On the Distribution of Analytic $\sqrt{|\text{Ш}|}$ Values on Quadratic Twists of Elliptic Curves

Patricia L. Quattrini

CONTENTS

The aim of this paper is to analyze the distribution of analytic (and signed) square roots of Ш values on imaginary quadratic twists of elliptic curves.

Given an elliptic curve E of rank zero and prime conductor N, there is a weight-$\frac{3}{2}$ modular form g associated with it such that the d-coefficient of g is related to the value at $s = 1$ of the L-series of the $(-d)$-quadratic twist of the elliptic curve E. Assuming the Birch and Swinnerton-Dyer conjecture, we can then calculate for a large number of integers d the order of Ш of the $(-d)$-quadratic twist of E and analyze their distribution.

1. INTRODUCTION

Let E be an elliptic curve of prime conductor N and rank zero, and let

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

be the L-function of E. By recent work of Wiles and others it is known that

$$f = \sum_{m=1}^{\infty} a_m q^m, \quad q = e^{2\pi i \tau},$$

is a modular form of weight 2, level N, and $L(E, s) = L(f, s)$. Moreover, f is a cusp form and an eigenfunction for all the Hecke operators T_n acting on $M_2(\Gamma_0(N))$. If we normalize to have $a_1 = 1$, then the Fourier coefficients a_i are the eigenvalues.

For d a positive integer such that $-d \equiv 0, 1 \pmod 4$, we denote by ϵ_{-d} the quadratic character of $(\mathbb{Z}/d\mathbb{Z})^*$ determined by $\epsilon_{-d}(p) = \left(\frac{-d}{p}\right)$ for primes p. Then

$$f \otimes \epsilon_{-d} = \sum_{m \geq 1} a_m \epsilon_{-d}(m) q^m,$$

the twist of f, is the weight-2, level-dividing-Nd^2 modular form of the $(-d)$-quadratic twist of the curve E, which we will denote by E_d; and $L(E_d, s) = L(f \otimes \epsilon_{-d}, s)$.

2000 AMS Subject Classification: Primary 11F33; Secondary 11Y70

Keywords: Elliptic curves, Tate-Shafarevich groups, modular forms

1058-6458/2006 $0.50 per page
Experimental Mathematics 15:3, page 355

A special case of Waldspurger's formula appears in [Gross 87] that relates the product $L(f,1)L(f\otimes\epsilon_{-d},1)$ to the squared d-coefficient of a weight-$\frac{3}{2}$ modular form g under Shimura correspondence to f.

Moreover, Gross states a procedure for calculating the weight-$\frac{3}{2}$ form g given the weight-2, level-N modular form f. This procedure comes from the connection between modular forms on $\Gamma_0(N)$ and the quaternion algebra B ramified at N and ∞.

Basically, one constructs the theta series associated with certain rank-3 lattices in the quaternion algebra. These theta series are then modular forms of weight $\frac{3}{2}$. The weight-$\frac{3}{2}$ modular form g corresponding to the weight-2 modular form f will be a linear combination of these, given by the coefficients of an eigenvector v of the Brandt matrices of level N.

We will briefly state this procedure, following the notation in [Gross 87]. Consider a maximal order R in the quaternion algebra B, ramified at N and ∞, and let $\{I_1,\dots,I_n\}$ be a set of left-ideal classes for the order R. Let R_i denote the right (maximal) order for the ideal I_i.

For each right order R_i, one constructs the theta series g_i of the following rank-three $\mathbb{Z}$-lattices: Define S_i^0 as the subgroup of elements of trace zero in the R_i-suborder $\mathbb{Z}+2R_i$. Let $\mathbb{N}$ denote the norm form, which is positive definite. Then define the theta series g_i by

$$g_i(\tau)=\frac{1}{2}\sum_{b\in S_i^0}q^{\mathbb{N}b}=\frac{1}{2}+\sum_{d>0}a_i(d)q^d,\quad i=1,\dots,n.$$

If t is the type number, that is, the number of distinct conjugacy classes of maximal orders in B, one gets t different theta series g_i (some are repeated).

These theta series are modular forms of weight $\frac{3}{2}$, level $4N$, and trivial character, and the coefficients a_d satisfy

$$a_d=0 \text{ unless } -d\equiv 0 \pmod 4 \text{ and } \left(\frac{-d}{N}\right)\neq 1. \quad (\star)$$

This is the Kohnen subspace of modular forms of weight $\frac{3}{2}$, which has dimension t and is stable under the Hecke algebra. The theta series lie in a lattice of rank t, denoted by M^*, which consists of those forms that in addition to satisfying $(\star)$, have integral coefficients, except (possibly) for a_0, which lies in $\frac{1}{2}\mathbb{Z}$.

1.1 Jacquet–Langlands Correspondence

Let N be a prime and $S_2(\Gamma_0(N))$ the space of cusp forms of weight 2 for the congruence subgroup $\Gamma_0(N)$. The Hecke operators T_p act on this space, and we are interested in eigenforms f:

$$f=\sum_{n=1}^{\infty}a_nq^n\quad(a_1=1),\qquad T_p(f)=a_pf.$$

To each of these modular forms f corresponds an eigenvector of the Brandt matrices of prime level N: there is a dimension-one space of eigenvectors v such that $B(N,p)v=a_pv$ for all primes p (and for all $n\in\mathbb{N}$).

Let $v=(v_1,\dots,v_n)$ be (up to a constant factor) the eigenvector of the Brandt matrices of prime level N corresponding to our $f\in S_2(\Gamma_0(N))$ coming from the elliptic curve E.

Define $e_f=(e_1,\dots,e_n)=(v_1/w_1,\dots,v_n/w_n)$, where w_i is one-half the number of units of the order R_i.

Then

$$g=\sum_{i=1}^{n}e_ig_i=\sum_{d>0}m_dq^d$$

is the weight-$\frac{3}{2}$ modular form that corresponds to the weight-2 modular form f. And this is the form involved in the Waldspurger formula, as related by Gross.

1.2 Waldspurger's Formula

Let N be a prime number, f a cusp form of weight 2 and trivial character for $\Gamma_0(N)$, and $f\otimes\epsilon_{-d}$ the twist of f by the character ϵ_{-d} of $(\mathbb{Z}/d\mathbb{Z})^*$ determined by $\epsilon_{-d}(p)=\left(\frac{-d}{p}\right)$ for primes p. For d a positive integer such that $-d$ is a fundamental discriminant and $\left(\frac{-d}{N}\right)\neq 1$, we have

$$L(f,1)\ L(f\otimes\epsilon_{-d},1)=k_N\,\frac{(f,f)\,m_d^2}{\sqrt{d}\langle e_f,e_f\rangle},$$

where $k_N=2$ if $d\equiv 0 \pmod N$ and is 1 otherwise, and (f,f) is the Peterson product. The product $\langle .,.\rangle$ is defined as follows: if $v=\sum_{i=1}^n v_ie_i$ and $u=\sum_{i=1}^n u_ie_i$, then

$$\langle v,u\rangle=\sum_{i=1}^{n}w_iv_iu_i.$$

2. RESTATEMENT AND PROCEDURE

Now we will restate the above formula in a more convenient way. We can replace the product (f,f) in the formula above if we take E to be a strong Weil curve and use the following result, which can be found in [Cremona 95]: Let $f(\tau)$ be a normalized new form of weight 2 for $\Gamma_0(N)$. The periods of $2\pi if(\tau)$ form in this case a lattice Λ_f, and the modular elliptic curve $E_f=\mathbb{C}/\Lambda_f$ is defined over $\mathbb{Q}$

and has conductor N. Let $\varphi : X = \Gamma_0(N)\backslash\mathcal{H}^* \longrightarrow E_f$ be the associated modular parameterization. Then

$$4\pi^2\|f\|^2 = \deg(\varphi)\,\mathrm{Vol}(E_f),$$

where

$$\|f\|^2 = \int_X |f(\tau)|^2 du\,dv, \quad \tau = u + iv.$$

If we write the lattice Λ_f as generated by $\Omega_f(1,\tau)$, where Ω_f is the real period of E_f, then

$$\mathrm{Vol}(E_f) = \Omega_f^2\,\mathrm{Im}(\tau),$$

where $\mathrm{Im}(z)$ denotes the imaginary part of z and $\mathrm{Vol}(E_f)$ is the volume of the lattice Λ_f. Replacing this in Waldspurger's formula and rearranging in a convenient way, we have

$$\frac{L(f,1)}{\Omega_f}\;\frac{L(f\otimes\epsilon_{-d},1)}{\frac{2\Omega_f\,\mathrm{Im}(\tau)}{\sqrt{d}}} = k_N\;\frac{\deg(\varphi)\,m_d^2}{\langle e_f, e_f\rangle},$$

for $\left(\frac{-d}{N}\right) \neq 1$,where $\deg(\varphi)$ is taken from Cremona's tables. The factor $\frac{L(f,1)}{\Omega_f}$ on the left is a rational number, which we can calculate with PARI-GP. The denominator $\frac{2\Omega_f\,\mathrm{Im}(\tau)}{\sqrt{d}}$ is "almost" the real period of the $(-d)$-twist of f, $f\otimes\epsilon_{-d}$. That is, it is a rational calculable multiple of it that depends sometimes on d modulo 8.

2.1 BSD: The Rank-Zero Case

For an elliptic curve E of rank zero, the Birch and Swinnerton-Dyer (BSD) conjecture states that

$$\frac{L(E,1)}{\Omega} = \frac{|Ш|\prod_p c_p}{|\,\mathrm{Tor}(E)|^2},$$

where $\mathrm{Tor}(E)$ is the torsion group of E, and Ω is the integral over $E(\mathbb{R})$ of the invariant differential ω. This is the real period of E or twice the real period, depending on whether the polynomial $p(x)$ defining E in $y^2 = p(x)$ has negative or positive discriminant.

For E_d, the $(-d)$-twist of the elliptic curve E, we have $L(E_f\otimes\epsilon_{-d},1) = L(E_d,1)$, and we substitute the equality above given by the BSD conjecture into Waldspurger's formula. We then have

$$\frac{L(E,1)}{\Omega}\;\frac{|Ш_d|\prod_p c_{p,d}}{|\,\mathrm{Tor}(E_d)|^2}\;q_d = \frac{k_N 2\deg(\varphi)m_d^2}{\langle e_f, e_f\rangle}.$$

The order of $\mathrm{Tor}(E_d)$ is constant. The factor q_d is the rational multiple that comes from the quotient $\Omega_d/\frac{\Omega_f\,\mathrm{Im}(\tau)}{\sqrt{d}}$. In calculated examples, q_d is the constant 2, or it equals 2 or 4 depending on the divisibility of d modulo 8. The quotient of $L(E,1)$, the period Ω, and the product of the fudge factors $\prod_p c_{p,d}$ can be calculated with PARI-GP.

This is the identity we use to calculate the order of $Ш_d$ for a family of imaginary quadratic twists of the elliptic curve E, having previously calculated the weight-$\frac{3}{2}$ modular form g:

$$g(\tau) = \sum_{d>0} m_d q^d.$$

Moreover, as is known, the order of the Tate–Shafarevich group is a square. Then we can get signed square roots of $Ш_d$ with the sign given by the m_d-coefficient of the weight-$\frac{3}{2}$ modular form g.

We will concentrate our attention on arithmetic aspects of the density distribution of the square roots of $|Ш|$ values obtained in the family of $(-d)$-quadratic twists of an elliptic curve E. There are relevant results concerning the distribution of values of L-series due to Conrey, Keating, Farmer, Rubinstein, Snaith, and Delaunay that will not be mentioned here. For references see [Conrey et al. 04, Delaunay 01].

3. AN EXAMPLE

We will write explicitly all calculations for the prime conductor $N = 17$. From Cremona's tables we see that there is one isogeny class of elliptic curves of conductor $N = 17$ and rank zero. We take the curve number one in the class, that is, the strong Weil curve, in order to use the above formula to calculate (f,f). This is, in the format $[a_1, a_2, a_3, a_4, a_6]$ given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

the curve $E = [1,-1,1,-1,-14]$; its torsion has four elements, and the degree of the modular parameterization φ is 1.

With this curve we have to associate a modular form g of weight $\frac{3}{2}$, which will be a linear combination of the theta series g_i of the lattices S_i^0 constructed from right orders R_i in the quaternion algebra ramified at 17 and ∞.

3.1 Calculation of the Theta Series g_i

For our calculations we used routines from A. Pacetti's `qalgmodforms` [Pacetti 01] for doing arithmetic over quaternion algebras and from G. Tornaria's `qftheta3` [Tornaria 04], both of which run under PARI-GP. We will employ the following notation: $[b_0, b_1, b_2, b_3]$ stands for $b_0 + b_1 i + b_2 j + b_3 k$ in the quaternion algebra.

First, we take a maximal order R in the quaternion algebra ramified at $N = 17$ and ∞ and calculate a set of representatives $I_1, \dots, I_n$ of left ideals for the order R. For each of these ideals I_i we calculate the right (maximal) orders R_i. We then take the trace-zero elements of the lattices $\mathbb{Z} + 2R_i$. The modular forms g_i will be the theta series of these lattices. This can be done in the following way with routines from the packages above: $\mathtt{qsetprime}(17)$ sets the quaternion algebra ramified at $N = 17$ and ∞, and returns a maximal order R in it:

$$R = \left[[\tfrac{1}{2}, 0, \tfrac{1}{2}, 0], [0, \tfrac{1}{2}, 0, \tfrac{1}{2}], [0, 0, \tfrac{1}{3}, \tfrac{1}{3}], [0, 0, 0, 1], 1\right].$$

Then qdef tells us which quaternion algebra we are in:

$$\mathtt{qdef} = [-17, -3].$$

That is, the quaternion algebra ramified at $N = 17$ and ∞ is

$$B = \{b_0 + b_1 i + b_2 j + b_3 k, b_i \in \mathbb{Q}, i^2 = -17, j^2 = -3\}.$$

We then have to calculate a set of representatives of left ideals for the maximal order R:

$$\begin{aligned}\mathtt{qidcl}(R) = \Bigg[\Big[& \left[\tfrac{1}{2}, 0, \tfrac{1}{2}, 0\right], \left[0, \tfrac{1}{2}, 0, \tfrac{1}{2}\right], \left[0, 0, \tfrac{1}{3}, \tfrac{1}{3}\right], \\ & [0, 0, 0, 1], 1\Big], \\ \Big[& [1, 0, 1, 0], [1, 0, -1, 0], \left[0, 0, \tfrac{-1}{3}, \tfrac{-1}{3}\right], \\ & \left[\tfrac{1}{2}, \tfrac{-1}{2}, \tfrac{1}{6}, \tfrac{1}{6}\right], 2\Big]\Bigg].\end{aligned}$$

Thus in this case, we have two different ideal classes. Then the class number n is 2, and the left ideals are

$$\begin{aligned} I_1 &= \left[\left[\tfrac{1}{2}, 0, \tfrac{1}{2}, 0\right], \left[0, \tfrac{1}{2}, 0, \tfrac{1}{2}\right], \left[0, 0, \tfrac{1}{3}, \tfrac{1}{3}\right], [0, 0, 0, 1], 1\right], \\ I_2 &= \Big[[1, 0, 1, 0], [1, 0, -1, 0], \left[0, 0, \tfrac{-1}{3}, \tfrac{-1}{3}\right], \\ &\qquad \left[\tfrac{1}{2}, \tfrac{-1}{2}, \tfrac{1}{6}, \tfrac{1}{6}\right], 2\Big]. \end{aligned}$$

Now we calculate the right orders: $R_i = \mathtt{qrorder}(I_i)$ gives a (maximal) right order for the ideal I_i:

$$\begin{aligned} R_1 &= \Big[[1, 0, 0, 0], \left[\tfrac{-1}{2}, 0, \tfrac{-1}{2}, 0\right], \left[\tfrac{-1}{2}, \tfrac{-1}{2}, \tfrac{1}{6}, \tfrac{1}{6}\right], \\ &\qquad \left[\tfrac{1}{2}, \tfrac{-1}{2}, \tfrac{-1}{6}, \tfrac{-1}{6}\right], 1\Big], \\ R_2 &= \Big[[1, 0, 0, 0], \left[\tfrac{-1}{2}, 0, \tfrac{1}{3}, \tfrac{-1}{3}\right], \left[\tfrac{-1}{2}, 0, \tfrac{2}{3}, \tfrac{1}{6}\right], \\ &\qquad \left[0, \tfrac{-1}{2}, \tfrac{-1}{2}, 0\right], 1\Big]. \end{aligned}$$

To calculate the lattices S_i^0 we have to take the trace-zero elements of $\mathbb{Z} + 2R_i$. The $\mathbb{Z} + 2R_i$ are generated by

$$\begin{aligned} \mathbb{Z} + 2R_1 &= \Big[[1, 0, 0, 0], [0, 0, -1, 0], \left[0, -1, \tfrac{1}{3}, \tfrac{1}{3}\right], \\ &\qquad \left[0, -1, \tfrac{-1}{3}, \tfrac{-1}{3}\right], 1\Big], \\ \mathbb{Z} + 2R_2 &= \Big[[1, 0, 0, 0], \left[0, 0, \tfrac{2}{3}, \tfrac{-1}{3}\right], \left[0, 0, \tfrac{4}{3}, \tfrac{1}{3}\right], \\ &\qquad [0, -1, -1, 0], 1\Big]. \end{aligned}$$

Then we have

$$\begin{aligned} S_1^0 &= \Big[[0, 0, -1, 0], \left[0, -1, \tfrac{1}{3}, \tfrac{1}{3}\right], \left[0, -1, \tfrac{-1}{3}, \tfrac{-1}{3}\right], 1\Big], \\ S_2^0 &= \Big[\left[0, 0, \tfrac{2}{3}, \tfrac{-1}{3}\right], \left[0, 0, \tfrac{4}{3}, \tfrac{1}{3}\right], \\ &\qquad [0, -1, -1, 0], 1\Big], \end{aligned}$$

and the corresponding theta series

$$g_i(\tau) = \frac{1}{2} \sum_{b \in S_i^0} q^{\mathbb{N}b} = \frac{1}{2} \sum_{x \in \mathbb{Z}^3} q^{x^t A_i x},$$

where A_i is one-half the matrix of the bilinear form $\mathrm{Tr}(x\overline{y})$ restricted to the lattice S_i^0. More precisely, if f_1, f_2, f_3 is a basis for the lattice L, then the matrix A is given by

$$A = \frac{1}{2} \mathrm{Tr}(f_i \overline{f_j}).$$

With $\mathtt{qgram}\,(S_i^0)/2$ we now have the corresponding quadratic forms: We calculate $A_i = \frac{1}{2}\mathtt{qgram}\,(S_i^0)$:

$$A_1 = \begin{bmatrix} 3 & -1 & 1 \\ -1 & 23 & 11 \\ 1 & 11 & 23 \end{bmatrix}; \quad A_2 = \begin{bmatrix} 7 & -3 & -2 \\ -3 & 11 & -4 \\ -2 & -4 & 20 \end{bmatrix}.$$

Now we have to calculate the coefficients of the series

$$g_i(\tau) = \frac{1}{2} \sum_{x \in \mathbb{Z}^3} q^{x^t A_i x}, \quad i = 1, 2.$$

These are computed by the routine $\mathtt{qfminim3}\,(A_i, b, 0, 3)$, which returns a small vector of length $b+1$ whose $(k+1)$th component is the number of elements of norm k, that is, the k-coefficient of the theta series given by the norm form A_i. Then we calculate ten million coefficients of the modular forms g_i with $\frac{1}{2}\mathtt{qfminim3}\,(A_i, 10000000, 0, 3)$.

3.2 Calculation of the Weight-$\frac{3}{2}$ Form g

Once we have these forms, we have to calculate the "right" linear combination of them. We need the number of units in R_i, which we calculate with $\mathtt{qrepnum}\,(R_i, 1)$. Then we have

$$\begin{aligned} w_1 &= \mathtt{qrepnum}\,(R_1, 1)/2 = 3, \\ w_2 &= \mathtt{qrepnum}\,(R_2, 1)/2 = 1. \end{aligned}$$

Now we look for the eigenvector of the Brandt matrices corresponding to the modular form f defined above: We know that there exists an eigenvector v of all the Brandt matrices of prime level 17 such that $B_p(v) = a_p v$ for all prime p. The eigenvalues a_p are the eigenvalues of the modular form f under the action of the Hecke operators T_p. We use the PARI-GP routine `ellap` (E, p) and calculate

$$a_2 = -1,\ \ a_3 = 0,\ \ a_5 = -2,\ \ a_7 = 4,\ \ \ldots .$$

Then we calculate the Brandt matrix B_2:

$$B_2 = \texttt{brandt}(R, 2) = \begin{bmatrix} 0 & 3 \\ 1 & 2 \end{bmatrix}.$$

Recall that R is our maximal order in the quaternion algebra ramified at 17 and ∞. Since $a_2 = -1$, we look for the kernel of

$$B_2 - (-\texttt{matid}(2)) = \begin{bmatrix} 1 & 3 \\ 1 & 3 \end{bmatrix}.$$

This kernel already has dimension one. Then any vector in it, for example $v = (-3, 1)$, will be eigenvector of all Brandt matrices with the required eigenvalues. If it did not have dimension one, we would need to intersect with the kernel of $B_3 - a_3 I$, and so on, until we obtained a dimension-one eigenspace.

Now we have the eigenvector $v = (-3, 1)$ and the values $w_1 = 3$, $w_2 = 1$. Then we set $e_f = (\frac{v_1}{w_1}, \frac{v_2}{w_2}) = (-1, 1)$, and the weight-$\frac{3}{2}$ modular form we want is

$$g = g_{\mathbf{17}} = \frac{v_1}{w_1} g_1 + \frac{v_2}{w_2} g_2 = -g_1 + g_2.$$

3.3 $|\text{Ш}_d|$ Formula

We want now to calculate the $|\text{Ш}|$ value of the $(-d)$-quadratic twists of E. If m_d is the d-coefficient of the modular form $g_{\mathbf{17}}$, then we know that

$$\frac{L(f,1)}{\Omega_f}\ \frac{L(f \otimes \epsilon_{-d}, 1)}{\frac{2\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}} = \frac{\deg(\varphi) m_d^2}{\langle e_f, e_f \rangle},$$

and we can calculate $\langle e_f, e_f \rangle = w_1 e_{f1}^2 + w_2 e_{f2}^2 = 3(-1)^2 + 1 \cdot 1^2 = 4$. From Cremona's tables we get $\deg(\varphi) = 1$. With PARI-GP we calculate $L(f,1)/\Omega_f = \frac{1}{4}$. So the term $L(f,1)/\Omega_f$ on the left cancels with $\deg(\varphi)/\langle e_f, e_f \rangle$ on the right.

The ratio $\Omega_d / \frac{2\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}$ does not depend on d, and we have

$$\Omega_d = 2\, \frac{\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}.$$

The polynomials $p_d(x)$ defining the equations of the twisted curves E_d have negative discriminant. So we have

$$\frac{L(f \otimes \epsilon_{-d})}{\frac{2\Omega_f \operatorname{Im}(\tau)}{\sqrt{d}}} = \frac{L(f \otimes \epsilon_{-d})}{\Omega_d} = \frac{|\text{Ш}_d| \prod_p c_{p,d}}{|\operatorname{Tor}(E_d)|^2}.$$

For the order of the group of torsion points of the $(-d)$-twists of E, we have $|\operatorname{Tor}(E_d)| = 2$.

Putting all this together gives us

$$|\text{Ш}_d| = \frac{4 m_d^2}{\prod_p c_{p,d}},$$

which gives us a way for calculating, with the coefficients of the form $g_{\mathbf{17}}$, the values of $|\text{Ш}_d|$. Moreover, since the order of Ш is known to be a square,

$$\sqrt{|\text{Ш}_d|} = \frac{m_d}{\sqrt{\frac{\prod_p c_{p,d}}{4}}}$$

gives us a signed square root of $|\text{Ш}_d|$ with the sign given by the coefficient m_d. This is what we have calculated for different elliptic curves of prime conductors and rank zero.

4. EXPERIMENT AND OBSERVATIONS

By the procedure described above, we can calculate the signed square root of the analytic value $|\text{Ш}_d|$ for the imaginary $(-d)$-quadratic twist E_d of a strong Weil curve E of prime conductor N and rank zero.

This has been done for curves of conductors $N = 11, 17, 19, 37, 67, 73, 89, 109, 139$ and for $N = 307$, this last one in the four existing isogeny classes of curves all of rank zero.

To be more precise, we pick a strong Weil curve E of prime conductor N and rank zero, and calculate between 3 and 10 million coefficients of the weight-$\frac{3}{2}$ modular form g associated with the weight-2 modular form f of the elliptic curve E.

For those d such that $(-d)$ is a fundamental discriminant and $\left(\frac{-d}{N}\right) \neq 1$ (that is, the sign of the functional equation is $+1$), we have by the Gross formula and the BSD conjecture that either both $L(E_d, 1)$ and m_d equal zero, or both are nonzero and we have a relationship $|\text{Ш}_d| = q_d^2 m_d^2$, where q_d is a rational number that involves the product of the fudge factors $c_{p,d}$. Then the (integer) number $q_d m_d$ is a signed square root of the order of the group Ш_d with the sign given by the coefficient m_d. We will denote this number by S_d:

$$\mathrm{S}_d = \begin{cases} q_d m_d & \text{if } L(E_d, 1) \neq 0, \\ 0 & \text{if } L(E_d, 1) = 0. \end{cases}$$

The zero coefficients m_d with $(-d)$ a fundamental discriminant and $\left(\frac{-d}{N}\right) \neq 1$ correspond to nontrivial zeros of $L(E_d, 1)$, so by counting these coefficients, we can obtain the density of curves E_d such that the L-function vanishes nontrivially at $s = 1$.

From this information we made graphs for the density distribution of the S_d values obtained (over all of the d's with $(-d)$ fundamental and $\left(\frac{-d}{N}\right) \neq 1$).

4.1 Observations

Conrey, Keating, Rubinstein, and Snaith [Conrey et al. 04] have obtained conjectures for the value distribution of the Fourier coefficients m_d based on conjectures from random-matrix theory for the value distribution of $L(E_d, 1)$. They observed that for primes p dividing the order of the torsion group of E, the probability that the Fourier coefficient m_d is divisible by p deviates from Delaunay's prediction for the probability of $|\text{Ш}|$ being divided by a given prime.

In [Rubinstein 02], Rubinstein makes a graph of the distribution of the coefficients m_d of the modular form of weight $\frac{3}{2}$, normalized by the product of the fudge factors, for the elliptic curve of conductor $N = 11$. He points out that in the histogram it is seen that primes 2 and 5 behave differently. He also compares the density of coefficients divided by primes p with Delaunay's prediction [Delaunay 01] for the probability of $|\text{Ш}|$ being divisible by p among elliptic curves of rank zero.

We will state here the observations we made from our experimental data and explain the density of S_d values divided by p when p is an odd prime that divides $|\operatorname{Tor}(E)|$. From the graphs, it is clear that there is a symmetry in the behavior of the positive and negative S_d values. The sign of S_d seems to play no role. For this reason we will sometimes restrict our attention to the positive part in further analysis.

In all examples, the density graphs split essentially into two, and this splitting corresponds to the parity of the S_d values. We get two density curves: one for odd values of S_d and one for even values. Further, when the base elliptic curve E has nontrivial torsion, these odd/even density curves also seem to "split" or have a "shadow" (see Figures 1 and 2).

The order of the group of torsion points of $E(\mathbb{Q})$ seems to affect the behavior of these graphs in the following manner.

1. Curves E with odd nontrivial torsion: For elliptic curves with conductors 11, 19, and 37, the groups of torsion points of $E(\mathbb{Q})$ have, respectively, orders $5, 3, 3$, and these are the only cases of nontrivial odd torsion (as for prime conductors, the order of the group of torsion points is one or two—for conductors 64 plus a square—except for the three cases above and for conductor 17, in which case the torsion is 4). For these three cases, we get two density curves that "split": those above correspond to odd values of S_d and those below to even values.

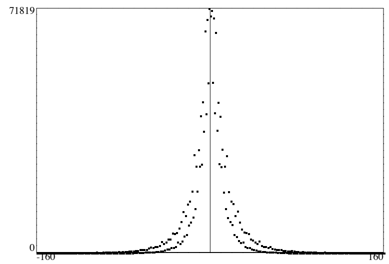

FIGURE 1. Density distribution of S_d for $N = 11$, $|\operatorname{Tor}(E)| = 5$.

Graphically, it is remarked that those values of Ш divided by the order of the group of torsion points have a larger density. What we mean by this is (from right to left) to choose a point in the density graph of (say) odd values for (say) conductor $N = 11$ that has a "slightly" greater density than its near points in the same "odd-value curve." The next point on the left with the same "property" will be the fifth, and so on. The same goes for $N = 19$, 67, and 3.

2. Curves E with trivial torsion: For conductors 67, 109, 139, and 307 the torsion group of the base elliptic curves E is trivial, and we get two well-differentiated density curves, separated into odd values of S_d for the upper density curve and even values of S_d for the bottom one.

3. Curves E with even torsion: The behavior for conductors 17, 73, and 89 is different. The odd/even density curves cross each other. The orders of the groups of torsion points of the elliptic curves are, respectively, 4, 2, and 2. In these cases, small even values of S_d have greater densities than the odd ones; then they are equal, and for larger values, odd S_d's have greater densities than even ones.

This "crossing" of the even/odd density curves is seen more clearly in the logarithmic graph, as shown in Figure 3. Here again, the odd/even density graph splits, with those S_d divided by $|\operatorname{Tor}(E)| = 4$ or 2, depending on the case, having greater densities than the remaining ones.

All of this raises the following question: are S_d values divided by 5 more frequent for $N = 11$ than for the other

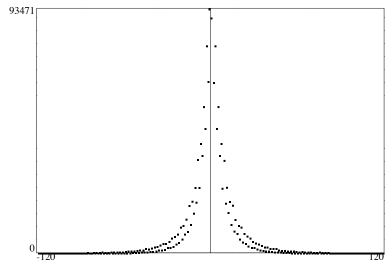

FIGURE 2. Density distribution of S_d for $N = 67$, $|\operatorname{Tor}(E)| = 1$.

conductors calculated? One has the same question for 3 and conductors $N = 19, 37$, for 4 and conductor $N = 17$, and for 2 and conductors $N = 73, 89$.

These questions are the motivation for Table 1, in which we calculated for each conductor the density of those values S_d divided by all the orders of the torsion groups as well as other small primes p.

In the table, T is the order of the group of torsion points, I denotes the isogeny class, and mult n stands for the density of curves E_d whose S_d value is a multiple of n. "Zeros" is the density of curves E_d with positive analytic rank, that is, the density of those curves in which the corresponding L-series vanishes nontrivially at the symmetry center $s = 1$ (recall that we are looking only at quadratic twists in which the sign of the functional equation is $+1$), and finally, m denotes the total number (in millions) of d's calculated.

CL is a Cohen–Lenstra heuristic on class numbers and **D** is Delaunay's heuristic for $|Ш|$ being divisible by a prime p. We will refer to this in the next sections.

This table is to be read by columns. For example, there is, in general, around 40% of even S_d values, and this percentage increases to 50% or more when the elliptic curve E has even torsion ($N = 17, 73, 89$). If we look at S_d values divided by 3, they are in the examples about 35%, except for conductors $N = 19, 37$, in which the group of torsion points has order 3 and this percentage increases to 40%. Something similar is seen for S_d values divided by 4 and 5.

We will now give heuristics for the density of Ш values divided by the order of the group of torsion points for conductors 11, 19, and 37 by the Cohen–Lenstra heuristics [Cohen and Lenstra 84] on class groups of number fields.

4.2 The Hurwitz Class Number

Let $-d$ be a negative discriminant and K the imaginary quadratic extension of $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{-d})$. Let $\mathcal{O}$ be an order of discriminant $-d$ in K, and denote by $h(\mathcal{O})$ the order of the finite group $\operatorname{Pic}(\mathcal{O})$ and by $u(\mathcal{O})$ the order of $\mathcal{O}^*/\mathbb{Z}^*$. Then $u(\mathcal{O}) = 1$ unless $d = -3, -4$, which give $3, 2$ respectively.

The Hurwitz class number is given by

$$H(d) = H(\mathcal{O}) = \sum_{\mathcal{O}\subset\mathcal{O}'\subset\mathcal{O}_{\mathcal{K}}} \frac{h(\mathcal{O}')}{u(\mathcal{O}')}.$$

As stated in [Gross 87], the prime N is used to define the modified invariant $H_N(d)$ by

$$H_N(d) = \begin{cases} 0 & \text{if } N \text{ splits in } \mathcal{O}, \\ H(\mathcal{O}) & \text{if } N \text{ is inert in } \mathcal{O}, \\ \frac{1}{2}H(\mathcal{O}) & \text{if } N \text{ is ramified in } \mathcal{O} \text{ but does not divide the conductor of } \mathcal{O}, \\ H_N(d/N^2) & \text{if } N \text{ divides the conductor of } \mathcal{O}, \end{cases}$$

which is zero unless $-d \equiv 0, 1 \pmod 4$ and $\left(\frac{-d}{N}\right) \neq 1$, and if $W = \prod_{i=1}^n w_i$, then $WH_N(d)$ is integral.

If d is such that $(-d)$ is a fundamental discriminant, then $\mathcal{O} = \mathcal{O}_{\mathcal{K}}$ and $H(\mathcal{O}_{\mathcal{K}}) = h_d/u(\mathcal{O}_{\mathcal{K}})$, where $\mathcal{O}_{\mathcal{K}}$ is the ring of integers in K and h_d is the class number. Furthermore, if we request that $\left(\frac{-d}{N}\right) \neq 1$, then N is either inert or ramifies in $\mathcal{O}_{\mathcal{K}}$ and then $H_N(d)$ becomes

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

Recall that $u(\mathcal{O}_{\mathcal{K}}) = 1$, except for exactly 2 values of d.

4.3 The Cohen–Lenstra Heuristics and $|Ш|$ Divisibility by 5 for Conductor $N = 11$

Let G be the weight-$\frac{3}{2}$ Eisenstein series defined by

$$G = \sum_{i=1}^{n} \frac{1}{w_i} g_i,$$

where g_i are the theta series of the lattices S_i^0 in the quaternion algebra ramified at N and ∞, and w_i is half the number of units of the right orders R_i, as stated previously.

Gross has proved that G has Fourier expansion

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

and mentions, for $N = 11$, the following congruence between the modular form of weight $\frac{3}{2}$, $g_{\mathbf{11}}$, and the weight-$\frac{3}{2}$ Eisenstein series $G_{\mathbf{11}}$:

$$2g_{\mathbf{11}} = -2g_1 + 2g_2 \equiv 3g_1 + 2g_2 = 6G_{\mathbf{11}} \pmod{5M^*}$$

N	T	I	zeros	mult 2	mult 3	mult 4	mult 5	mult 7	mult 11	m
11	5	A	0.042	0.369	0.353	0.185	0.234	0.146	0.097	10
17	4	A	0.079	0.592	0.353	0.303	0.210	0.156	0.115	10
19	3	A	0.065	0.371	0.407	0.189	0.206	0.150	0.105	3
37	3	B	0.054	0.440	0.413	0.223	0.207	0.149	0.101	10
67	1	A	0.058	0.403	0.355	0.204	0.208	0.150	0.103	10
73	2	A	0.086	0.539	0.356	0.269	0.212			3
89	2	B	0.072	0.507	0.354	0.257	0.209			3
109	1	A	0.076	0.391	0.322	0.199	0.208	0.153	0.109	3
139	1	A	0.073	0.394	0.354	0.192	0.209			3
307	1	A	0.091	0.390	0.354	0.200	0.210			3
307	1	B	0.087	0.405	0.354	0.208	0.210			3
307	1	C	0.076	0.391	0.354	0.199	0.207			3
307	1	D	0.071	0.401	0.354	0.205	0.209			3
D	-	-	-	**0.580**	**0.360**	-	**0.206**	**0.145**	**0.091**	
CL	-	-	-	-	**0.439**	-	**0.239**	**0.163**	**0.099**	
26	3	A	0.043	-	0.415	-	0.207	0.147	0.098	10
26	7	B	0.036	-	0.353	-	0.207	0.160	0.095	10

TABLE 1. Density of S_d values divisible by $2, 3, 4, 5, 7, 11$.

(where M^* is the lattice defined in Section 1), and in particular,

$$m_d \equiv 3H_{11}(d) \pmod 5.$$

We shall now use this congruence and the Cohen–Lenstra heuristics for class numbers to explain the density of $|Ш|$ divisible by 5 in the family of quadratic twists of the elliptic curve $[0, -1, 1, -10, -20]$ of conductor 11. The order of $Ш_d$ is given by m_d^2 divided by a power of 2. So the density of S_d values divided by 5 is the density of the m_d's divided by 5.

Denote by h_d the class number of the quadratic field $\mathbb{Q}(\sqrt{-d})$. Then the congruence above shows that

$$\{d : m_d \equiv 0 \pmod 5\} = \{d : h_d \equiv 0 \pmod 5\},$$

where both sets are taken over d's with $-d$ a fundamental discriminant and $\left(\frac{-d}{11}\right) \neq 1$. If we make the assumption that class number being divisible by a prime p and having a particular Kronecker symbol are independent facts, which at least numerically is so, then we have

$$\frac{|\{0 < d < X : h_d \equiv 0 \pmod 5 \text{ and } \left(\frac{-d}{11}\right) \neq 1\}|}{|\{0 < d < X : \left(\frac{-d}{11}\right) \neq 1\}|} \sim \frac{|\{0 < d < X : h_d \equiv 0 \pmod 5\}|}{|\{0 < d < X\}|}$$

as $X \to \infty$, where, as before, the sets are taken over d's such that $-d$ is a fundamental discriminant.

Here is where the Cohen–Lenstra heuristics come in [Cohen and Lenstra 84]. These are heuristics for the probability that the class number of a quadratic imaginary extension of $\mathbb{Q}$ is divisible by a prime p:

$$\lim_{X\to\infty} \frac{|\{0 < d < X : h_d \equiv 0 \pmod p\}|}{|\{0 < d < X\}|} = f(p),$$

where

$$f(p) = 1 - \prod_{i\geq 0}\left(1 - \frac{1}{p^i}\right) = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^7} + \cdots.$$

By the assumption made above we can say that $f(5) \approx 0.239$ is the probability of S_d being divisible by 5 among negative quadratic twists for conductor $N = 11$.

4.4 $|Ш|$ Divisibility by 3 for $N = 19$ and $N = 37$

This exact argument explains the density of Ш values divided by 3 for conductors $N = 19$ and $N = 37$, since the following congruence holds among the respective weight-$\frac{3}{2}$ modular form and Eisenstein series, for both conductors

$$g \equiv G \pmod{3M^*}.$$

Then we have in these two cases that the density of Ш values divisible by 3 is $f(3) \approx 0.439$.

This is general and can also be applied when the conductor N is not prime: if p is an odd prime that divides $|\operatorname{Tor}(E)|$, then the density of $|Ш| \equiv 0 \pmod p$ in the family of negative quadratic twists of E is given by the Cohen–Lenstra heuristics on class numbers in quadratic imaginary extensions of $\mathbb{Q}$ being divisible by p. We are still working out the details and will return to the topic in the future.

In order to compare data, in Table 1 we have calculated the densities of $|Ш|$ divisible by p for curves 26A and 26B (as in Cremona's tables), which have, respectively, groups of torsion points of orders 3 and 7. The ternary forms and linear combination that gives the weight-$\frac{3}{2}$ modular forms have been taken from Tornaria's data [Tornaria 04]. We restricted for simplicity to d's coprime to the conductor, and we have an additional restriction on the sign of $\left(\frac{-d}{p}\right)$ for primes p dividing N. Only these can be obtained by this method.

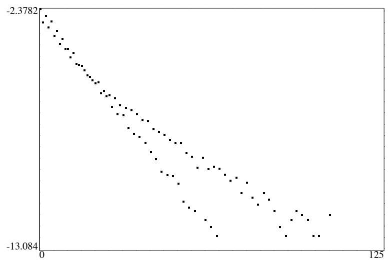

FIGURE 3. Logarithmic graph for curve E of conductor $N = 17$ of even torsion.

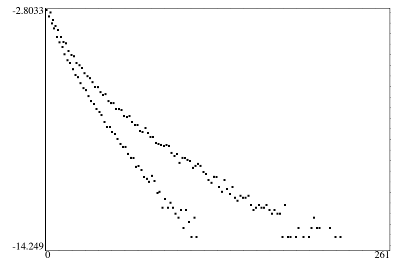

FIGURE 4. Logarithmic graph for conductor $N = 67$.

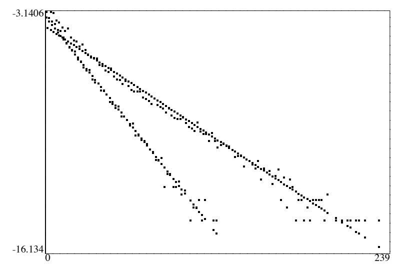

FIGURE 5. Logarithmic graph and best linear approximation for conductor $N = 11$.

It is clearly seen that $p = 3$ and $p = 7$ have bigger density for curves 26A and 26B respectively, and though the size of the experiment is rather small, these densities are not far from Cohen–Lenstra's prediction. We did not take into account $p = 2$, since we have not divided by the fudge factors to obtain the order of Ш.

For completeness we also compared our results with Delaunay's heuristics for the probability of the order of Ш being divided by a prime p. We remark that Delaunay's heuristics are for elliptic curves of rank zero, ordered by conductor. However, for small odd primes p this prediction seem to be applicable to families of even-rank negative quadratic twists of an elliptic curve. This density is denoted by $\mathbf{D}$ in Table 1. Although for $p = 2$ this prediction does not seem to apply, since in general the density of even values of Ш is less than 50%, it does seem to be applicable for $N = 17$. If we are to suppose that if a prime p divides $\text{Tor}(E)$ then the density of $|\text{Ш}|$ values divided by p is bigger than if it does not, then this case goes in the same direction, since the group of torsion points of E is of order 4.

4.5 More Observations

Our next question refers to the nature of the density curves. In trying to understand the density distribution and expecting an exponential type, we made graphs for the logarithm of positive S_d values. In the logarithmic graphs one can see clearly the consequences of the previous assertion about the curves corresponding to even and odd values of S_d crossing each other (see Figure 3) for twists of elliptic curves E of even torsion, instead of the typical situation of odd S_d values remaining above even ones.

Though for the first examples calculated ($N = 11, 17, 19, 37$), these logarithmic density graphs seemed to behave linearly for even values of S_d, for $N = 67$ this was not the case. In other examples ($N = 73, 89, 109, 139, 307$), it is seen that we cannot assume a linear behavior, since for small values of S_d we get a (greater or lesser) separation (above) from the line. Instead, it is clear that the logarithm of odd S_d values is not linear, having greater densities for small values and aligning with the even-S_d graph. There is one exception to this, for conductor $N = 37$, in which both even and odd logarithmic values behave almost linearly. We observe, for what it's worth, that this elliptic curve is the only one in the examples analyzed that has two connected components over the real numbers.

The typical situation for curves E of trivial or odd torsion is shown in Figures 4 and 5. The situation is the same for density logarithmic graphs of curves E of even torsion.

4.6 About Theta Series

Graphs have been made for densities of the coefficients a_d of each of the weight-$\frac{3}{2}$ theta series g_i involved in the linear combination that gives the theta series g associated with the elliptic curve E. Most of the coefficients are zero. Between the nonzero ones there is no evidence of the order of the group of torsion points of the elliptic curve E in the density of the coefficients divided by $2, 3, 4, 5$ as in the S-values, even if we restrict to those d's that are fundamental discriminants and with the correct Kronecker symbol.

It is surprising, however, that for conductor 11 the density distribution for the coefficients of one of the theta series is a graph that separates into five density curves, which is the order of the group of torsion points. Odd

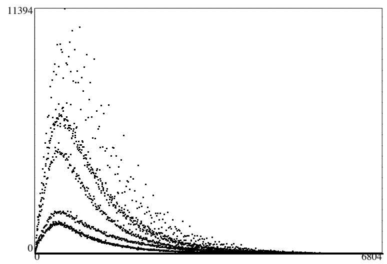

FIGURE 6. Density distribution of theta coefficients g_1; ternary form has four automorphisms, E of conductor 11.

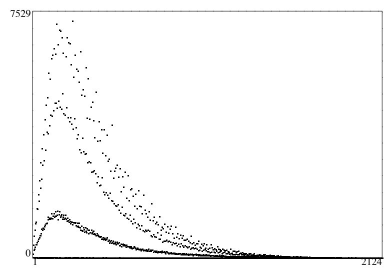

FIGURE 7. Density distribution of theta coefficients g_1; ternary form has four automorphisms, E of conductor 19.

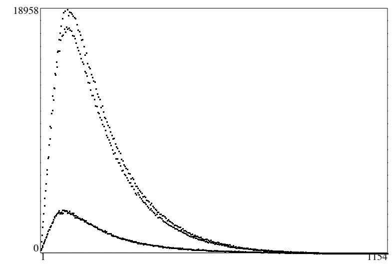

FIGURE 8. $N = 67$, coefficient density for theta series of ternary form with two automorphisms.

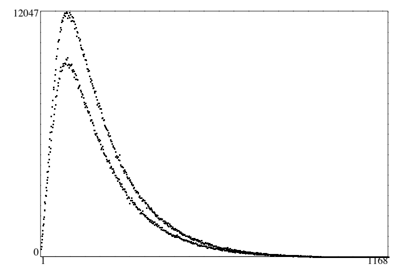

FIGURE 9. $N = 67$, coefficient density for theta series of ternary form with one automorphism.

coefficients are insignificant, and the even ones split according to their congruence modulo 24. The same occurs for $N = 19$ and 37: the graph for the density distribution of the coefficients of the theta series splits into three, corresponding to the congruence of the coefficients modulo 8 or 4 (depending on the case). For $N = 17$ we also have a graph that splits into five density curves, similar to that for conductor 11, according to congruency modulo 24.

The only difference we can point out at the moment in the examples calculated is that when the order of the group of torsion points of E is greater than 2, we obtain "cloudy" graphs.

When the elliptic curve E has torsion 1 or 2, the situation in the examples calculated seems to be clearer. We get neat graphs and the shapes of these density coefficient graphs seem to depend on the number of automorphisms of the corresponding ternary form. The density graphs for nonzero coefficients divide essentially in two, depending on the number of automorphisms of the ternary form involved. For ternary forms that have one automorphism, the coefficients split essentially into even/odd ones, with major density for the even ones. For two automorphisms, odd coefficients are in a much lower proportion than even ones. The density curve for the even coefficients splits in two, depending on congruence modulo 4. For four automorphisms, odd coefficients are in an insignificant proportion. The typical situation is exemplified in Figures 8 and 9 for a curve E of conductor $N = 67$ of torsion 1. All these graphs can be found online at http://www.expmath.org/expmath/volumes/15/15.3/quattrini/.

Of the graphs available at the web site, `twist`N`rtshadist.ps` gives the density distribution of the signed square roots of Ш for the elliptic curve of conductor N with sign given by the d-coefficient m_d. The graphs for the density distribution of the coefficients of the theta series g_i are in `twist`N`distgi.ps`. The theta series are numbered accordingly with ternary forms, which we do not give explicitly here, but they are at the web site. The graph `twist`N`distg.ps` gives the coefficient distribution of the linear combination g that corresponds to f.

REFERENCES

[Cohen and Lenstra 84] H. Cohen and H. W. Lenstra, Jr. "Heuristics on Class Groups of Number Fields." In *Number Theory*, edited by H. Jager, pp. 33–62, Lecture Notes in Math. 1068. Berlin: Springer-Verlag, 1984.

[Conrey et al. 04] J. B. Conrey, J. P. Keating, M. O. Rubinstein, and N. C. Snaith. "Random Matrix Theory and the Fourier Coefficients of Half-Integral Weight Forms." arXiv:math.NT/0412083 v2, 2004.

[Cremona 95] J. E. Cremona. "Computing the Degree of the Modular Parametrization of a Modular Elliptic Curve." *Math. Comp.* 64:211 (1995), 1235–1250.

[Delaunay 01] C. Delaunay. "Heuristics on Tate–Shafarevitch Groups of Elliptic Curves Defined over $\mathbb{Q}$." *Exper. Math.* 10:2 (2001), 191–196,

[Gross 87] B. Gross. "Heights and the Special Values of L-Series." In *CMS Conference Proceedings* 7. Providence: American Math. Soc., 1987.

[Pacetti 01] A. Pacetti. "Qalgmodforms." Available online (http://www.ma.utexas.edu/users/villegas/cnt/cnt-frames.html), 2001.

[Pizer 80] A. Pizer. "An Algorithm for Computing Modular Forms on $\Gamma_0(N)$." *Journal of Algebra* 64 (1980), 340–390.

[Rubinstein 02] M. O. Rubinstein. Private communication, 2002.

[Shimura 73] G. Shimura. "On Modular Forms of Half Integral Weight." *Ann. Math. Sec. Ser.* 97:3 (1973), 440–481.

[Tornaria 04] G. Tornaria. "Data about the Central Values of the L-Series of (Imaginary and Real) Quadratic Twists of Elliptic Curves." Available online (http://www.ma.utexas.edu/users/tornaria/cnt), 2004.

Patricia L. Quattrini, Universidad de Buenos Aires, Departamento de Matematica, FCEyN, Pab. I, Ciudad Universitaria, 1428 Buenos Aires, Argentina (pquattri@dm.uba.ar)

Received March 3, 2005; accepted October 6, 2005.