisfy many properties that are very similar to those satisfied by differences of singular moduli found by Gross and Zagier, [8].
To illustrate this, consider the case $D_1 = -43$, $D_2 = -163$. First consider $N = 6$, $p = 3$. The following embeddings into R are used:

$$\phi_1(\tfrac{1+\sqrt{-43}}{2}) = \tfrac{1}{2} + \tfrac{3}{2}i + \tfrac{3}{2}j - \tfrac{5}{2}k,$$
$$\phi_2(\tfrac{1+\sqrt{-163}}{2}) = \tfrac{1}{2} + \tfrac{1}{2}i + \tfrac{9}{2}j - \tfrac{9}{2}k.$$

Up to 150 digits of 3-adic precision, $J_6^{(3)}(\tau_1, \tau_2)$ satisfies the quadratic equation:

$$929481868492960000000x^2 - 3812328474564167050067x + 2727732351591040000000$$

The discriminant is a highly divisible integer that factorizes as:

$$3^4 \cdot 13^2 \cdot 19^6 \cdot 23^4 \cdot 37^2 \cdot 43 \cdot 67^2 \cdot 109^2 \cdot 139^2 \cdot 157^2 \cdot 163,$$

and so is the leading term

$$2^{10} \cdot 5^6 \cdot 73^2 \cdot 137^2 \cdot 241^2,$$

and the constant term

$$2^{12} \cdot 5^6 \cdot 29^2 \cdot 257^2 \cdot 277^2.$$

The factors of the discriminant are smaller than $\max(D_1, D_2)$ and the factors of the leading and constant terms are inert in both $\mathbb{Q}(\sqrt{D_1})$ and $\mathbb{Q}(\sqrt{D_2})$ and divide to an odd power an integer of the form $\frac{D-x^2}{4\cdot 2\cdot 3}$ where $D = D_1D_2$. Observe that

$$43 \cdot 163 \equiv 1 \pmod{12},$$

and the four square roots of 1 modulo 12 are $\{+1, -1, +5, -5\}$. Following (4), define

$$\delta(x) = \begin{cases} +1 & \text{if } x \equiv \pm 5 \pmod{12}, \\ -1 & \text{if } x \equiv \pm 1 \pmod{12}. \end{cases}$$

Then $F(\frac{D-x^2}{4N})$ and $\delta(x)$ for $|x|$ odd and less than $\sqrt{D} \sim 83.719$ are given by the following table, where F is defined in (1) and $m = m(x) = \frac{D-x^2}{4N}$. For any

$\lvert x\rvert$	$\frac{D-x^2}{4N}$	$F(m)$	$\delta(x)$	$\lvert x\rvert$	$\frac{D-x^2}{4N}$	$F(m)$	$\delta(x)$	$\lvert x\rvert$	$\frac{D-x^2}{4N}$	$F(m)$	$\delta(x)$
1	292	73	-1	31	252	7	$+1$	61	137	137	-1
5	291	3^2	$+1$	35	241	241	-1	65	116	29	$+1$
7	290	1	$+1$	37	235	5^2	-1	67	105	1	$+1$
11	287	7^2	-1	41	222	1	$+1$	71	82	2^2	-1
13	285	1	-1	43	215	5^2	$+1$	73	70	1	-1
17	280	1	$+1$	47	200	2^2	-1	77	45	5	$+1$
19	277	277	$+1$	49	192	3	-1	79	32	2^3	$+1$
23	270	1	-1	53	175	7	$+1$	83	5	5	-1
25	266	1	-1	55	166	2^2	$+1$				
29	257	257	$+1$	59	147	3	-1				

Table 2: Values of $F(\frac{D-x^2}{4N})$ and $\delta(x)$ for $|x|$ odd and less than $\sqrt{D}$.

other embedding $\tilde{\tau}_1$, $\tilde{\tau}_2$, the invariant $J_6^{(3)}(\tilde{\tau}_1, \tilde{\tau}_2)$ satisfies the same polynomial, up to inverting constant and leading term, as predicted by section 3. However, if we consider $N = 6$ and $p = 2$, the 2-adic quantity $J_6^{(2)}(\tau_1, \tau_2)$, as expected, satisfies a different polynomial. The discriminant of this polynomial is still highly factorizable, and so are the constant and coefficient terms whose factors are again among those in the table. Remarkably, the norm of $J_6^{(2)}(\tau_1, \tau_2)$ and of $J_6^{(3)}(\tau_1, \tau_2)$ is the same:

$$N_{\mathbb{Q}(\sqrt{D_1D_2})/\mathbb{Q}}(J_6^{(3)}(\tau_1, \tau_2)) = N_{\mathbb{Q}(\sqrt{D_1D_2})/\mathbb{Q}}(J_6^{(2)}(\tau_1, \tau_2)) = \Big(\frac{2^2 \cdot 29^2 \cdot 257^2 \cdot 277^2}{73^2 \cdot 137^2 \cdot 241^2}\Big)^2.$$

Using table 2, we verify that indeed

$$\prod_{\substack{x^2 \leq 43\cdot 163 \\ x^2 \equiv 43\cdot 163 \pmod{24}}} F\Big(\frac{43 \cdot 163 - x^2}{24}\Big)^{\delta(x)} = \frac{2^2 \cdot 29^2 \cdot 257^2 \cdot 277^2}{73^2 \cdot 137^2 \cdot 241^2}.$$

These properties hold for all invariants computed and we list here below a series of remarks that are supported by the computed results.

Theorem 18. *For any p dividing N, for any embeddings τ_1 and τ_2 of discriminant D_1 and D_2 respectively, the invariant $J_N^{(p)}(\tau_1, \tau_2)$ belongs to the compositum of the respective ring class fields $H_{D_1}H_{D_2}$ and satisfies a polynomial equation over $\mathbb{Z}$ of degree $2h(D_1)h(D_2)$.*

Observation 19. *The leading coefficient and the constant term of the integer polynomial equation satisfied by $J_N^{(p)}(D_1, D_2)$ are highly divisible integers. For each prime factor l of both the leading coefficient and the constant term there is an odd integer $|x| < \sqrt{D_1D_2}$ such that $F(\frac{D_1D_2-x^2}{4pq})$ is a power of l.*

Conjecture 20. *The invariant $\mathcal{J}_N(D_1, D_2)$, i.e. the norm of $J_N^{(p)}(\tau_1, \tau_2)$, recovered from the tables as the square of the quotient of the constant and leading term of its minimal polynomial, is independent of the choice of the prime p dividing N and of the choice of complex multiplication points τ_1, τ_2 of discriminant D_1 and D_2.*

As mentioned in section 3 the p-adic quantity $J_N^{(p)}(\tau_1, \tau_2)$ is itself invariant of the choice of embeddings in the case the discriminants are of class number one. For discriminants of higher class numbers, we empirically obtain 2 different invariants when D_1 is of class number 3, and 3 different invariants when it is of class number 5. Even though the data is not extensive, this might suggest that for an element $\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}_D)$ we have that $J_N^{(p)}(\tau_1^{\sigma_\mathfrak{a}}, \tau_2)$ and $J_N^{(p)}(\tau_1^{-\sigma_\mathfrak{a}}, \tau_2)$ satisfy the same polynomials.

Finally all data in the tables seem to suggest that $\mathcal{J}_N(D_1, D_2)$ admits a factorisation very similar to that proved by Gross and Zagier, introduced as conjecture 3 in the introduction. There are 4 square roots of $D = D_1D_2$ modulo $2N$, say $\{a, -a, b, -b\}$. Define

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

Conjecture 21. *Using the same notations as Gross-Zagier's Theorem 1, the following formula holds:*

$$\mathcal{J}_N(D_1, D_2)^{\pm\frac{4}{w_1w_2}} = \prod_{\substack{x^2<D \\ x^2\equiv D (mod\ 4N)}} F\Big(\frac{D-x^2}{4N}\Big)^{2\delta(x)}.$$

The choice of a and b in the definition of the function δ is arbitrary, as the invariant $\mathcal{J}_N^{(p)}(D_1, D_2)$ is considered up to multiplicative inverse.

The tables in the following section supply convincing evidence for this formula.

We conclude this section with some further remarks.

Remark 1. We have also computed $J_N^{(p)}(\tau_1, \tau_2)$ for N such that X_N is not a genus 0 curve. In general GP/PARI fails to recognize $J_N^{(p)}(\tau_1, \tau_2)$ as an algebraic number (as expected). However this was not the case for $N = 14, p = 17$. For $D_1 = -11$ and $D_2 = -3$ (both of class number 1), the quantity $J_N^{(p)}(\tau_1, \tau_2)$ seems to satisfy, up to 100 digits of 17-adic precision, the equation:

$$2x^4 - 293x^2 + 2.$$

Similarly, for $D_1 = -11$ and $D_2 = -163$, the invariant $J_N^{(p)}(\tau_1, \tau_2)$ seems to satisfy (again up to 100 digits of 17-adic precision) the polynomial

$$57122x^4 - 11631377x^2 + 76832,$$

whose leading and constant term again are highly divisible and its factors behave as those in observation 19.

Remark 2. The quantity $J(\tau_1, \tau_2)$ is computed by considering the action of all elements in R that have norm p^{2k} for an *even* power. However, if both even and odd powers are considered, the result seems to have remarkable properties as well. Indeed it seems to satisfy a palindromic polynomial over $\mathbb{Z}$ of degree $2h(D_1)h(D_2)$ whose leading term is again highly factorisable and its factors again follow observation 19. Table 12 illustrates an example for the pair $N = 10$ and $p = 5$, and they hold also for the other pairs (N, p) mentioned above.

6 Tables

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $p = 3$, $M = 150$							
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	Δ_f	a_n	a_0
-19	-43	$i + 3j - 3k$	$3i + 3j - 5k$	$7750656x^2 - 14480299x$ $+1478656$	$7^4 \cdot 13^2 \cdot 19^3$ $\cdot 37^2 \cdot 43$	$2^{10} \cdot 3^2 \cdot 29^2$	$2^{12} \cdot 19^2$
-19	-67	$i + 3j - 3k$	$3i + 3j - 7k$	$12290826496x^2 - 95390057659x$ $+6219530496$	$7^4 \cdot 11^4 \cdot 13^4$ $\cdot 19 \cdot 43^2 \cdot 61^2 \cdot 67$	$2^8 \cdot 13^4 \cdot 41^2$	$2^8 \cdot 3^2 \cdot 31^2 \cdot 53^2$
-19	-163	$i + 3j - 3k$	$i + 9j - 9k$	$137614689009110557696x^2$ $-361232222403682556459x$ $+208106107946555293696$	$3^4 \cdot 7^4 \cdot 13^4 \cdot 19^5$ $\cdot 23^4 \cdot 67^2 \cdot 109^2$ $\cdot 139^2 \cdot 157^2 \cdot 163$	$2^{10} \cdot 29^2 \cdot 31^2$ $\cdot 37^2 \cdot 103^2 \cdot 107^2$	$2^{14} \cdot 13^4 \cdot 59^2$ $\cdot 89^2 \cdot 127^2$
-43	-67	$3i + 3j - 5k$	$3i + 3j - 7k$	$66564000000x^2 - 194519700667x$ $+51076000000$	$11^4 \cdot 13^2 \cdot 19^2 \cdot 37^2$ $\cdot 43^3 \cdot 61^2 \cdot 67$	$2^8 \cdot 3^2 \cdot 5^6 \cdot 43^2$	$2^8 \cdot 5^6 \cdot 113^2$
-43	-163	$3i + 3j - 5k$	$i + 9j - 9k$	$929481868492960000000x^2$ $-3812328474564167050670x$ $+2727732351591040000000$	$3^4 \cdot 13^2 \cdot 19^6 \cdot 23^4$ $\cdot 37^2 \cdot 43 \cdot 67^2 \cdot 109^2$ $\cdot 139^2 \cdot 157^2 \cdot 163$	$2^{10} \cdot 5^6 \cdot 73^2$ $\cdot 137^2 \cdot 241^2$	$2^{12} \cdot 5^6 \cdot 29^2$ $\cdot 257^2 \cdot 277^2$
-67	-163	$3i + 3j - 7k$	$i + 9j - 9k$	$2417986405054008100000000x^2$ $-5237146236856322922885947x$ $+2592057051817902244000000$	$3^4 \cdot 11^4 \cdot 13^4 \cdot 19^4$ $\cdot 23^4 \cdot 43^2 \cdot 61^2 \cdot 67^3$ $\cdot 109^2 \cdot 139^2 \cdot 157^2 \cdot 163$	$2^8 \cdot 5^8 \cdot 13^4$ $\cdot 31^2 \cdot 67^2$ $\cdot 443^2$	$2^8 \cdot 5^6 \cdot 79^2$ $\cdot 101^2 \cdot 233^2$ $\cdot 433^2$

Table 3: Results for the pair $N = 6$, $p = 3$ with D_1, D_2 of class number 1

$B = \left(\frac{-1,-3}{\mathbb{Q}}\right)$, $p = 2$, $M = 300$							
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	Δ_f	a_n	a_0
-19	-43	$-4i - j$	$-4i - 3j$	$16553403x^2 - 35711431x + 3158028$	$5^6 \cdot 13^2 \cdot 19^3 \cdot 37^2 \cdot 43$	$3^9 \cdot 29^2$	$2^2 \cdot 3^7 \cdot 19^2$
-19	-67	$-4i - j$	$-8i - j$	$105000146667x^2 - 162229401334x$ $+53133254667$	$2^{10} \cdot 5^6 \cdot 13^4$ $\cdot 19 \cdot 43^2 \cdot 61^2 \cdot 67$	$3^7 \cdot 13^4 \cdot 41^2$	$3^9 \cdot 31^2 \cdot 53^2$
-19	-163	$-4i - j$	$-4i - 7j$	$293909496936449989923x^2$ $-1422549305157681125971x$ $+444460994217887136048$	$5^6 \cdot 11^6 \cdot 13^4$ $\cdot 17^6 \cdot 19 \cdot 67^2 \cdot 109^2$ $\cdot 139^2 \cdot 157^2 \cdot 163$	$3^7 \cdot 29^2 \cdot 31^2$ $\cdot 37^2 \cdot 103^2 \cdot 107^2$	$2^4 \cdot 3^7 \cdot 13^4$ $\cdot 59^2 \cdot 89^2 \cdot 127^2$
-43	-67	$4i - 3j$	$-8i - j$	$67049853003x^2 - 158527527670x$ $+87381674667$	$2^{10} \cdot 13^2 \cdot 19^2$ $\cdot 37^2 \cdot 43^3 \cdot 61^2 \cdot 67$	$3^7 \cdot 7^4 \cdot 113^2$	$3^9 \cdot 7^4 \cdot 43^2$
-43	-163	$4i - 3j$	$4i - 7j$	$30504357551201515947x^2$ $-804203716040070393175x$ $+895205444855524877228$	$11^6 \cdot 13^2 \cdot 17^6 \cdot 19^2$ $37^2 \cdot 43 \cdot 67^2 \cdot 109^2$ $139^2 \cdot 157^2 \cdot 163$	$3^7 \cdot 7^4 \cdot 73^2$ $\cdot 137^2 \cdot 241^2$	$2^2 \cdot 3^7 \cdot 7^4$ $\cdot 29^2 \cdot 257^2 \cdot 277^2$
-67	-163	$-8i - j$	$-4i - 7j$	$31742037947788327077748675x^2$ $-6752068041752221534377382x$ $+3402714470588532762628707$	$2^{10} \cdot 11^6 \cdot 13^4 \cdot 17^6$ $\cdot 43^2 \cdot 61^2 \cdot 67^3 \cdot 109^2$ $\cdot 139^2 \cdot 157^2 \cdot 163$	$3^7 \cdot 5^2 \cdot 7^4 \cdot 13^4$ $\cdot 31^2 \cdot 67^2 \cdot 443^2$	$3^7 \cdot 7^4 \cdot 79^2$ $\cdot 101^2 \cdot 233^2 \cdot 433^2$

Table 4: Results for the pair $N = 6$, $p = 2$ with D_1, D_2 of class number 1

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $p=5$, $M=150$							
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	Δ_f	a_n	a_0
-3	-43	$i+j-k$	$3i+3j-5k$	$128x^2 - 32211x + 1458$	$3^9 \cdot 5^2 \cdot 7^2 \cdot 43$	2^7	$2 \cdot 3^6$
-3	-67	$i+j-k$	$3i+3j-7k$	$31250x^2 - 331587x + 93312$	$3^{11} \cdot 7^2 \cdot 13^2 \cdot 67$	$2 \cdot 5^6$	$2^7 \cdot 3^6$
-3	-163	$i+j-k$	$i+9j-9k$	$14512627712x^2 + 181853220987x$ $+22781250$	$3^9 \cdot 7^2 \cdot 13^2 \cdot 17^2$ $\cdot 29^2 \cdot 31^2 \cdot 73^2 \cdot 163$	$2^{13} \cdot 11^6$	$2 \cdot 3^6 \cdot 5^6$
-43	-67	$3i+3j-5k$	$3i+3j-7k$	$1905152x^2 - 8143659x$ $+1062882$	$3^{14} \cdot 5^2$ $\cdot 13^2 \cdot 43 \cdot 67$	$2^9 \cdot 61^2$	$2 \cdot 3^{12}$
-43	-163	$3i+3j-5k$	$i+9j-9k$	$24363515282x^2 - 4428320247459x$ $+221011431552$	$3^{12} \cdot 5^2 \cdot 13^2 \cdot 17^2$ $\cdot 29^2 \cdot 31^2 \cdot 43 \cdot 73^2 \cdot 163$	$2 \cdot 19^2 \cdot 37^2 \cdot 157^2$	$2^7 \cdot 3^{14} \cdot 19^2$
-67	-163	$3i+3j-7k$	$i+9j-9k$	$78059116962x^2 + 269138928987x$ $+23762000000$	$3^{14} \cdot 17^2 \cdot 29^2$ $\cdot 31^2 \cdot 67 \cdot 73^2 \cdot 163$	$2 \cdot 3^{12} \cdot 271^2$	$2^7 \cdot 5^6 \cdot 109^2$

Table 5: Results for the pair $N = 10$, $p = 5$ with D_1, D_2 of class number 1

$B = \left(\frac{-2,-5}{\mathbb{Q}}\right)$, $p=2$, $M=300$							
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	Δ_f	a_n	a_0
-3	-43	$\frac{1}{2}i - \frac{1}{2}k$	$-\frac{1}{2}i + 2j - \frac{3}{2}k$	$18225x^2 + 20547x + 1600$	$3^9 \cdot 19^2 \cdot 43$	$3^6 \cdot 5^2$	$2^6 \cdot 5^2$
-3	-67	$\frac{1}{2}i - \frac{1}{2}k$	$-\frac{7}{2}i + 2j + \frac{3}{2}k$	$390625x^2 + 1789587x + 1166400$	$3^{11} \cdot 11^2 \cdot 31^2 \cdot 67$	5^8	$2^6 \cdot 3^6 \cdot 5^2$
-3	-163	$\frac{1}{2}i - \frac{1}{2}k$	$-\frac{11}{2}i + 4j + \frac{3}{2}k$	$284765625x^2 + 197378004987x$ $+181407846400$	$3^9 \cdot 17^2 \cdot 19^2$ $\cdot 59^2 \cdot 73^2 \cdot 79^2 \cdot 163$	$3^6 \cdot 5^8$	$2^{12} \cdot 5^2 \cdot 11^6$
-43	-67	$-\frac{1}{2}i + 2j - \frac{3}{2}k$	$-\frac{7}{2}i + 2j + \frac{3}{2}k$	$1166905600x^2 + 1901875707x$ $+651015225$	$3^{14} \cdot 11^2 \cdot 19^2$ $\cdot 31^2 \cdot 43 \cdot 67$	$2^8 \cdot 5^2 \cdot 7^2 \cdot 61$	$3^{12} \cdot 5^2 \cdot 7^2$
-43	-163	$-\frac{1}{2}i + 2j - \frac{3}{2}k$	$-\frac{11}{2}i + 4j + \frac{3}{2}k$	$41336989225x^2 + 432007151787x$ $+374984769600$	$3^{12} \cdot 17^2 \cdot 43$ $\cdot 59^2 \cdot 73^2 \cdot 79^2 \cdot 163$	$5^2 \cdot 7^2 \cdot 37^2 \cdot 157^2$	$2^6 \cdot 3^{14} \cdot 5^2 \cdot 7^2$
-67	-163	$-\frac{7}{2}i + 2j + \frac{3}{2}k$	$\frac{11}{2}i + 4j - \frac{3}{2}k$	$8080094344529025x^2$ $+123636715485433347x$ $+2459664025000000$	$3^{14} \cdot 11^2 \cdot 17^2 \cdot 19^2$ $\cdot 31^2 \cdot 59^2 \cdot 67$ $\cdot 73^2 \cdot 79^2 \cdot 163$	$3^{12} \cdot 5^2 \cdot 7^2$ $\cdot 13^2 \cdot 271^2$	$2^6 \cdot 5^8 \cdot 7^2$ $\cdot 13^2 \cdot 109^2$

Table 6: Results for the pair $N = 10$, $p = 2$ with D_1, D_2 of class number 1

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $p = 11$, $M = 150$							
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	Δ_f	a_n	a_0
-3	-67	$i + j - k$	$3i + 3j - 7k$	$16x^2 + 1931x + 1024$	$3^7 \cdot 5^2 \cdot 67$	2^4	2^{10}
-3	-163	$i + j - k$	$i + 9j - 9k$	$62500x^2 - 91827x + 2916$	$3^9 \cdot 7^4 \cdot 163$	$2^2 \cdot 5^6$	$2^2 \cdot 3^6$
-67	-163	$3i + 3j - 7k$	$i + 9j - 9k$	$465124x^2 - 6823331x + 4218916$	$3^{10} \cdot 5^2 \cdot 7^4 \cdot 67 \cdot 163$	$2^2 \cdot 11^2 \cdot 31^2$	$2^2 \cdot 13^2 \cdot 79^2$

Table 7: Results for the pair $N = 22$, $p = 11$ with D_1, D_2 of class number 1

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $p = 3$, $M = 400$						
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	a_n	a_0
-19	-139	$3i + 3j - k$	$3i + 3j - 11k$	$3740673368395874304x^6 - 2317659493712920576 0x^5$ $-20755082902892852710 4x^4 - 52613578344068152787 5x^3$ $+66890048163232670233 6x^2 - 32510469759063162880 0x$ $+27846466248235810816$	$2^{28} \cdot 3^2 \cdot 19^4 \cdot 109^2$	$2^{28} \cdot 53^2 \cdot 59^2 \cdot 103$
-19	-139	$3i + 3j - k$	$3i + 7j - 9k$	$27846466248235810816x^6 - 47825602354653429760x^5$ $+47359177666285816320x^4 - 132261177144435337795x^3$ $+109190282930744023552x^2 - 34661929157414092800x$ $+3740673368395874304$	$2^{28} \cdot 53^2 \cdot 59^2 \cdot 103$	$2^{28} \cdot 3^2 \cdot 19^4 \cdot 109^2$

Table 8: Results for the pair $N = 6$, $p = 3$ with D_1 and D_2 of class numbers 1 and 3.

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $p=5$, $M=400$, $h(D_1)=1$, $h(D_2)=3$						
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	a_n	a_0
-3	-83	$i+j-k$	$i+j-9k$	$8000000x^6 + 87689228x^5 + 98048780x^4$ $+1226958115x^3 - 405690430x^2 + 36134400x + 32768$	$2^9 \cdot 5^6$	2^{15}
-3	-83	$i+j-k$	$3i+5j-7k$	$8000000x^6 - 27544000x^5 + 4920898x^4$ $-56968587x^3 + 4933248x^2 + 610048x + 32768$	$2^9 \cdot 5^6$	2^{15}
-3	-107	$i+j-k$	$i+5j+9k$	$512000000x^6 - 6857888000x^5 + 1663526528x^4$ $-966944227x^3 + 122681138x^2 - 5048832x + 32768$	$2^{15} \cdot 5^6$	2^{15}
-3	-107	$i+j-k$	$3i+7j-7k$	$512000000x^6 - 19008101888x^5 + 260093249970x^4$ $-1369977644475x^3 - 20457333140x^2 - 78218860x + 32768$	$2^{15} \cdot 5^6$	2^{15}

Table 9: Results for the pair $N = 10$, $p = 5$, with D_1 and D_2 of class number 1 and 3.

$B = \left(\frac{-2,-5}{\mathbb{Q}}\right)$, $p=2$, $M=400$, $h(D_1)=1$, $h(D_2)=3$						
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	a_n	a_0
-3	-83	$\frac{1}{2}i - \frac{1}{2}k$	$\frac{1}{2}i + 2j - \frac{1}{2}k$	$15625000000x^6 + 60242691875x^5 + 91343260675x^4$ $+70619968993x^3 + 31052796025x^2 + 7304880000x + 64000000$	$2^6 \cdot 5^{12}$	$2^{12} \cdot 5^6$
-3	-83	$\frac{1}{2}i - \frac{1}{2}k$	$\frac{9}{2}i + 2j + \frac{3}{2}k$	$1000000x^6 - 24430625x^5 + 200812125x^4$ $-652527162x^3 + 1022500850x^2 - 794453125x + 244140625$	$2^6 \cdot 5^6$	5^{12}
-3	-107	$\frac{1}{2}i - \frac{1}{2}k$	$\frac{7}{2}i - 4j + \frac{1}{2}k$	$64000000x^6 + 10564976875x^5 - 185491592725x^4$ $+658571721273x^3 + 2893058101425x^2 + 3039135920000x + 1000000000000$	$2^{12} \cdot 5^6$	$2^{12} \cdot 5^{12}$
-3	-107	$\frac{1}{2}i - \frac{1}{2}k$	$\frac{7}{2}i + 2j + \frac{5}{2}k$	$1000000x^6 + 13560000x^5 - 121353125x^4$ $-1370626807x^3 + 2493941725x^2 - 17822890625x + 15625000000$	$2^6 \cdot 5^6$	$2^6 \cdot 5^{12}$

Table 10: Results for the pair $N = 10$, $p = 2$ with D_1 and D_2 of class number 1 and 3.

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $p = 5$, $M = 400$, $h(D_1) = 1$, $h(D_2) = 5$						
D_1	D_2	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	a_n	a_0
-3	-227	$i + j - k$	$5i + 9j + 11k$	$12958758682492928x^{10} - 1444081532225454 08x^9$ $-19888304037183308 80x^8 - 3286376744306760960x^7$ $+5971107636278988 9570x^6 - 1352691695216767926 43x^5$ $-9247003381324375732x^4 - 1008445398321967500x^3$ $-2396325805200000 0x^2 - 343989000000000 0x$ $+32000000000000$	$2^{29} \cdot 17^6$	$2^{17} \cdot 5^{12}$
-3	-227	$i + j - k$	$i + j + 15k$	$12958758682492928x^{10} - 646020893010755584x^9$ $+1223178496482285 6704x^8 - 8891949080134289 2428x^7$ $+70193346426476252060x^6 - 99347332285733017 3443x^5$ $+50693441356350097 5094x^4 - 213918311762720848644x^3$ $-18945017122067231 2x^2 - 1455144099200000 0x$ $+32000000000000$	$2^{29} \cdot 17^6$	$2^{17} \cdot 5^{12}$
-3	-227	$i + j - k$	$3i + 7j - 13k$	$12958758682492928x^{10} + 165598265700515 84x^9$ $+517712357413060608x^8 - 3443498619887489280x^7$ $+4460885188982986880x^6 - 2803972112177973163x^5$ $-2803972112177973163x^5 + 1023573447688487266x^4$ $+25030309697920000x^2 - 1418389504000000x$ $+32000000000000$	$2^{29} \cdot 17^6$	$2^{17} \cdot 5^{12}$

Table 11: Results for the pair $N = 10$, $p = 5$ with D_1 and D_2 of class number 1 and 5

$B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, $p=5$, $M=400$, $h(D_1)=1$, $h(D_2)=1$							
D_1	D_2	$h(D_1)$	$h(D_2)$	$\phi(\sqrt{D_1})$	$\phi(\sqrt{D_2})$	$f = a_d x^d + .. + a_1 x + a_0$	$a_n = a_0$
-3	-43	1	1	$i+j-k$	$3i+3j-5k$	$256x^2 - 1422737x + 256$	2^8
-3	-67	1	1	$i+j-k$	$3i+3j-7k$	$4000000x^2 - 142822961x + 4000000$	$2^8 \cdot 5^6$
-3	-163	1	1	$i+j-k$	$i+9j-9k$	$453519616000000x^2 + 45363419412546679361x$ $+453519616000000$	$2^{14} \cdot 5^6 \cdot 11^6$
3	-83	1	3	$i+j-k$	$i+j-9k$	$262144000000x^6 + 3247564950011904x^5$ $-45539487902717184x^4 + 160269973118726744 9x^3$ $-45539487902717184x^2 + 3247564950011904x$ $+262144000000$	$2^{24} \cdot 5^6$
-3	-83	1	3	$i+j-k$	$3i+5j-7k$	$262144000000x^6 + 1432363008000x^5$ $-14380699489536x^4 - 3251311475160953x^3$ $-14380699489536x^2 + 1432363008000x$ $+262144000000$	$2^{24} \cdot 5^6$
-3	-107	1	3	$i+j-k$	$i+5j+9k$	$16777216000000x^6 - 27943786512384000x^5$ $+121801116623426304x^4 - 705115548724245833x^3$ $+121801116623426304x^2 - 27943786512384000x$ $+16777216000000$	$2^{30} \cdot 5^6$
-3	-107	1	3	$i+j-k$	$3i+7j-7k$	$16777216000000x^6 - 648092010307190784x^5$ $-1415626487864538392064x^4 - 1887482728251722883609929x^3$ $-1415626487864538392064x^2 - 648092010307190784x$ $+16777216000000$	$2^{30} \cdot 5^6$

Table 12: Results for the pair $N=10$, $p=5$ considering both even and odd indices.

7 Comparison to Errthum's work

7.1 Errthum's work

In this section we aim to compare our results with what has already been computed by Errthum. In [6], Errthum computes singular moduli on Shimura curves using Borcherd's lifts. With notations as in the first sections, and denoting by $N_{B^*}(R)$ the normaliser in B^* of the maximal order R, define $\Gamma^* = \iota(N_{B^*}(R))/\langle \pm 1 \rangle \subseteq PSL_2(\mathbb{R})$. Errthum then considers the Shimura curves

$$X_N^* = \Gamma^* \backslash \mathcal{H},$$

that relate to this paper's curve X_N as follows:

$$X_N^* = X_N / \mathcal{W},$$

where $\mathcal{W}$ is the Atkin Lehner group mentioned in section 2.
For $N = 6$ and 10, Errthum computes a generator $t_N : X_N^* \to \mathcal{P}^1$ of the function field of X_N^*. In particular his method allows him to compute the *norm* of the value of t_6 at CM points of arbitrary large discriminants and the explicit value of t_6 at the *rational* CM points of X_D^*. In particular, since CM points of discriminant of class number 1 are rational, we may compare our results with his tables for those points.

7.2 Case of $N = 6$

This section considers the case $N = 6$ and follows [1]. Consider $\mathcal{W} = \{1, w_2, w_3, w_6\}$ the Atkin-Lehner group of involutions on X_6.

Set for $i = 2, 3$ or 6, $X^{(i)} = X/\langle w_i \rangle$. As mentioned, $X_6^* \cong X_6/\mathcal{W}$ so $X_6 \to X_6^*$ is a map of degree four and we have reduction maps:

$$\begin{array}{ccccc} & & X_6 & & \\ & \swarrow & \downarrow & \searrow & \\ X^{(2)} = X_6/\langle w_2 \rangle & & X^{(3)} = X_6/\langle w_3 \rangle & & X^{(6)} = X_6/\langle w_6 \rangle. \\ & \searrow & \downarrow & \swarrow & \\ & & X_6^* = X_6/\mathcal{W} & & \end{array}$$

The maps $X_6 \to X^{(i)}$ are ramified at the fixed points of w_i where $i \in \{2, 3, 6\}$, denote these points y_2, y_3, y_6 respectively. Errthum (page 486) calls these points $y_2 = P_4$, $y_3 = P_6$ and $y_6 = P_2$ and one has that :

$$y_2 \in \mathrm{CM}(\mathbb{Z}[\sqrt{-1}]), \quad y_3 \in \mathrm{CM}(\mathbb{Z}[\tfrac{1+\sqrt{-3}}{2}]), \quad y_6 \in \mathrm{CM}(\mathbb{Z}[\sqrt{-6}]).$$

The function $t_6 : X_6^* \to \mathbb{P}^1(\mathbb{C})$ constructed by Errthum satisfies:

$$\begin{cases} t_6(y_2) = 0, \\ t_6(y_3) = \infty, \\ t_6(y_6) = 1. \end{cases}$$

From this function, we first construct uniformisers $j^{(i)} : X^{(i)} \to \mathbb{P}^1(\mathbb{C})$ for $i = 2, 3, 6$. Considering the degree of the maps and the ramified points, we may set:

$$j^{(2)}(z)^2 = c_2 \cdot (t_6(z) - 1), \quad j^{(3)}(z)^2 = c_3 \frac{t_6(z)}{t_6(z) - 1}, \quad j^{(6)}(z)^2 = c_6 \cdot t_6(z)$$

for some constant c_2, c_3, c_6. Observe that we may take $j^{(6)} = j^{(2)} \cdot j^{(3)}$ and hence set

$$c_6 = c_2 \cdot c_3.$$

The following hold:

$$c_6 j^{(2)}(z)^2 - c_2 j^{(6)}(z)^2 + c_2 c_6 = 0; \tag{10}$$

$$j^{(i)} \circ w_i = j^{(i)} \quad \text{for } i = 2, 3, 6; \tag{11}$$

$$j^{(i)} \circ w_k = -j^{(i)} \quad \text{for } i, k = 2, 3, 6 \text{ and } i \neq k; \tag{12}$$

$$j^{(2)}(y_2) = \pm\sqrt{-c_2},\ j^{(2)}(y_3) = \infty,\ j^{(2)}(y_6) = 0; \tag{13}$$

$$j^{(3)}(y_2) = 0,\ j^{(3)}(y_3) = \pm\sqrt{c_3},\ j^{(3)}(y_6) = \infty; \tag{14}$$

$$j^{(6)}(y_2) = 0,\ j^{(6)}(y_3) = \infty,\ j^{(6)}(y_6) = \pm\sqrt{c_6}. \tag{15}$$

Since $y_2 \in \mathrm{CM}(\mathbb{Z}([\sqrt{-1}])$, then $j^{(i)}(y_2) \in H_{-1} = \mathbb{Q}(\sqrt{-1})$ for all $i = 2, 3, 6$. Similarly, since $y_3 \in \mathrm{CM}(\mathbb{Z}([\frac{1+\sqrt{-3}}{2}])$, then $j^{(i)}(y_3) \in H_{-3} = \mathbb{Q}(\sqrt{-3})$ for all $i = 2, 3, 6$.
This means $\sqrt{-c_2} \in \mathbb{Q}(\sqrt{-1})$ and $\sqrt{c_3} \in \mathbb{Q}(\sqrt{-3})$, so we may choose:

$$c_2 = 1, \quad c_3 = -3, \quad c_6 = c_2 c_3 = -3.$$

Hence

$$3j^{(2)}(z)^2 + j^{(6)}(z)^2 + 3 = 0$$

It is known that the Shimura curve X_6 admits a model $\phi : \mathcal{H} \to \mathbb{P}^2(\mathbb{C})$, with coordinate functions

$$\tau \mapsto (u_1(\tau) : \ u_2(\tau) : 1),$$

that satisfy

$$u_1^2 + u_2^2 + 3 = 0. \tag{16}$$

Letting

$$u_1 = \frac{3}{j^{(3)}}, \quad u_2 = \frac{3}{j^{(6)}},$$

we verify that equation (16) holds.

Finally, set:

$$j_6 = \frac{iu_1 - u_2}{\sqrt{3}} = i\frac{\sqrt{3}}{j^{(3)}} - \frac{\sqrt{3}}{j^{(6)}}.$$

Using properties (11) and (12), we have the following:

$$\begin{aligned} j_6 \circ w_2 &= -j_6, \\ j_6 \circ w_3 &= \tfrac{1}{j_6}, \\ j_6 \circ w_6 &= -\tfrac{1}{j_6}. \end{aligned}$$

These properties allow us to rewrite the J-quantity as follows:

$$J_6^{(3)}(\tau_1, \tau_2) = \frac{(j_6(\tau_2) - j_6(\tau_1))^2}{(j_6(\tau_2) + j_6(\tau_1))^2},$$
$$J_6^{(2)}(\tau_1, \tau_2) = \frac{(j_6(\tau_2) - j_6(\tau_1))^2}{(j_6(\tau_2) \cdot j_6(\tau_1) - 1)^2}.$$

We have computed the above *complex* quantities for all discriminants for which Errthum computes an explicit value of t_6. For example, consider the smallest class numbers of discriminant 1, $D_1 = -19$, $D_2 = -43$. Errthum computes

$$t_6(\tau_1) = -\frac{3^7}{2^{10}}, \quad t_6(\tau_2) = -\frac{3^7 7^4}{2^{10} 5^6}.$$

For $i = 1, 2$ let

$$j^{(3)}(\tau_i) = \sqrt{-3t_6(\tau_i)}, \quad j^{(6)}(\tau_i) = \sqrt{-3\frac{t_6(\tau_i)}{t_6(\tau_i) - 1}}.$$

From these we compute

$$j_6(\tau_i) = i\frac{\sqrt{3}}{j^{(3)}(\tau_i)} - \frac{\sqrt{3}}{j^{(6)}(\tau_i)}.$$

Then again using PARI's `algdep` function, up to 300 digits of real precision, the complex number $\frac{(j_6(\tau_2) - j_6(\tau_1))^2}{(j_6(\tau_2) + j_6(\tau_1))^2} = J_6^{(3)}(\tau_1, \tau_2)$ satisfies the quadratic polynomial

$$7750655x^2 - 14480299x + 1478656,$$

which is exactly the one found in table 3. Similarly $\frac{(j_6(\tau_2) - j_6(\tau_1))^2}{(j_6(\tau_2) j_6(\tau_1) - 1)^2} = J_6^{(2)}(\tau_1, \tau_2)$ satisfies the quadratic polynomial

$$1653403x^2 - 35711431x + 3158020$$

of table 4. For all other pairs of discriminants of class number one the results obtained are algebraic numbers that satisfy exactly the same polynomials as those in the tables 3 and 4.

References

[1] P. Bayer and A. Travesa. Uniformizing functions for certain Shimura curves, in the case D=6. *Acta Arithmetica*, 126(4):315–339, 2007.

[2] M. Bertolini and H. Darmon. *Heegner points on Mumford?Tate curves*, volume 126. 1996.

[3] H. Darmon and J. Vonk. Arithmetic intersections of modular geodesics. *Journal of Number Theory*, 2021.

[4] H. Darmon and J. Vonk. Singular moduli for real quadratic fields: a rigid analytic approach. *Duke Mathematical Journal*, 170(1):23 – 93, 2021.

[5] N. D. Elkies. *Shimura curve computations*, volume 1423 of *Lecture Notes in Computer Science*, chapter Algorithmic Number Theory, pages 1–47. Springer, Berlin, Heidelberg, 1998.

[6] E. Errthum. Singular moduli of Shimura curves. *Canad. J. Math.*, 63(4):826–861, 2011.

[7] L. Gerritzen and M. van der Put. *Schottky groups and Mumford curves*, volume 817 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[8] B.H. Gross and D.B. Zagier. On singular moduli. *J. Reine Agew. Math.*, 355:191–220, 1985.

[9] X. Guitart, M. Masdeu, and X. Xarles. A quaternionic construction of p-adic singular moduli.

[10] I. Negrini. On the computation of p-adic theta functions arising from the Hurwitz quaternions. Master's thesis, Università degli Studi di Milano, Concordia University, 2017.

[11] J. Rickards. *Intersections of closed geodesics on Shimura curves*. PhD thesis, McGill University, 2020.

[12] M.F. Vigneras. *Arithmétique des algèbres de quaternions*. Number 800 in Lecture Notes in Mathematics. Springer, Berlin, 1980.

Sofia Giampietro
Institute of Mathematics, École Polytechnique Fédérale de Lausanne, Route Cantonale, 1015 Lausanne, Switzerland
E-mail address: `sofia.giampietro@inf.ethz.ch`

Henri Darmon
Department of Mathematics and Statistics, McGill University, Montreal, Canada.
E-mail addres: `henri.darmon@mcgill.ca`

A Code

```
##AUXILIARY FUNCTIONS:

def findT(omax,B,p,Units,Q1):
    T=[]
    Q1copy=deepcopy(Q1)
    for i in range(0,p+1):
        t=Q1copy[0];
        C=[ multquat(t,u,B) for u in Units ]
        for c in C:
            Q1copy.remove(c)
        T.append(t)
    return(T)

def Subpowers(a,m):
    atemp=1
    L=list([atemp])
    for i in range(0,m):
        atemp=atemp*a
        L.append(atemp)
    return(L)

def fastevaluate(f,subpowers,m):
    rrp=f.list()[0].parent()
    F=f.list()
    fi=rrp(0)
    for i in range(0,min(len(F),len(subpowers))):
        fi=fi+(F[i]*subpowers[i])
    return(fi)

def quattomatpadic(u,B,p):
    a=B[0]
    b=B[1]
    if (p!=2 and kronecker(a,p)==1):
        f=R3(y0^2-a)
        A=f.roots()[1][0]
        return(matrix([[u[0]+u[1]*A , b*(u[2]+u[3]*A)],[u[2]-u[3]*A,
                                                        u[0]-u[1]*A]]))
    else:
        Y=Qp3(6)
        f=R3(y0^2-a*Y^2-b)
        X=f.roots()
        while(len(X)==0):
            Y=Y+1
            f=R3(y0^2-a*Y^2-b)
```

```
            X=f.roots()
        X=X[0][0]
        return(matrix([[u[0]+X*u[2]-a*Y*u[3] , a*u[1]+a*Y*u[2]-a*X*u[3]],
                       [u[1]-Y*u[2]+X*u[3], u[0]-X*u[2]+a*Y*u[3]]]) )


def mobius(M,tau):
    return((M[0,0]*tau+M[0,1])/(M[1,0]*tau+M[1,1]))

def invp(M):
    return(matrix([[M[1,1],-M[0,1]],[-M[1,0],M[0,0]]]))

def redmodp2(q,M,p):
    F3=GF(p)
    a=Zp3(M[0,0])
    b=Zp3(M[0,1])
    c=Zp3(M[1,0])
    m1=Zp3(q[0,0])
    m2=Zp3(q[0,1])
    m3=Zp3(q[1,0])
    m4=Zp3(q[1,1])
    A=m4*m1*a+m2*m4*c-m1*m3*b+m2*m3*a
    B=-m1*m2*a-m2*m2*c+m1*m1*b-m1*m2*a
    C=m3*m4*a+m4*m4*c-m3*m3*b+m4*m3*a
    D=-A
    if( val3(C)==0 ):
        f=RZ3( val3.reduce(Zp3(C))*y^2 - val3.reduce(Zp3(2*A))*y
              -val3.reduce(Zp3(B)))
        if len(f.roots())!=1:
            print("non p-discriminant !")
        return(ZZ(f.roots()[0][0]))
    else:
        return(ZZ(p))

def multquat(a,b,B):
    v1=a[0]*b[0]+B[0]*a[1]*b[1]+B[1]*a[2]*b[2]-B[0]*B[1]*a[3]*b[3]
    v2=a[0]*b[1]+a[1]*b[0]-a[2]*b[3]*B[1]+a[3]*b[2]*B[1]
    v3=a[0]*b[2]+a[2]*b[0]-a[3]*b[1]*B[0]+a[1]*b[3]*B[0]
    v4=a[0]*b[3]+a[1]*b[2]-a[2]*b[1]+a[3]*b[0]
    return(list([v1,v2,v3,v4]))


##USER GIVEN INFORMATION - TO BE MODIFIED
B=[-1,-1]
omax=matrix([[1, 0, 1/2, 0], [0, 1, 0, 1/2], [0, 0, 1/2, 0],[0, 0, 0, 1/2]])
p=2
```

```
mprec=300

D1=43
D2=163

M1emb=[0,3,3,-5]
M2emb=[0,9,9,-1]

data=open("/Users/Sofia/Documents/MCGILL/dataHamilton.txt", "r")
units= eval(data.readline())
Q1= eval(data.readline())
data.close()

##DEFINE OBJECTS AND CONSTANTS NEEDED

Qp3=Qp(p,mprec)
R3.<y0> = PolynomialRing(Qp3,'y0')
Zp3=Qp3.integer_ring()
RZ3.<y> = PolynomialRing(GF(p),'y')
val3=Zp3.valuation()

M1=quattomatpadic(M1emb,B,p)
print(M1.determinant())
M2=quattomatpadic(M2emb,B,p)
print(M2.determinant())

f=R3(M1[1,0]*(y0**2)-(M1[0,0]-M1[1,1])*y0-M1[0,1])
Kp.<t>=Qp3.ext(f)
Pol.<s>=PolynomialRing(Kp,'s')
f=Pol(M1[1,0]*(s**2)-(M1[0,0]-M1[1,1])*s-M1[0,1])
tau2=f.roots()[0][0]
tau1=f.roots()[1][0]

Rp.<x>=PowerSeriesRing(Kp,'x',mprec)

f=Pol(M2[1,0]*(s**2)-(M2[0,0]-M2[1,1])*s-M2[0,1])
zet2=f.roots()[0][0]
zet1=f.roots()[1][0]

zetapows=[]
zetapows2=[]
for i in range(0,p):
    zetapows.append(Subpowers(1/(zet1-i),mprec+1))
    zetapows2.append(Subpowers(1/(zet2-i),mprec+1))
zetapows.append(Subpowers(zet1,mprec+1))
zetapows2.append(Subpowers(zet2,mprec+1))
```

```
T= findT(omax,B,p,units,Q1)
Tmat=[ quattomatpadic(t,B,p) for t in T]
Tmatinv=[ invp(t) for t in Tmat ]
unitmat=[ quattomatpadic(u,B,p) for u in units]
Q1mat=[quattomatpadic(q,B,p) for q in Q1]

Q1js=[]
for i in range(0,p+1):
    Q1js.append(list())
for q in Q1mat:
    a=redmodp2(q,M1,p)
    Q1js[a].append(q)
print([len(Q1js[j]) for j in range(0,p+1)])




##COMPUTE SET OF BAD INDICES GIVING NON PRIMITIVE QUATERNIONS

badij=[]
for i in range(0,p+1):
    Tm=Tmat[i]
    t1=Zp3(Tm[0,0])
    t2=Zp3(Tm[0,1])
    t3=Zp3(Tm[1,0])
    t4=Zp3(Tm[1,1])
    if val3(t3)==0:
        badij.append(ZZ(-val3.reduce(t4)/val3.reduce(t3)))
    else:
        if val3(t4) == 0:
            badij.append(ZZ(p))
        else:
            if val3(t1)==0:
                badij.append( ZZ(-val3.reduce(t2)/val3.reduce(t1)))
            else:
                if val3(t2)==0:
                    badij.append(ZZ(p))


##COMPUTE INDICES Tij

Tij=[]
for i in range(0,p+1):
    a=Zp3(Tmat[i][0,0])
```

```
    b=Zp3(Tmat[i][0,1])
    c=Zp3(Tmat[i][1,0])
    d=Zp3(Tmat[i][1,1])
    if val3(c)==0:
        Tij.append(ZZ(val3.reduce(a)/val3.reduce(c)))
    else:
        if val3(a)==0:
            Tij.append(ZZ(p))
        else:
            if val3(d)==0:
                Tij.append(ZZ(val3.reduce(b)/val3.reduce(d)))
            else:
                if val3(b)==0:
                    Tij.append(ZZ(p))


##COMPUTE LEVEL 1 FUNCTION

##Finite part:
Fjs=list()
Fjs2=list()
for j in range(0,p):
    Fj=Rp(1)
    Fj2=Rp(1)
    for q in Q1js[j]:
        r1=mobius(q,tau1)
        r2=mobius(q,tau2)
        Fj=Fj*((1+x*(j-r1))/(1+x*(j-r2)))
        Fj2=Fj2*((1+x*(j-r2))/(1+x*(j-r1)))
    Fjs.append(Fj)
    Fjs2.append(Fj2)

##Infinite part:
Fj=Rp(1)
Fj2=Rp(1)
for q in Q1js[p]:
    r1=(mobius(q,tau1))
    r2=(mobius(q,tau2))
    Fj=Fj*((1/x-1/r1)/(1/x-1/r2))
    Fj2=Fj2*((1/x-1/r2)/(1/x-1/r1))
Fjs.append(Fj)
Fjs2.append(Fj2)


##COMPUTE ALL SUBSTITUTIONS NEEDED FOR RECURSION:
```

```
Tsubs=[]
for a in range(0,p+1):
    i=Tij.index(a)
    Xi=[]
    t1=Tmatinv[i][0,0]
    t2=Tmatinv[i][0,1]
    t3=Tmatinv[i][1,0]
    t4=Tmatinv[i][1,1]
    for j in range(0,p+1):
        if j!= badij[i]:
            if (a==p):
                if (j==p):
                    Xi.append((t1*x+t2)/(t3*x+t4))
                if (j!=p):
                    Xi.append((t3*x+t4)/(t1*x+t2-j*(t3*x+t4) ))
            if (a!=p):
                if (j==p):
                    Xi.append((t1+x*(a*t1+t2))/(t3+x*(a*t3+t4)))
                if (j!=p):
                    Xi.append((t3+x*(t3*a+t4))/ (t1+x*(t1*a+t2)-
                                        j*(t3+x*(t3*a+t4))))
        if j==badij[i]:
            Xi.append(0)
    Tsubs.append(Xi)

Tsubpowers=[]
for a in range(0,p+1):
    Tsa=[]
    for j in range(0,p+1):
        if(Tsubs[a][j]!=0):
            Tsa.append(Subpowers(Tsubs[a][j],mprec))
        else:
            Tsa.append(0)
    Tsubpowers.append(Tsa)



Phi=[0,Fjs]
Phi2=[0,Fjs2]

Fprev=Phi[1]
Fprev2=Phi2[1]

##COMPUTE ALL LEVELS RECURSIVELY
```

```
for n in range(2,mprec):
    QN=[]
    QN2=[]
##recursion :
    for a in range(0,p+1):
        Fa=Rp(1)
        Fa2=Rp(1)
        for j in range(0,p+1):
            if (Tsubpowers[a][j]!=0):
                Fa=Fa*(fastevaluate(Fprev[j], Tsubpowers[a][j], mprec ))
                Fa2=Fa2*(fastevaluate(Fprev2[j], Tsubpowers[a][j],mprec))
        Fa=Fa/(Fa.list()[0])
        Fa2=Fa2/(Fa2.list()[0])
        QN.append(Fa)
        QN2.append(Fa2)
    Fprev=QN
    Fprev2=QN2
    Phi.append(QN)
    Phi2.append(QN2)



##compute level 0 product:
phi2=prod([(zet1-mobius(u,tau1))/(zet1-mobius(u,tau2)) for u in unitmat])
phi22=prod([(zet2-mobius(u,tau2))/(zet2-mobius(u,tau1)) for u in unitmat])
result=phi2*phi22

##multiply everything together:
for i in range(1,len(Phi)-1):
    if (i%2==0):
        for j in range(0,p+1):
            result=result*fastevaluate(Phi[i][j],zetapows[j],mprec)*
                    fastevaluate(Phi2[i][j],zetapows2[j],mprec)


JD1D2=(sqrt(result))
```