Journal of Number Theory 131 (2011) 195–211

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The effect of torsion on the distribution of Ш among quadratic twists of an elliptic curve

Patricia L. Quattrini

Departamento de matemática, FCEyN, Universidad de Buenos Aires, Int. Guiraldes 2160, 1428 Buenos Aires, Argentina

ARTICLE INFO

Article history:
Received 7 August 2009
Revised 5 July 2010
Accepted 7 July 2010
Available online 9 October 2010
Communicated by J. Brian Conrey

Keywords:
Distribution of Ш
Congruences of modular forms
Torsion points of elliptic curves

ABSTRACT

Let E be an elliptic curve of rank zero defined over $\mathbb{Q}$ and ℓ an odd prime number. For E of prime conductor N, in Quattrini (2006) [Qua06], we remarked that when $\ell \mid |E(\mathbb{Q})_{\mathrm{Tor}}|$, there is a congruence modulo ℓ among a modular form of weight 3/2 corresponding to E and an Eisenstein series. In this work we relate this congruence in weight 3/2, to a well-known one occurring in weight 2, which arises when $E(\mathbb{Q})$ has an ℓ torsion point. For N prime, we prove that this last congruence can be lifted to one involving eigenvectors of Brandt matrices $B_p(N)$ in the quaternion algebra ramified at N and infinity. From this follows the congruence in weight 3/2. For N square free we conjecture on the coefficients of a weight 3/2 Cohen–Eisenstein series of level N, which we expect to be congruent to the weight 3/2 modular form corresponding to E.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor N and analytic rank zero. For $-d$ a fundamental discriminant, $d > 0$, consider the $-d$ quadratic twist of E. We will denote it by E_d and $|Ш_d|$ will denote the analytic order of its Tate–Shafarevich group as predicted from the Birch and Swinnerton-Dyer conjecture, including the value 0 if the elliptic curve has analytic rank greater than zero.

Let ℓ be an odd prime number, dividing the order of the group of torsion points of the elliptic curve E, thus ℓ will be 3, 5 or 7.

In [Qua06] we described a series of numerical examples on the distribution of the analytic orders of the Tate–Shafarevich groups associated to imaginary quadratic twists of a fixed elliptic curve of

E-mail address: pquattri@dm.uba.ar.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.07.007

prime conductor N. We observed that when E has a rational ℓ-torsion point, then, among its negative quadratic twists there is a bigger proportion of them which have the analytic order of Ш divisible by ℓ. That something different occurred in this situation had been already noticed in [CKRS], though not giving an explanation for this phenomena.

It is worth pointing out that something similar occurs with number fields. In [Mal08] G. Malle gives numerical evidence indicating that the Cohen–Lenstra–Martinet heuristics for class groups of number fields seem not to be applicable to the p-part of the class group when the base field or some intermediate field contains pth roots of unity.

There are several results concerning the ℓ divisibility of the order of Ш among quadratic twists of an elliptic curve having a point of prime order ℓ. In [Won99] Wong proves, using results of Frey [Fre88], that there are infinitely many negative fundamental discriminants $-d$, $d > 0$, such that the $(-d)$-quadratic twist of the elliptic curve $X_0(11)$ has analytic rank zero and $Ш_d$ has an element of order 5. Ono in [Ono01] obtains a more general result, combining ideas of Wong, Frey and himself, for elliptic curves whose torsion subgroup is $\mathbb{Z}/\ell\mathbb{Z}$ and satisfy several technical conditions at ℓ. James in [Jam99] also has results on the 3 divisibility of the order of Ш among negative quadratic twists of an elliptic curve with a point of order 3, and relates this to the divisibility by 3 of class numbers of negative quadratic fields. These works are based on results of Frey regarding the Selmer groups of quadratic twists of elliptic curves having a rational point of odd prime order.

In this work we focus on congruences among modular forms that occur when the elliptic curve E has a rational point of odd prime order ℓ.

We showed in [Qua06] that, in the three strong Weil elliptic curves of prime conductor with a torsion point of odd prime order ℓ, there is a congruence, modulo ℓ, among modular forms of weight 3/2. One of these forms is associated to central values of L-series corresponding to the twists of E, and the other one is an Eisenstein series whose coefficients are known to be related to class numbers of imaginary quadratic fields.

These are the elliptic curves $11A1$, $19A1$ and $37B1$, following Cremona's tables [Cre97]. The first one has a 5-torsion point, and the other two, a point of order 3. We will denote by f_N the newform associated to the elliptic curve of conductor N, and by g_N the weight 3/2 newform under Shimura correspondence to f_N, lying in Kohnen subspace, as constructed in [Gro87]. By $\mathcal{H}_{\mathbf{N}}$ we will mean the Eisenstein series of weight 3/2 and level $4N$.

We have the following congruences:

$$g_{\mathbf{11}} \equiv 3\mathcal{H}_{\mathbf{11}}(5); \qquad g_{\mathbf{19}} \equiv \mathcal{H}_{\mathbf{19}}(3); \qquad g_{\mathbf{37}} \equiv \mathcal{H}_{\mathbf{37}}(3)$$

where, in each case, the modulus ℓ of the congruence is an odd prime dividing the order of the group of torsion points of the strong Weil curve of conductor N.

From a congruence as above we have that the proportion of Ш values divisible by ℓ in the family of imaginary quadratic twists of E, with $(\frac{-d}{N}) \neq 1$, is the same as the proportion of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ divisible by ℓ, with $(\frac{-d}{N}) \neq 1$.

Further, if we assume the Cohen–Lenstra heuristics on the probability of class numbers being divisible by a prime, and assume that this probability is valid when restricted to discriminants $-d$ with $(\frac{-d}{N}) \neq 1$, then this proportion is equal to

$$P(\ell) = 1 - \prod_{i \geqslant 0} \left(1 - \frac{1}{\ell^i}\right) = \frac{1}{\ell} + \frac{1}{\ell^2} - \frac{1}{\ell^3} - \frac{1}{\ell^7} \cdots.$$

The goal of this work is to analyze the situation for square-free conductors and prove, when possible, that the before mentioned congruence of modular forms in weight 3/2 comes from a well-known congruence arising in weight 2, under the presence of an ℓ-torsion point.

For elliptic curves E of prime conductor N, it is a known fact that when E has a point of prime order ℓ, the weight 2 newform f attached to E is congruent modulo ℓ to the normalized Eisenstein series e_2 in $M_2(N)$. By this we mean that the coefficients, and thus the eigenvalues of the Hecke operators acting on $M_2(N)$, are equivalent modulo the prime ℓ.

The existing congruence in weight 3/2, among a newform g under Shimura correspondence to f, and an Eisenstein series $\mathcal{H}_{3/2}$ corresponding to e_2, should be a reflection of the situation occurring in weight 2.

The procedure used for constructing the modular form g, corresponding to f and involved in Waldspurger formula (see [Wal81]), uses Brandt matrices in certain quaternion algebra. It is a well-known fact (see, for example, [Piz80]) that to an order $\mathcal{O}$ of level N, in a definite quaternion algebra $\mathcal{B}$ defined over $\mathbb{Q}$ and ramified at some specific primes, one can attach certain theta series which turn out to be modular forms of weight 2 and level N. Each newform of level N is represented in this space of theta series. The Brandt matrices of level N and prime degree p, $\{B_p\}$, act on this space as the Hecke operators $\{T_p\}$ act on $M_2(N)$ and, to a newform $f = \sum a_n q^n$, corresponds a dimension one eigenspace of the Brandt matrices in the following way: if $T_p f = a_p f$, then there is a dimension one eigenspace $\langle v\rangle$, $v \in \mathbb{Q}^\kappa$ such that $B_p v^t = a_p v^t$, for every prime p. Here κ is the number of left-ideal classes for $\mathcal{O}$ and the Brandt matrices lie in $\mathbb{Q}^{\kappa\times\kappa}$.

Suppose we have in $M_2(N)$ a congruence $f \equiv e_2 \bmod \ell$ among a normalized modular form f and a normalized Eisenstein series e_2. Then f and e_2 are represented in some quaternion algebra $\mathcal{B}$ and to each of them corresponds a one-dimensional eigenspace of the Brandt matrices B_p whose eigenvalues are equivalent modulo the prime ℓ.

If we can assert that the reduced Brandt matrices $\{B_p\}$ modulo ℓ have a one-dimensional eigenspace associated to the eigenvalues $\{a_p\}$ then, by construction, the modular form g of weight 3/2 that corresponds to f, and whose coefficients are related to the central values of the L-series of the twists of E, is congruent modulo ℓ to a scalar multiple in $\mathbb{F}_\ell^\times$ of the Cohen–Eisenstein series $\mathcal{H}_{3/2}$ of level N, associated to e_2. This happens, at least, for N prime. Our interest in this concerns the orders of Ш-groups of twists of elliptic curves. Assuming the Birch and Swinnerton-Dyer conjecture, we have that the square of the d-coefficient of the modular form g is, essentially, the order of Ш_d divided by a power of 2. The congruence above permits us to assert that $|\text{Ш}_d|$ is divisible by the prime ℓ if, and only if, the class number of $\mathbb{Q}(\sqrt{-d})$ is divisible by ℓ.

For composite levels, the situation is more difficult, as the space of Eisenstein series is no longer one-dimensional. However, the situation should be as in the prime case. For square-free level N, the newform f is congruent modulo ℓ to a specific weight 2 Eisenstein series, when E has an ℓ torsion point. This should be reflected in a congruence in weight 3/2. Though we cannot prove a congruence among eigenvectors of Brandt matrices, we give numerical examples in Section 3.7 and conjecture on the coefficients of the weight 3/2 Cohen–Eisenstein series that corresponds to the weight 2 Eisenstein series just mentioned.

2. General construction

In this section we give an outline of the general constructions we need. The results are known but for the sake of self-containness we include a summary.

E will be an elliptic curve of analytic rank zero and square-free conductor N. The sign of the functional equation for the L-series of E must be $+1$ or, equivalently, the sign of the Atkin–Lehner W_N is -1. As the sign of W_N equals the product of the signs of the Atkin–Lehner at each prime $p \mid N$, we have that there is an odd number of primes $p \mid N$ for which $W_p = -1$.

Along this section we will write $N = DM$, where D is the product of those primes $p \mid N$ such that the Atkin–Lehner involution W_p acting on f_N has sign -1, while M is the product of those acting on f_N with sign $+1$.

We will work in the quaternion algebra $\mathcal{B}$ ramified exactly at those finite primes $p \mid D$. Note that, as this number of primes is odd, $\mathcal{B}$ is also ramified at infinity and the norm form in $\mathcal{B}$ is positive definite.

We consider the family of negative quadratic twists E_d of E, for those $d > 0$ such that $-d$ is a fundamental discriminant and $(\frac{-d}{p})\operatorname{sgn} W_p \neq -1$ for every $p \mid N$. Let $f_N = \sum a_n q^n$ be the weight 2 and level N modular form associated to E, then $f_N \otimes \epsilon_{-d}$ is the modular form associated to the $-d$ twist of E.

2.1. How to construct weight 3/2 modular forms.

In [Gro87] B. Gross states a special case of the Waldspurger's [Wal81] formula concerning the twists of a modular form f of weight 2 and conductor N prime. This formula relates the product $L(f,1)L(f\otimes\epsilon_{-d},1)$ to the squared d-coefficient of a weight 3/2 modular form g, under Shimura correspondence to f. This relation together with the Birch and Swinnerton-Dyer conjecture give us the order of Ш_d as the square of the d-coefficient of a modular form times a rational square. For examples calculated with N prime, this rational square was a power of 2. We will come back on this later.

Given f_N of weight 2 and prime level N, in [Gro87] we have an explicit procedure for constructing the modular form g_N of weight 3/2 involved in the Waldspurger formula.

In [BS90], Bocherer and Schulze-Pillot generalized Gross' construction for square-free level N. We give a very brief outline here which goes, roughly, as in the prime case.

Consider a definite quaternion algebra $\mathcal{B}$ ramified at some set of primes $\{p_1,\dots,p_r\}$ and split at all other primes. Put $D=p_1\cdots p_r$ and let $N=DM$ be any square-free integer.

Take an order $\mathcal{O}$ of level N, $I_1,\dots,I_\kappa$ representatives of left-ideal classes for $\mathcal{O}$, and $R_1,\dots,R_\kappa$ the respective right orders (of level N) of each ideal I_i.

For each R_i take the rank-three lattice $L_i=\mathbb{Z}+2R_i$ and S_i^0 the elements of trace zero in L_i. Define g_i to be the theta series

$$g_i=\frac{1}{2}\sum_{b\in S_i^0}q^{\mathbb{N}(b)}$$

where $\mathbb{N}$ is the norm form and $q=e^{2\pi i\tau}$.

The forms g_i are in the *Kohnen* subspace $M^{3/2}(N)$ which are those modular forms of weight 3/2 on $\Gamma_0(4N)$ whose Fourier coefficient a_n is zero unless $-n\equiv 0,1 \bmod 4$.

Let w_i be the number of units in $R_i^\times/\{\pm1\}$.

To each modular form f_N in $M_2(N)$, with coefficients in $\mathbb{Z}$, which is a newform and thus an eigenfunction for all Hecke operators, with $T_pf=a_pf$ corresponds a one-dimensional eigenspace $\langle v=(v_1,\dots,v_\kappa)\rangle$, of the Brandt matrices $\{B_p\}$ in $\mathcal{B}$ corresponding to $\mathcal{O}$, such that

$$B_pv^t=a_pv^t.$$

This last equality valid, in principle, for $p\nmid N$, is also true for every p, as we will see in Section 3.3.

We can always take v with integer and relatively prime coordinates.

Then

$$g_N=\sum_{i=1}^{\kappa}\frac{v_i}{w_i}g_i$$

is in $M^{3/2}(N)$ and corresponds to f_N under Shimura map.

The form g_N is trivially zero unless we have

$$\operatorname{sgn}W_p=\begin{cases}-1 & \text{for } p\mid D,\\ 1 & \text{for } p\mid M\end{cases}$$

where $\operatorname{sgn}W_p$ denotes the sign of W_p acting on f_N (see [BS90] for details).

This *lift* from modular forms of weight 2 to modular forms of weight 3/2 is also valid for Eisenstein series. Thus take

$$\mathcal{H}_N = \sum_{i=1}^{\kappa} \frac{1}{w_i} g_i,$$

this is a weight 3/2 *Eisenstein* series corresponding to the eigenvector $u = (1, \dots, 1)$ (κ ones), and thus to an Eisenstein series of weight 2. If $w = \prod w_i$, then $w\mathcal{H}_N \in M^{3/2}(N)$.

2.2. Waldspurger's formula

A similar special case of Waldspurger's formula to that described in [Gro87] is valid for square-free levels, as shown in [BS90].

Let $f_N \in S_2(N)$ be a normalized newform of square-free level N, with sign $+1$ in the functional equation for $L(f_N, s)$. Let $-d$ be a fundamental discriminant and $f_N \otimes \epsilon_d$ the $(-d)$-quadratic twist of f_N.

Let $g_N = \sum m_d q^d$ be the weight 3/2 modular form corresponding to f_N as constructed above, in the definite quaternion algebra $\mathcal{B}$ ramified at those primes $p \mid D$, and $v = (v_1, \dots, v_\kappa)$ the eigenvector of the Brandt matrices in $\mathcal{B}$ corresponding to f_N.

We have

$$\prod_{p \mid \frac{N}{\gcd(N,d)}} \left(1 + \left(\frac{-d}{p}\right) \operatorname{sgn} W_p\right) L(f_N, 1) L(f_N \otimes \epsilon_d, 1) = 2^r \frac{(f_N, f_N) m_d^2}{\sqrt{d} \sum \frac{v_i^2}{w_i}} \tag{1}$$

where r is the number of prime divisors of N and (f_N, f_N) is the Petterson inner product.

Note that the left-hand side is zero unless $(\frac{-d}{p}) \operatorname{sgn} W_p \neq -1$ for every prime $p \mid N$.

This means that m_d is zero unless for every $p \mid N$, $(\frac{-d}{p})$ coincides with the sign of W_p, or, it is zero. Thus we will only get a proportion of the twists of f_N by this construction, unless N is prime in which case we get all them.

3. Eisenstein series

We give an Eisenstein series congruent to the weight 2 modular form f corresponding to E, when this last has an ℓ torsion point. Recall we are assuming ℓ is prime and $\ell > 2$.

We know that $M_2(N) = S_2(N) \oplus E_2(N)$, but for non-prime N the space of Eisenstein series is not one-dimensional. Thus, we would like to have:

- An Eisenstein series $e_2 = \sum c_n q^n$ such that for every prime p (and thus for every n), $a_p \equiv c_p \bmod \ell$.
- The eigenvectors of the Brandt matrices corresponding f_N and e_2 to be linearly dependent modulo ℓ.
- The relation among the coefficients of the corresponding weight 3/2 Eisenstein series $\mathcal{H}_N$ and the class numbers of imaginary quadratic number fields.

In this section we focus on the first item and show this Eisenstein series is represented in the quaternion algebra $\mathcal{B}$ ramified at exactly those primes $p \mid N$ for which the Atkin–Lehner involution W_p has sign equal to -1.

3.1. The row sums of Brandt matrices

Here, as before, $\mathcal{B}$ is a definite quaternion algebra ramified at finite primes $p \mid D$, $\mathcal{O}$ an order of level $N = DM$ and B_n the corresponding Brandt matrices.

The *zeta function* of $\mathcal{O}$ is the sum

$$\zeta_{\mathcal{O}} = \sum \frac{1}{\mathbb{N}(I)^{2s}}$$

where the sum extends over all integral $\mathcal{O}$-left ideals I.

Eichler in [Eic72, §6] proves that the row sums of the Brandt matrices B_n equals the n-coefficient of the zeta function of $\mathcal{O}$. That is, if

$$\zeta_{\mathcal{O}} = \sum_{n=1}^{\infty} \frac{b(n)}{n^{2s}}$$

then $b(n)$ is the sum of (any) row in the matrix B_n.

The zeta function can be expressed as an Euler product [Eic72, II §2] with local factor at a prime p given as follows:

$$\begin{aligned}
\zeta_p(s) &= \left(1 - p^{-2s}\right)^{-1}\left(1 - p^{1-2s}\right)^{-1} && \text{for } p \nmid DM,\\
\zeta_p(s) &= \left(1 - p^{-2s}\right)^{-1} && \text{for } p \mid D,\\
\zeta_p(s) &= \left(1 + p^{1-2s}\right)\left(1 - p^{-2s}\right)^{-1}\left(1 - p^{1-2s}\right)^{-1} && \text{for } p \mid M,
\end{aligned}$$

which, if we put:

$$\begin{cases} \alpha_p = 1, \quad d_p = 0 & \text{if } p \mid D,\\ \alpha_p = p+1, \quad d_p = -p & \text{if } p \nmid D, \end{cases} \qquad \begin{cases} \beta_p = 1, \quad h_p = 0 & \text{if } p \mid DM,\\ \beta_p = p+1, \quad h_p = -p & \text{if } p \nmid DM, \end{cases}$$

we can re-write as

$$\begin{aligned}
\zeta_{\mathcal{O}}(s) &= \prod_p \zeta_p(s) = 2\prod_p\left(1 - \alpha_p p^{-2s} - d_p p^{-4s}\right)^{-1} - \prod_p\left(1 - \beta_p p^{-2s} - h_p p^{-4s}\right)^{-1}\\
&= 2\sum_{n\geqslant 1}\frac{\mu(n)}{n^{2s}} - \sum_{n\geqslant 1}\frac{\nu(n)}{n^{2s}} = \sum_{n\geqslant 1}\frac{b(n)}{n^{2s}}
\end{aligned}$$

where $\mu(1) = \nu(1) = 1$ and for each k ($k \geqslant 1$, or $k \geqslant 2$, as corresponds), the following recursion formulas hold:

$$\begin{cases} \mu\left(p^k\right) = 1 & \text{for } p \mid D,\\ \mu(p) = p+1;\, \mu\left(p^k\right) = \mu(p)\mu\left(p^{k-1}\right) - p\mu\left(p^{k-2}\right) & \text{for } p \nmid D, \end{cases}$$

$$\begin{cases} \nu\left(p^k\right) = 1 & \text{for } p \mid DM,\\ \nu(p) = p+1;\, \nu\left(p^k\right) = \nu(p)\nu\left(p^{k-1}\right) - p\nu\left(p^{k-2}\right) & \text{for } p \nmid DM. \end{cases}$$

Thus $b(n) = 2\mu(n) - \nu(n)$ satisfies

$$b(1) = 1; \qquad b(p) = \begin{cases} 1 & \text{for } p \mid D,\\ 2p+1 & \text{for } p \mid M,\\ p+1 & \text{for } p \nmid DM \end{cases} \tag{2}$$

with

$$b(p^k) = \begin{cases} 1 & \text{for } p \mid D, \\ 2\mu(p^k) - 1 & \text{for } p \mid M, \\ b(p)b(p^{k-1}) - pb(p^{k-2}) & \text{for } p \nmid DM. \end{cases} \tag{3}$$

Note that, as the row sums of the Brandt matrices B_n is a constant $b(n)$, the vector $u = (1, 1, \ldots, 1)$ (κ ones) is an eigenvector of the Brandt matrices of level N. We have $B_n u^t = b(n)u^t$, for all $n \in \mathbb{N} \cup \{0\}$. If we take, in the Brandt matrix series $\Theta = (\theta_{ij}) = \sum B_n q^n$, the sum of any row

$$\sum_j \theta_{ij}(\tau)$$

this is an Eisenstein series whose q-expansion is given by

$$e_2(z) = b(0) + \sum_{n \geqslant 1} b(n)q^n.$$

The zero-coefficient is (see [Eic72, p. 95] for details)

$$b(0) = \sum_{i=1}^{n} \frac{1}{2w_i} = \frac{1}{24} \prod_{p \mid D} (p-1) \prod_{q \mid M} (q+1). \tag{4}$$

The series $e_2(z)$ is a modular form of weight 2 and level N, as it is a linear combination of theta series that are modular forms of weight 2 and level N.

Though this is a known result, we summarize it in the following

Proposition 3.1. *Let $N = DM$ be a square-free integer as before and $\mathcal{B}$ the quaternion algebra ramified at exactly those primes $p \mid D$ and at infinity. Let $b(n)$ be the row sum of the Brandt matrix B_n, associated to an order of level N in $\mathcal{B}$. Then $e_2 = b(0) + \sum_{n \geqslant 1} b(n)q^n$ is a weight 2, level N, Eisenstein series. If we associate to it the vector $u = (1, \ldots, 1)$ (κ ones), we have $B_n u^t = b(n)u^t$.*

Note that for N prime, we get the series

$$e_2(z) = \frac{N-1}{24} + \sum_{n \geqslant 1} \sigma(n)_N q^n = E_2(z) - NE_2(Nz)$$

where E_2 is the non-holomorphic Eisenstein series of weight 2 and level 1. Recall that $\sigma(n)_N$ denotes the sum of the divisors of n which are prime to N.

The space of Eisenstein series in $M_2(N)$, for N prime, is one-dimensional, and it is thus generated by $e_2(z)$.

3.2. A (known) congruence among two weight two modular forms

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, with an ℓ torsion point P defined over $\mathbb{Q}$, where $\ell > 2$ is prime. Let $f = \sum_{n \geqslant 1} a_n q^n$ be the normalized modular form of weight 2 and level N associated to E.

It is a known fact (see, for example, [Ser68]) that for any prime p of good reduction, that is, for any $p \nmid N$ (including the prime ℓ if necessary), we have a congruence:

$$a_p \equiv 1 + p \mod \ell.$$

For a prime p of bad reduction we have:

$$a_p = -\operatorname{sgn} W_p$$

where W_p is the Atkin–Lehner involution at the prime p.

Note that this gives, following the notation of the previous section:

- $b(p) \equiv a_p \mod \ell$ for any $\ell \nmid DM$.
- $b(p) = 1 = a_p$. In particular, $b(p) \equiv a_p \mod \ell$ for any $p \mid D$.

For primes $p \mid M$ we have

- $2p + 1 = b(p) \equiv a_p = -1 \mod \ell$ if and only if $\ell \mid 2(p+1)$.

As the group of nonsingular points $\widetilde{E}_p$ has order $p+1$ and a point of order ℓ, this last congruence also holds. In fact, the ℓ-torsion point P reduces to a nonsingular point in the reduced curve $\widetilde{E}_p$ and the group of nonsingular points in $\widetilde{E}_p$ has order

$$\begin{aligned} &p-1 \quad \text{if } a_p = 1\text{, that is, } E \text{ has split multiplicative reduction at } p,\\ &p+1 \quad \text{if } a_p = -1\text{, that is, } E \text{ has non-split multiplicative reduction at } p. \end{aligned} \tag{5}$$

Thus ℓ must divide $p+1$ if $a_p = -1$ or, equivalently, $\operatorname{sgn} W_p = 1$, and ℓ must divide $p-1$ if $a_p = 1$ or $\operatorname{sgn} W_p = -1$.

Note that this also shows that ℓ divides each factor in the numerator of (4).

From the recursion formulas for a_n and $b(n)$ it follows that $a_n \equiv b(n)$ modulo ℓ for every n. As the coefficients a_n and $b(n)$ are multiplicative, it is enough to check this for n equal to a prime power. Further, for any prime $p \nmid DM$ the recursion formulas for a_{p^k} and $b(p^k)$ are the same, and there is nothing to check. For $p \mid D$, $a_{p^k} = b(p^k) = 1$. Thus we only need to see that $b(q^k) \equiv a_{q^k}$ modulo ℓ, for primes $q \mid M$.

Here $u(q) = q + 1 \equiv 0 \mod \ell$, $u(1) = 1$ and $-q \equiv 1 \mod \ell$, and the recursion formula for $u(q^k) = u(q)u(q^{k-1}) - qu(q^{k-2})$ give

$$u\big(q^k\big) \underset{\ell}{\equiv} \begin{cases} 1 & \text{if } k \text{ is even,}\\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

This gives

$$b\big(q^k\big) = 2u\big(q^k\big) - 1 \underset{\ell}{\equiv} \begin{cases} 1 & \text{if } k \text{ is even,}\\ -1 & \text{if } k \text{ is odd,} \end{cases}$$

which is the same as $a_{q^k} = (-1)^k$. This gives $b(n) \equiv a_n \mod \ell$ for every $n \in \mathbb{N}$.

Further, the zero-coefficient $b(0)$ is divisible by the prime ℓ. Thus we have the following

Proposition 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve of square-free conductor $N = DM$ and analytic rank zero. Assume E has a torsion point defined over $\mathbb{Q}$, of odd prime order ℓ. Let $f = \sum_{n\geqslant 1} a_n q^n$ be the weight 2, level N newform associated to E and $e_2(z)$ the weight 2 Eisenstein series for $\Gamma_0(N)$, represented in the quaternion algebra $\mathcal{B}$, ramified at the primes $p \mid D$ and whose coefficients are the row sums of the Brandt matrices of level N. Then*

$$f \equiv e_2 \mod \ell.$$

Note that, as the elliptic curve E has analytic rank zero, and thus the sign of its functional equation is $+1$, if N is prime, this sign is $\epsilon = -\epsilon_N$ and thus $a_N = 1$. Then we have, for each prime p, $a_p \equiv \sigma(p)_N \bmod \ell$, which gives for each index $n \geqslant 1$ the congruence

$$a_n \equiv \sigma(n)_N \mod \ell.$$

3.3. A congruence among eigenvectors of Brandt matrices

We know that the Brandt matrices B_p for p prime to the level, act as the Hecke operators T_p on the space of newforms. We know further, that to a newform f corresponds an eigenvector v such that, for $(p, N) = 1$,

$$B_p v = a_p v.$$

In fact we have that this equality holds for *every* prime p, as we will now show.

Take the Brandt matrix series

$$\Theta(z) = \sum_{m=0}^{\infty} B_m q^n.$$

Recall this is a $\kappa \times \kappa$ matrix whose entries are theta series θ_{ij}.

$$\Theta v = \left(\sum_{m \geqslant 0} B_m q^m\right) v.$$

We have

$$T_p(\Theta v) = \left(\sum_{m \geqslant 0} B_p B_m q^m\right) v = \sum_{m \geqslant 0} B_m (B_p v) q^m = a_p \left(\sum_{m \geqslant 0} B_m q^m\right) v = a_p(\Theta v).$$

Thus $\sum_j \theta_{ij} v_j$ if it is non-zero, it is an eigenfunction for all the Hecke operators T_p with eigenvalue a_p; at least for p prime to the level N.

We know that there is a basis of $S_2(N)$ whose elements are eigenforms for all the T_n with $(n, N) = 1$. The *multiplicity one* statement says that, restricting our attention to *newforms*, to each set of eigenvalues $\{a_n\}$ for n prime to the level, corresponds a one-dimensional eigenspace $\langle f \rangle$. As the operators T_p commute for all p, f will be an eigenfunction for *all* T_p and it is determined by the Fourier coefficients a_p with $(p, N) = 1$.

This means that $\sum_j \theta_{ij} v_j = \lambda_i f$, for some λ_i. Further, we have: λ_i is the coefficient of q in the Fourier expansion of

$$\theta_{ij} v_j = \sum_m \left(\sum_j \theta_{ij}(m) v_j\right) q^m$$

which is $\sum_j \theta_{ij}(1) v_j = v_i$ as B_1 is the identity matrix.

Consider a prime $p \mid N$, and some index i, such that $v_i \neq 0$. Thus $v_i f = \sum_j \theta_{ij} v_j$ and the Hecke operator T_p acts on $v_i f$ as

$$T_p\left(\sum_j \theta_{ij} v_j\right) = \sum_j T_p \theta_{ij} v_j = \sum_j T_p\left(\sum_m \theta_{ij}(m) q^m\right) v_j = \sum_j \sum_m \theta_{ij}(pm) v_j q^m,$$

$$a_p v_i f = \sum_m \left(\sum_j \theta_{ij}(pm) v_j\right) q^m.$$

Comparing coefficients for $m = 1$,

$$a_p v_i = \sum_j \theta_{ij}(p) v_j$$

which means that

$$a_p v = B_p v.$$

This shows that the coefficients $\{a_p\}$ are the eigenvalues of v, for *every* prime p, and thus for every n. Then the congruence in Proposition 3.2 shows up in the quaternion algebra $\mathcal{B}$ as a congruence among eigenvalues, as we state in the following

Proposition 3.3. *Let E be an elliptic curve of conductor $N = DM$ as above, having a rational ℓ-torsion point, ℓ odd. Let $e_2 = \sum b(n) q^n$ with $b(n)$ as in* (2), (3), (4) *of* 3.1, *and let f be the modular form of level N, corresponding to E. Let v be the eigenvector of the Brandt matrices, corresponding to f, and u the one corresponding to e_2. Then, for every n, the respective eigenvalues, of the Brandt matrices B_n, of v and u, are congruent modulo ℓ.*

What can we say about the eigenvectors v and u modulo ℓ?

Suppose we can prove $\lambda v \equiv u \bmod \ell$, for some $\lambda \in \mathbb{F}_\ell^\times$. This would mean that we will have the same relation modulo ℓ among respective modular forms of weight 3/2.

For prime conductors N we can prove more: the Brandt matrices reduced modulo ℓ have a one-dimensional eigenspace for the reduced eigenvalues $b(p)$.

As for elliptic curves of non-prime conductors we have calculated several examples with $N = pM$, such that W_p acts on E with -1 sign, and W_q with sign $+1$ for every other prime $q \mid M$. This means that we work in a quaternion algebra ramified at exactly one finite prime.

In the examples calculated we obtained that the eigenspace of the Brandt matrices associated to the eigenvalues $\{b(p)\}$, reduced modulo ℓ, is of dimension one. We do not know if this represents the general situation or not. See Section 3.7.

3.4. *N prime: multiplicity one*

Recall that for prime conductor N, $e_2 = \frac{N-1}{24} + \sum_{n \geqslant 1} \sigma(n)_N q^n$.

We are going to see that if we consider the reduced Brandt matrices modulo the prime ℓ, there is a dimension one eigenspace for the system of eigenvalues $\sigma(n)_N \bmod \ell$.

We will need some results on the *Eisenstein ideal*, as well as modular forms over rings which can be found in the work of Mazur [Maz77, Chapter II, §5, §9].

Consider the weight 2 Eisenstein series for $\Gamma_0(N)$

$$e_2(z) = \frac{N-1}{24} + \sum_{n \geqslant 1} \sigma(n)_N q^n.$$

Remove the constant term and consider the formal power series

$$\delta = \sum_{n \geqslant 1} \sigma(n)_N q^n.$$

By the work of Mazur [Maz77, Chapter II, §5], δ is a modular form modulo an integer m if and only if m divides $\frac{N-1}{2}$ and it is a cusp form if m divides the exact numerator, η, of $\frac{N-1}{12}$.

Note that, if $f \equiv e_2 \bmod \ell$, for a prime ℓ and a cusp form f, then δ is clearly a cusp form modulo ℓ and thus ℓ divides η.

Let R denote the ring $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$, and $M(R)$, $S(R)$ the space or modular forms and cusp forms, of weight 2 and level N, with coefficients in R (as described in [Maz77]). If $f \in S(R)$ is an eigenvector for all T_p, $p \neq N$ and for T_N then $L(f,s)$ has an Euler product and f is determined, up to a scalar, by the eigenvalues.

By the Hecke algebra $\mathbb{T}$ we shall mean the algebra generated by T_p for $p \nmid N$ and T_N.

Let $\mathcal{M} \subset \mathbb{T}$ be a maximal ideal with residue field k of characteristic p. Denote $S(\mathbb{F}_p)[\mathcal{M}]$ the kernel of the ideal $\mathcal{M}$ in $S(\mathbb{F}_p)$. This may be viewed as a k-vector space.

Proposition 3.4. *$S(\mathbb{F}_p)[\mathcal{M}]$ is of dimension one over k.*

The *Eisenstein ideal* $\mathcal{I} \subset \mathbb{T}$ is the ideal generated by the elements $1 + p - T_p$ and $1 - T_N$. Thus any element in $S(R)[\mathcal{I}]$ is an eigenvector for the operators T_p $(p \neq N)$ and T_N, with eigenvalues $c_p = 1 + p$ $(p \neq N)$ and $c_N = 1$.

In $R[[q]]$ the generating eigenvector for these c_p eigenvalues is the power series δ. Thus the q-expansion of any element in the R-module $S(R)[\mathcal{I}]$ is a scalar multiple of δ.

Proposition 3.5 *(Mazur).*

(1) *Let m be any integer divisible by $\eta =$ the exact numerator of $\frac{N-1}{12}$. Then $S(\mathbb{Z}/m\mathbb{Z})[\mathcal{I}]$ is a cyclic group of order η, generated by $\frac{m}{\eta}\delta$.*

(2) *$\mathbb{T}/\mathcal{I} = \mathbb{Z}/\eta\mathbb{Z}$; the Eisenstein ideal $\mathcal{I}$ contains the integer η.*

For details on this see [Maz77, §9].

A prime ideal $\mathcal{M}$ in the support of the Eisenstein ideal is called an Eisenstein prime. The Eisenstein primes $\mathcal{M}$ are in one-to-one correspondence with the primes $p \mid \eta$. For $p \mid \eta$ the Eisenstein prime corresponding to p is given by $\mathcal{M} = (\mathcal{I}, p)$. Then $\mathbb{T}/\mathcal{M} = \mathbb{F}_p$ and $\mathcal{M}$ is a maximal ideal and it is the unique Eisenstein prime whose residue field is of characteristic p.

Let $\mathcal{X}$ denote the free $\mathbb{Z}$ module of divisors supported on the set of singular points of the curve $X_0(N)$ in characteristic N. This set is in bijection with the set of isomorphism classes of supersingular elliptic curves in $\overline{\mathbb{F}}_N$. Brandt matrices of prime level N are related to isogenies between them.

The Hecke algebra $\mathbb{T}$ acts on the module $\mathcal{X}$. Let $\mathcal{M}$ be an Eisenstein prime of residue characteristic ℓ. Recall that $\mathbb{T}/\mathcal{M} \simeq \mathbb{F}_\ell$, thus the set of points in $\mathcal{X}/\ell\mathcal{X}$ annihilated by the Eisenstein prime $\mathcal{M}$ is a vector space over $\mathbb{F}_\ell$.

In a form closer to our present setting, we can think the module $\mathcal{X}$ as the $\mathbb{Z}$-module generated by the ideal classes $I_1, \ldots, I_\kappa$ of a maximal order $\mathcal{O}$ in the quaternion algebra $\mathcal{B}$ ramified at N and at ∞. We will denote this $\mathbb{Z}$-module by $\mathcal{X}(\mathcal{O})$. The action of the Hecke algebra $\mathbb{T}$ on $\mathcal{X}$ corresponds to the action of the Brandt matrices in $\mathcal{X}(\mathcal{O})$ as follows:

Let $x = \sum_{i=1}^{\kappa} m_i I_i$, then B_n acts by multiplication: if $(s_1, \ldots, s_\kappa)^t = B_n(m_1, \ldots, m_\kappa)^t$, then $B_n.x = \sum_{i=1}^{\kappa} s_i I_i$.

To see that these two settings are parallel situations see, for example, [Eme02] and [PT07].

The eigenvectors u and v correspond to the elements $X = \sum I_i$ and $Y = \sum v_i I_i$ in $\mathcal{X}(\mathcal{O})$, whose eigenvalues are congruent modulo ℓ. Let us denote by $\mathbb{B}$ the $\mathbb{Z}$-algebra generated by the Brandt matrices. Consider the maximal Eisenstein prime $\mathcal{M}$ of $\mathbb{B}$ given by $\mathcal{M} = \langle B_p - (p+1)\,\mathrm{id}, B_N - \mathrm{id}, \ell \rangle$. Then $\mathbb{B}/\mathcal{M} = \mathbb{F}_\ell$.

Call $\bar{u}$, $\bar{v}$ the reductions of u and v modulo ℓ. Thus $\bar{u}$ and $\bar{v}$ correspond to the elements $\bar{X}$, $\bar{Y}$ in $\mathcal{X}(\mathcal{O})/\ell\mathcal{X}(\mathcal{O})$ that are in the kernel of the action of $\mathcal{M}$. Then $\bar{X}, \bar{Y} \in \mathcal{X}(\mathcal{O})/\ell\mathcal{X}(\mathcal{O})[\mathcal{M}]$ which is a $\mathbb{B}/\mathcal{M}$-module, and thus an $\mathbb{F}_\ell$ vector space. If $\mathcal{X}(\mathcal{O})/\ell\mathcal{X}(\mathcal{O})[\mathcal{M}]$ is of dimension one over $\mathbb{F}_\ell$, then $\bar{X} = \lambda\bar{Y}$ and thus $u \equiv \lambda v \bmod \ell$ for some $\lambda \in \mathbb{F}_\ell^\times$.

Going back to the $\mathbb{Z}$-module $\mathcal{X}$ and the Hecke algebra $\mathbb{T}$ we need to prove that $\mathcal{X}/\ell\mathcal{X}[\mathcal{M}]$ is of dimension one over $\mathbb{T}/\mathcal{M}$.

In [Eme02] M. Emerton works on the spanning of spaces of modular forms by theta series and gives a detailed analysis of the $\mathbb{T}$-module $\mathcal{X}$. In particular, it is shown that $\mathcal{X}/\ell\mathcal{X}[\mathcal{M}]$ and $\mathcal{X}/\mathcal{M}$ are of the same dimension over $\mathbb{T}/\mathcal{M}$ and that $\mathcal{X}/\mathcal{M}$ has dimension one over $\mathbb{T}/\mathcal{M}$. We refer the reader to [Eme02, Lemma 4.1 and the proof of Theorem 4.2].

This proves the following

Theorem 3.6. *Let $\mathcal{B}$ be the quaternion algebra ramified at the prime N and at infinity. Let $\{B_p\}$ be the Brandt matrices of prime degree p and level N. Let ℓ be a prime dividing the exact numerator η of $\frac{N-1}{12}$ and consider the reduced Brandt matrices $B_p \bmod \ell$. Then the eigenspace associated to the system of eigenvalues $\{\sigma(p)_N\} \bmod \ell$ has dimension one.*

3.5. A congruence among modular forms of weight 3/2

To the Eisenstein series e_2 corresponds the weight 3/2 Eisenstein series $\mathcal{H}_N$, which is defined by

$$\mathcal{H}_N = \sum \frac{1}{w_i} g_i.$$

If the eigenvectors v and u are proportional modulo ℓ, that is, $u \equiv \lambda v \bmod \ell$, then we automatically have $\lambda g_N \equiv \mathcal{H}_N \bmod \ell$, provided that the number of units w_i in the right orders R_i are prime to ℓ. For $\ell = 5, 7$ there is nothing to do, as $w_i \mid 12$.

Suppose $\ell = 3$. It is known that (see [Gro87, §1]) the product $\prod_{i=1}^{\kappa} w_i$ equals the exact denominator of $\frac{N-1}{12}$. Recall that, as δ is a cusp form modulo $\ell = 3$, 3 divides the exact numerator of $\frac{N-1}{12}$ and it cannot divide its exact denominator. Then we have,

$$3 \nmid \prod_{i=1}^{\kappa} w_i$$

and

$$\lambda g_N \equiv \mathcal{H}_N \mod \ell \quad \left(\lambda \in \mathbb{F}_\ell^\times\right).$$

For N prime we know the q-expansion of $\mathcal{H}_N$ and how its coefficients are related to class numbers of imaginary quadratic number fields: $\mathcal{H}_N$ has Fourier expansion

$$\mathcal{H}_N = \frac{N-1}{24} + \sum_{d>0} H_N(d) q^d$$

where

- $H_N(d)$ is zero unless $-d \equiv 0, 1(4)$ and $(\frac{-d}{N}) \neq 1$.
- For $d > 0$ such that $(-d)$ is a fundamental discriminant, let $K = \mathbb{Q}(\sqrt{-d})$, let $\mathcal{O}_d$ be the ring of integers in K, $h(d)$ its class number and $u(\mathcal{O}_d)$ one half the order of the units in K (this is 1, except for $d = 3, 4$).

$$H_N(d) = \begin{cases} \frac{h(d)}{u(\mathcal{O}_d)} & \text{if } N \text{ is inert in } K, \\ \frac{1}{2}\frac{h(d)}{u(\mathcal{O}_d)} & \text{if } N \text{ is ramified in } K. \end{cases}$$

Thus $H_N(d)$ is the class number $h(d)$ or $\frac{1}{2}h(d)$ except for, at most, 2 values of d.

For $w = \prod_{i=1}^{\kappa} w_i$, we have that $wH_N(d)$ is integral.

From the examples calculated for non-prime conductors N (see 3.7 below) we expect the following formula for $\mathcal{H}_N(d)$ to be true.

Conjecture 3.7. *Let $\mathcal{B}$ be a definite quaternion algebra ramified at exactly one finite prime p, and let $N = pM$ be a square-free integer. Denote by $\mathcal{H}_N$ the weight 3/2 Eisenstein series constructed in the quaternion algebra $\mathcal{B}$ as explained in* 2.1.

Let $d \in \mathbb{N}$ such that $-d$ is a fundamental discriminant such that

$$\left(\frac{-d}{p}\right) \neq 1 \quad \textit{and} \quad \left(\frac{-d}{q}\right) \neq -1 \quad \textit{for every } q \mid M. \tag{6}$$

Let $h(d)$ be the class number in $\mathbb{Q}(\sqrt{-d})$, $\mathcal{O}_d$ its ring of integers and $u(\mathcal{O}_d)$ the number of units in $\mathcal{O}_d$.

Set r to be the number of (distinct) primes that divide N and $s(d)$ the number of primes that divide N and ramify in $\mathbb{Q}(\sqrt{-d})$. Then we conjecture the following formula holds

$$H_N(d) = \frac{2^{r-1}}{2^{s(d)}}\frac{h(d)}{u(\mathcal{O}_d)}. \tag{7}$$

3.6. The order of analytic Ш

Recall that we want to analyze the distribution of Ш among negative quadratic twists of elliptic curves E, with associated modular form f.

For the strong Weil curves of rank zero and prime conductor N, having an odd torsion point of prime order ℓ, we have that the order of $Ш_d$ is the coefficient m_d^2 of the modular form g of weight 3/2 under Shimura correspondence to f, divided by a power of 2 (see [Qua06]). This amounts to the curves 11A1, 19A1 and 37B1. Thus, we have the following

Proposition 3.8. *Let E be one of the elliptic curves* 11A1, 19A1 *or* 37B1. *Consider the family $\{E_d\}$, of negative quadratic twists of E, for $-d$ a fundamental discriminant and $(\frac{-d}{N}) \neq 1$. Suppose E has a torsion point defined over $\mathbb{Q}$, of odd prime order ℓ. Then, $|Ш_d|$ is divisible by ℓ, if and only if the class number $h(d)$ of $\mathbb{Q}(\sqrt{-d})$ is divisible by ℓ.*

As we said in the introduction, if we further assume the Cohen–Lenstra heuristics on the probability of class numbers being divisible by a prime, and assume that this probability is valid when restricted to discriminants $-d$ with $(\frac{-d}{N}) \neq 1$, then the probability of Ш being divisible by ℓ among negative quadratic twists of E is given by

$$P(\ell) = 1 - \prod_{i \geqslant 0}\left(1 - \frac{1}{\ell^i}\right) = \frac{1}{\ell} + \frac{1}{\ell^2} - \frac{1}{\ell^3} - \frac{1}{\ell^7} \cdots.$$

It is worth pointing out here that we also obtained a relation $Ш_d = \frac{m_d^2}{2^*}$, where 2^* indicates some (even) power of 2 for all examples calculated for elliptic curves of prime conductor in [Qua06]: 17A1, 67A1, 73A1, 89B1, 109A1, 139A1 and 307A1, 307B1, 307C1, 307D1. This has been calculated numerically replacing in Waldspurger's formula (1) $L(f_N \otimes \epsilon_d, 1)$ by what it is expected by the Birch and Swinnerton-Dyer conjecture. This gives a formula for $|\text{Ш}_d|$ in terms of computable factors depending on d (which can be calculated with PARI-GP), and the coefficient m_d^2 of the weight 3/2 modular form (recall we are including the possibility "$|\text{Ш}_d| = 0$" if E_d has analytic rank > 0). This has been calculated for $d \leqslant 10^6$ in all cases mentioned above.

Also, we get the same formula for $|\text{Ш}_d|$ for curves 14A1, 26A1 and 26B1. This has been calculated for the smaller range $d \leqslant 2000$.

If for a particular elliptic curve E we can check that $|\text{Ш}_d| = \frac{m_d^2}{2^*}$, then we have the following result:

Proposition 3.9. *Let E be an elliptic curve of analytic rank zero and square-free conductor N. Suppose the sign of W_p acting on f is -1 for exactly one prime $p \mid N$. Consider the family $\{E_d\}$, of negative quadratic twists of E, satisfying the Kronecker conditions* (6)*. Suppose E has a torsion point defined over $\mathbb{Q}$, of odd prime order ℓ and that $|\text{Ш}_d| = \frac{m_d^2}{2^*}$. Then, assuming $\lambda u \equiv v \bmod \ell$ and* (7)*, we have that $|\text{Ш}_d|$ is divisible by ℓ, if and only if the class number $h(d)$ of $\mathbb{Q}(\sqrt{-d})$ is divisible by ℓ.*

3.7. Examples

Our goal was to obtain a similar result to 3.8 for square-free levels, or at least, have some conjecture on this. In this section we give some examples we have calculated to test multiplicity one mod ℓ and to conjecture on the coefficients of $H_N(d)$.

We will consider, an elliptic curve E of analytic rank zero and conductor $N = pq$, with p, q primes. Suppose that $\operatorname{sgn} W_p = -1$ and $\operatorname{sgn} W_q = 1$. Further, suppose that E has an ℓ-torsion point defined over $\mathbb{Q}$.

We showed in 3.1 and 3.2 that there is an Eisenstein series $e_2 = \sum c_n q^n$ such that for every prime p (and thus for every n), $a_p \equiv c_p \bmod \ell$. Here $f_N = \sum a_n q^n$ is the modular form of the elliptic curve E.

In the examples we focused on the following two points:

- The eigenvectors of the Brandt matrices corresponding f_N and e_2 to be linearly dependent modulo ℓ.
- The relation among the coefficients of the corresponding weight 3/2 Eisenstein series $\mathcal{H}_N$ and the class numbers of imaginary quadratic number fields.

We use the standard notation for elliptic curves: $[a_1, a_2, a_3, a_4, a_6]$ stands for $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and we name them as in Cremona's tables.

For our calculations we used routines from A. Pacetti [Pac] for doing arithmetic over quaternion algebras and from G. Tornaria [Tor04], both of which run under PARI-GP. The packages we use are *qalgmodforms* and *quadminim*.

The procedure is very similar to that used in [Qua06], so we will not give all the details but, briefly, state which routines we use.

- ***N* = 14.**
  The elliptic curve $E = (14A1) = [1, 0, 1, 4, -6]$ has conductor $N = 14$ and a 3-torsion point.
  The signs of the Atkin–Lehner at the primes $p = 7$ and $p = 2$ are, respectively, -1 and $+1$. These can be calculated with the routine `ellrootno` of PARI-GP.
  We work with an order $\mathcal{O}$ of level 14 in the quaternion algebra $\mathcal{B}$ ramified at the prime 7 and at ∞: `qsetprime(7)` sets the quaternion algebra and `qorderlevel(14)` returns an order of level 14 in $\mathcal{B}$. There are 2 left-ideal classes for $\mathcal{O}$, I_1, I_2 which are calculated with `qidcl(`$\mathcal{O}$`)`. Thus we have two right orders $\mathcal{R}_1$ and $\mathcal{R}_2$, given by `qrorder(`I_i`)`. The number of units in each right order is calculated with `qrepnum(`$\mathcal{R}_i$`, 1)`. We have that one half the units in each order R_i are $w_1 = 2$ and $w_2 = 1$.

With this we can calculate the weight 3/2 modular forms g_i. We need the rank-three lattices S_i^0. Once we have a basis for a lattice, we calculate with $\frac{1}{2}$qgram(S_i^0) the matrix A_i of the bilinear form restricted to the lattice, in the basis given. The routine $\frac{1}{2}$ qfminim3($A_i, b, 0, 3$) returns $b+1$ coefficients of the form g_i.

To calculate g we need the eigenvector v of the Brandt matrices. The first Fourier coefficients for the modular form f attached to E are $a_2 = -1, a_3 = -2, a_5 = 0, a_7 = 1, \ldots$. To calculate the eigenvector of the Brandt matrices corresponding to f we need to intersect the kernels of $(B_p - a_p I)$, for primes p, until we get a space of dimension one. We calculate (say) matker(Brandt($\mathcal{O}$,5)), as $a_5 = 0$ and we get the already one-dimensional space $\langle(-2,1)\rangle$. We put $v = (-2,1)$, $u = (1,1)$. Clearly $v \equiv u \bmod 3$ and thus the eigenvalues must be equivalent modulo 3 as we proved in 3.2.

If we calculate the kernel of $(B_p - b(p)I)$ modulo 3 we find that it is of dimension one.

If $g = \sum \frac{v_i}{w_i} g_i$ and $\mathcal{H}_{14} = \sum \frac{1}{w_i} g_i$ we will have

$$g \equiv \mathcal{H}_{14} \mod 3.$$

Recall that w_i are prime to ℓ.

We analyze the Fourier coefficients of the weight 3/2 Eisenstein series $\mathcal{H}_{14}$.

For this, we calculate the form $\sum \frac{1}{w_i} g_i$ and compare the coefficients with the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$, these last can be calculated with PARI-GP. This has been done for $d \leqslant 1000$.

Let $K_d = \mathbb{Q}(\sqrt{-d})$, let $\mathcal{O}_d$ be its ring of integers, and $h(d)$ its class number. Recall $u(\mathcal{O}_d) = 1$ except for $d = 3, 4$ which have, respectively, 3 and 2 units. Recall that a prime $p \in \mathbb{Z}$ is inert, splits or ramifies in $\mathcal{O}_d$ if the Kronecker symbol $(\frac{-d}{p})$ is, respectively, −1, 1, 0.

We have, for d such that $-d$ is a fundamental discriminant and $(\frac{-d}{7}) \neq 1$ and $(\frac{-d}{2}) \neq -1$:

$$H_{14}(d) = \begin{cases} 2h(d) & \text{if 7 is inert and 2 splits in } \mathcal{O}_d, \\ \frac{h(d)}{u(\mathcal{O}_d)} & \text{if 7 is inert and 2 ramifies in } \mathcal{O}_d, \\ h(d) & \text{if 7 is ramified and 2 splits in } \mathcal{O}_d, \\ \frac{1}{2}h(d) & \text{if 7 and 2 ramify in } \mathcal{O}_d. \end{cases} \tag{8}$$

Note that, as $u(\mathcal{O}_d) = 1$ for every $d \neq 3, 4$ we will not detect numerically if we have to divide by $u(\mathcal{O}_d)$ unless 3 or 4 is in the class of congruences we are considering. Further, as neither 3 or 4 is a product of 2 distinct primes, we can equally write $\frac{1}{2}\frac{h(d)}{u(\mathcal{O}_d)}$ in the last row of (8).

- $\boldsymbol{N = 26.}$

We have two elliptic curves of level 26 and analytic rank zero.

(26A) $E = (26A1) = [1, 0, 1, -5, -8]$ with $|\mathrm{Tor}(E)| = 3$.

We have $\operatorname{sgn} W_{13} = -1$ and $\operatorname{sgn} W_2 = +1$. We work in the quaternion algebra ramified at infinity and 13; and calculate the Brandt matrices for an order of level 26, and the eigenvector v corresponding to f_{26} (and to E). This gives the eigenvector $v = (-2, 1, 1)$ which again is clear that $v \equiv u = (1, 1, 1) \bmod 3$.

For the coefficients of the weight 3/2 Eisenstein series $\mathcal{H}_{26A}$, we obtain numerically, for d such that $-d$ is a fundamental discriminant and $(\frac{-d}{13}) \neq 1$ and $(\frac{-d}{2}) \neq -1$ exactly the same coefficients as in (8) replacing 7 by 13.

(26B) $E = (26B1)[1, -1, 1, -3, 3]$ with $|\mathrm{Tor}(E)| = 7$; $\operatorname{sgn} W_2 = -1$ and $\operatorname{sgn} W_{13} = +1$. We work in the quaternion algebra ramified at ∞ and 2.

The eigenvector for E is $v = (-4, 3, 3)$ which again is clear that $v \equiv 3u \bmod 7$.

As for the coefficients of $\mathcal{H}_{26B}$ we can correct Eq. (8), in what concerns dividing by the units in $\mathcal{O}_d$:

$$H_{26B}(d)=\begin{cases}2\frac{h(d)}{u(\mathcal{O}_K)} & \text{if 2 is inert and 13 splits in } \mathcal{O}_d,\\ \frac{h(d)}{u(\mathcal{O}_K)} & \text{if 2 is inert and 13 ramifies in } \mathcal{O}_d,\\ \frac{h(d)}{u(\mathcal{O}_K)} & \text{if 2 ramifies and 13 splits in } \mathcal{O}_d,\\ \frac{1}{2}\frac{h(d)}{u(\mathcal{O}_K)} & \text{if 13 and 2 ramify in } \mathcal{O}_d.\end{cases}$$

- ***N* = 77.**
  $E=(77B1)=[0,1,1,-49,600]$ with $|\mathrm{Tor}(E)|=3$; $\operatorname{sgn} W_7=-1$ and $\operatorname{sgn} W_{11}=+1$.
  The eigenvector for E is $v=(4,1,-2,1,-2,-2)$ and $v\equiv u \bmod 3$. And $H_{77}(d)$ is as in (7).
- ***N* = 30 = 2.3.5.**
  $E=(30A1)=[1,0,1,1,2]$ with $|\mathrm{Tor}(E)|=6$; $\operatorname{sgn} W_3=-1$ and $\operatorname{sgn} W_2=\operatorname{sgn} W_5=+1$. Here N is a product of three primes.
  The eigenvector for E is $v=(-1,-1,2,2)$. We have $-v\equiv u \bmod 3$.
  For the coefficients of $\mathcal{H}_{30}$ recall that we will only consider $(\frac{-d}{3})\neq 1$ and $(\frac{-d}{p})\neq -1$ for $p=2,5$. We obtain

$$H_{30}(d)=\begin{cases}2^2\frac{h(d)}{u(\mathcal{O}_K)} & \text{if 3 is inert and 2, 5 split in } \mathcal{O}_d,\\ 2\frac{h(d)}{u(\mathcal{O}_K)} & \text{if exactly one of the primes 2, 3, 5 ramifies in } \mathcal{O}_d,\\ \frac{h(d)}{u(\mathcal{O}_K)} & \text{if exactly two of the primes 2, 3, 5 ramify in } \mathcal{O}_d,\\ \frac{1}{2}\frac{h(d)}{u(\mathcal{O}_K)} & \text{if 2, 3 and 5 all ramify in } \mathcal{O}_d.\end{cases}$$

- ***N* = 58 = 2.29.**
  $E=(58B1)=[1,1,1,5,9]$ with $|\mathrm{Tor}(E)|=5$; $\operatorname{sgn} W_2=-1$. Then $\mathcal{B}$ is ramified at ∞ and 2.
  Eigenvector for E: $v=(-4,1,1)$, $v\equiv u \bmod 5$. As for the coefficients of $H_{58}(d)$ these are as in (7).
- **Some considerations.**
  In all the examples above, we have that the eigenspace of the Brandt matrices reduced modulo ℓ and associated to the eigenvalues of u is of dimension 1.
  Some more examples (picked "at random"):
  For $862D1=[1,0,0,8,64]$ and $1293A1=[0,1,1,-73,217]$, both with a 3-torsion point we still have a relation $v\equiv 2u \bmod 3$ (we have not checked multiplicity one mod 3).
  We want to observe that for curves $1006B1=[1,-1,0,8,0]$ and $862C1=[1,-1,1,6,-7]$ both with a torsion point of order 2, that we do not have any relation such as $v\equiv u \bmod 2$.

Acknowledgment

I want to thank Matthew Emerton for pointing me out his work [Eme02] from which the results in Section 3.3 follow.

References

[BS90] S. Bocherer, R. Schulze-Pillot, On a theorem of Waldspurger and on Eisenstein series of Klingen type, Math. Ann. 288 (1990) 361–388.
[CKRS] J.B. Conrey, J.P. Keating, M.O. Rubinstein, N.C. Snaith, Random matrix theory and the Fourier coefficients of half-integral-weight forms, Experiment. Math. 15 (1) (2006) 67–82.
[Cre97] J.E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, 1997.
[Eic72] M. Eichler, The basis problem for modular forms and the trace of the Hecke operators, in: Modular Functions of One Variable I, in: Lecture Notes in Math., vol. 320, Springer-Verlag, Berlin, 1972, pp. 75–151.
[Eme02] M. Emerton, Supersingular elliptic curves, theta series and weight two modular forms, J. Amer. Math. Soc. 15 (2002) 671–714.
[Fre88] G. Frey, On the Selmer group of twists of elliptic curves with q-rational torsion points, Canad. J. Math. XL (1988) 649–665.

[Gro87] B. Gross, Heights and the special values of L-series, in: CMS Conference Proceedings, vol. 7, American Mathematical Society, 1987.
[Jam99] K. James, Elliptic curves satisfying the Birch and Swinnerton Dyer conjecture mod 3, J. Number Theory 76 (1999) 16–21.
[Mal08] G. Malle, Cohen–Lenstra heuristic and roots of unity, J. Number Theory 128 (2008) 2823–2835.
[Maz77] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. Inst. Hautes Etudes Sci. 47 (1977) 33–186.
[Ono01] K. Ono, Nonvanishing of quadratic twists of modular l-functions and applications to elliptic curves, J. Reine Angew. Math. 553 (2001) 81–97.
[Pac] A. Pacetti, Qalgmodforms, http://www.ma.utexas.edu/users/villegas/cnt/cnt-frames.html.
[PT07] A. Pacetti, G. Tornaria, Shimura correspondence for level p^2 and the central values of l-series, J. Number Theory 124 (2007) 396–414.
[Piz80] A. Pizer, An algorithm for computing modular forms on $\Gamma_0(N)$, J. Algebra 64 (1980) 340–390.
[Qua06] P. Quattrini, On the distribution of analytic $\sqrt{|Ш|}$ values on quadratic twists of elliptic curves, Experiment. Math. 15 (3) (2006) 355–365.
[Ser68] J.P. Serre, Abelian l-Adic Representations and Elliptic Curves, Benjamin, 1968.
[Tor04] G. Tornaria, Data about the central values of the L-series of (imaginary and real) quadratic twists of elliptic curves, http://www.ma.utexas.edu/users/tornaria/cnt, 2004.
[Wal81] J.L. Waldspurger, Sur les coefficients de fourier des formes modulaires de poids demi-entier, J. Math. Pures Appl. 60 (1981) 375–484.
[Won99] S. Wong, Elliptic curves and class number divisibility, Int. Math. Res. Not. IMRN 12 (1999) 661–672.