COMPUTING CENTRAL VALUES OF L-FUNCTIONS

1.

How fast can we compute the value of an L-function at the center of the critical strip?

We will divide this question into two separate questions while also making it more precise. Fix an elliptic curve E defined over $\mathbb{Q}$ and let $L(E,s)$ be its L-series. For each fundamental discriminant D let $L(E,D,s)$ be the L-series of the twist E_D of E by the corresponding quadratic character; note that $L(E,1,s) = L(E,s)$.

A. How fast can we compute the central value $L(E,1)$?
B. How fast can we compute $L(E,D,1)$ for D in some interval say $a \le D \le b$?

These questions are obviously related but, as we will argue below, are not identical.

We should perhaps clarify what *to compute* means. First of all, we know, thanks to the work of Wiles and others, that $L(E,s) = L(f,s)$ for some modular form f of weight 2; hence, $L(E,s)$, first defined on the half-plane $\Re(s) > 3/2$, extends to an analytic function on the whole s-plane which satisfies a functional equation as s goes to $2-s$. In particular, it makes sense to talk about the value $L(E,1)$ of our L-function at the center of symmetry $s=1$. The same reasoning applies to $L(E,D,s)$.

As a first approximation to our question we may simply want to know the real number $L(E,D,1)$ to some precision given in advance; but we can expect something better. The Birch–Swinnerton-Dyer conjectures predict a formula of type

$$L(E,D,1) = \kappa_D\, m_D^2, \tag{1}$$

for some integer m_D and κ_D an explicit easily computable positive constant. (Up to the usual fudge factors the conjectures predict that m_D^2, if non-zero, should be the order of the Tate–Shafarevich group of E_D.) To compute $L(E,D,1)$ would then mean to calculate m_D *exactly.*

In fact, formulas à la Waldspurger have the form (1) with m_D the $|D|$-th coefficient of a modular form g of weight $3/2$ which is in Shimura correspondance with f. The main point of this note is to discuss informally how explicit versions of such formulas can be used for problem **B** above.

Let us also note the interesting fact that m_D, being related to the coefficient of a modular form, typically does not have a constant sign. The significance of the extra information provided by $\operatorname{sgn}(m_D)$ remains a tantalizing mystery.

2.

There is a standard analytic method to compute $L(E,1)$, which we now recall. If E has conductor N then the associated modular form f has level N and

$$f|_{w_N} = -\varepsilon f,$$

where w_N is the Fricke involution and ε is the sign of the functional equation for $L(E,s)$. Concretely, we have

$$f\left(\frac{i}{\sqrt{N}t}\right) = \varepsilon t^2 f\left(\frac{it}{\sqrt{N}}\right), \qquad t \in \mathbb{R}.$$

It follows that

$$\left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s)L(f,s) = \int_0^\infty f\left(\frac{it}{\sqrt{N}}\right) t^s \,\frac{dt}{t}.$$

Now break the integral as $\int_0^1 + \int_1^\infty$, make the substitution $t \mapsto 1/t$ in the first and use the functional equation to obtain

$$\left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s)L(f,s) = \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right) t^s \,\frac{dt}{t} + \varepsilon \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right) t^{2-s} \,\frac{dt}{t}.$$

(This is the classical argument to prove the functional equation of $L(E,s)$ and goes back to Riemann who used it for his zeta function.)

Now plug in $s = 1$ to get

$$\frac{\sqrt{N}}{2\pi} L(E,1) = (1+\varepsilon) \sum_{n \geq 1} \frac{a_n}{n} \, e^{-2\pi n/\sqrt{N}} \tag{2}$$

where f has Fourier expansion

$$f = \sum_{n \geq 1} a_n \, q^n, \qquad q = e^{2\pi i z}.$$

Assume for simplicity that $\gcd(N,D) = 1$. Then the conductor of E_D is ND^2 and (2) applied to E_D yields, more generally,

$$\frac{|D|\sqrt{N}}{2\pi} L(E,D,1) = (1+\varepsilon_D) \sum_{n \geq 1} \left(\frac{D}{n}\right) \frac{a_n}{n} \, e^{-2\pi n/|D|\sqrt{N}}, \tag{3}$$

with ε_D the sign in the functional equation of $L(E,D,s)$.

We know that $|a_n|$ grows no more than polynomially with n (a straightforward argument gives $|a_n| = O(n)$). It follows that for a fixed E and varying D we will need to take, very roughly, of the order of $O(|D|)$ terms in the sum to obtain a decent approximation to $L(E,D,1)$. Assuming the Birch–Swinnerton-Dyer conjectures we may use (3) to compute m_D^2 in (1) exactly. However, if we know that m_D is the D-th coefficient of some specific modular form (i.e. we have a formula à la Waldspurger) we would get $|m_D|$ but would not be able to recover $\operatorname{sgn}(m_D)$.

Using this method to compute, say, $L(E,D,1)$ for $|D| \leq X$ would take time of the order of $O(X^2)$. We will see below that using formulas of type (1) we can reduce this to $O(X^{3/2})$ for at least some fraction of such D's.

3.

Before tackling $L(E,D,1)$ let us consider the case of the special value of an Eisenstein series of weight 2 (as opposed to a cusp form as we have for $L(E,D,1)$). What follows is meant only as an illustration of the general case.

Let the L-function be $L(\left(\frac{D}{\cdot}\right), s-1)L(\left(\frac{D}{\cdot}\right), s)$ with $D < 0$ the discriminant of an imaginary quadratic field K. Its value at $s = 1$ is essentially $h(D)^2$, where $h(D)$ is the class number of K, and we find an analogue of (1) with $h(D)$ playing the role of m_D. There are many excellent algorithms for computing the class number $h(D)$

(see for example [1] chap. 5). Unfortunately, these do not obviously generalize to the calculation of m_D. The main reason for this is that the class group of K is easy to describe (both its elements and the group operation) in terms of binary quadratic forms, whereas its elliptic analogue, the Tate-Shafarevich group of E_D, is notoriously intractable.

The standard analytic method of the previous section yields the following formula (which was known to Lerch, see [2] vol. III, p. 171)

$$h(D)^2 = \frac{w_D^2\sqrt{|D|}}{2\pi} \sum_{n\geq 1} \left(\frac{D}{n}\right) \frac{\sigma(n)}{n}\, e^{-2\pi n/|D|}, \tag{4}$$

where w_D is the number of units in K and $\sigma(n) := \sum_{d|n} d$ is the divisor sum function. Again, we need to take, roughly, $O(|D|)$ number of terms in the sum to obtain a reasonable approximation of the left hand side. In this case, we in fact have an *exact* formula requiring D terms, namely, Dirichlet's class number formula

$$h(D) = -\frac{w_D}{2|D|} \sum_{n=1}^{|D|-1} n \left(\frac{D}{n}\right). \tag{5}$$

Neither one of these formulas is, however, particularly useful for computing $h(D)$ in practice. On the other hand, it may be worth pointing out that similar arguments yield the formula [2] vol. III, p. 153.

$$h(D) = w_D \sum_{n\geq 1} \left(\frac{D}{n}\right) \frac{1}{1-(-1)^n e^{\pi n/\sqrt{|D|}}}, \qquad D \equiv 5 \bmod 8,$$

with the number of necessary steps now reduced to the order of $O(\sqrt{|D|})$. (Analogous formulas can be given for D in other congruence classes modulo 8.)

To make the connection to the general case of computing $L(E, D, 1)$ that we are considering we mention two other possible approaches to computing $h(D)$ that do generalize.

(I) The first is to follow Gauss and realize ideal classes of K as classes of primitive, positive definite binary quadratic forms of discriminant D. Each class has a unique representative $Q = (a, b, c)$ in the standard fundamental domain (what is known as a *reduced form*) and we can simply enumerate these. A straightforward algorithm is as follows: run over values of b with $b \equiv D \bmod 2$ and $0 \leq b \leq \sqrt{|D|/3}$; for each b decompose $(b^2 - D)/4$ as ac with $0 < a \leq c$. Add one or two to the total count as the case may be if $\gcd(a, b, c) = 1$.

Though this algorithm also takes time $O(|D|)$ the constant of proportionality is very small making the algorithm quite practical. An important point to notice for our purpose, however, is that if we wanted to compute $h(D)$ for $0 \leq |D| \leq X$ we may simply run over all triples a, b, c of size at most $\sqrt{X/3}$ checking the necessary conditions on (a, b, c) for it to be a reduced form. In this way we obtain an algorithm which will run in time $O(X^{3/2})$.

(II) The second approach is again to follow Gauss but in a different direction. He proved that $h(D)$ is related to the number of representations of $|D|$ as a sum of three squares. One precise form of this relation is the following identity (see [3] p.177)

$$\frac{1}{2}\sum_{x\equiv y\equiv z \bmod 2} q^{x^2+y^2+z^2} = \frac{1}{2} + 12\sum_{D} H_2(D)\, q^{|D|} \tag{6}$$

where D runs through all negative discriminants (i.e. $D < 0$ and $D \equiv 0, 1 \bmod 4$), and H_2 is a variant of the Hurwitz class number (see [3], page 120). (For us it suffices to know that it is related to $h(D)$; for example for $D \equiv 5 \bmod 8$ a fundamental discriminant we have $H_2(D) = h(D)$.)

There are sophisticated techniques for computing the coefficients of the left hand side, such as *convolution* which uses the fast Fourier transform to compute products of q-series. But even a simple enumeration of the lattice points $x^2+y^2+z^2 \leq X, x \equiv y \equiv z \bmod 2$ would again take time $O(X^{3/2})$.

The two approaches (I) and (II) are of course related; they amount to *counting* (in an appropriate sense) the number of representations of D by a certain ternary quadratic form. In case (I) we count the number of solutions to $b^2 - 4ac = D$ up to $SL_2(\mathbb{Z})$-equivalence; in (II), the number of solutions to $|D| = x^2 + y^2 + z^2$ with $x \equiv y \equiv z \bmod 2$. Note the crucial difference that the ternary quadratic form involved is indefinite in case (I) and positive definite in case (II).

A more geometrical point of view is to think that we are dealing with *Heegner points*. In case (I) we may associate to a primitive positive definite binary quadratic form $Q = (a, b, c)$ the point $z_Q = (-b + \sqrt{D})/2a$ in the upper half plane $\mathcal{H}$. The respective actions of $SL_2(\mathbb{Z})$ on forms and $\mathcal{H}$ are compatible; hence, the class of Q determines a unique (Heegner) point in $SL_2(\mathbb{Z})\backslash\mathcal{H}$ of discriminant D.

It is a bit less intuitive how to think of Heegner points in case (II) but this was worked out by Gross [3]. The main ingredient is a positive definite quaternion algebra B over $\mathbb{Q}$ ramified, say, at ∞ and a prime N. Pick a maximal order R of B and let $I_1, \ldots, I_n$ be representatives for the (left) ideal classes of R. Let R_i be the right order of I_i for $i = 1, \cdots, n$.

Fix an imaginary quadratic field K of discriminant D. Then we can think of a Heegner point of discriminant D (what Gross calls a *special point*) as an (optimal) embedding of the ring of integers $\mathcal{O}_K$ into some R_i. Eichler has proved that the total number of such points, each counted up to conjugation by $R_i^\star$, is $(1 - \left(\frac{D}{N}\right))h(D)$. (In fact, the situation is quite analogous to that of case (I) if we take the *indefinite* algebra $B = M_2(\mathbb{Q})$ and $R = M_2(\mathbb{Z})$.)

For example, if $N = 2$ then the algebra B is the usual Hamilton quaternions and we may pick R to be the order discovered by Hurwitz (in standard notation)

$$R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\tfrac{1}{2}(1 + i + j + k).$$

In this case there is only one class of left R-ideals represented by R itself. Hence a Heegner point is an embedding $\phi : \mathcal{O}_K \to R$.

How do we find such embeddings? The main thing we need is a $w \in R$ with $w^2 = D$. Such a quaternion, because D is a scalar, necessarily has trace $t(w) = 0$ and norm $n(w) = -D$ and conversely. Elements of trace 0 in R form a rank 3 lattice and hence $n(w) = -D$ is a representation of D by a certain ternary quadratic form associated to R. A few congruence conditions are needed to actually produce an optimal embedding ϕ out of w but the upshot is that the problem becomes one about representations of $-D$ by ternary quadratic forms. For example, in the case $N = 2$ Eichler's count of embeddings can be completely encoded in the identity

(6); the presence of the factor 12 in that formula is due to the fact that this is the order of $R^\star/\pm 1$. More details on this setup are given below in §4 (II).

4.

We now return to the main case of computing $L(E, D, 1)$ and describe analogues of cases (I) and (II) of the previous section. These analogues are the remarkable results of Gross and Zagier.

(I) Let us assume for simplicity that E has conductor a prime N, sign of the functional equation equal to -1, $L'(E,1) \neq 0$, and $E(\mathbb{Q}) = \langle P_0 \rangle$. If f is the weight 2 eigenform associated to E then we get a map

$$\Phi: \quad \begin{array}{ccc} X_0(N) & \longrightarrow & \mathbb{C}/L \\ z & \mapsto & 2\pi i \int_{i\infty}^{z} f(u)\, du \end{array} \tag{7}$$

where $X_0(N)$ is the modular curve of level N and $L \subset \mathbb{C}$ is a certain lattice of periods of f. It is known that $\mathbb{C}/L = E'(\mathbb{C})$ for some elliptic curve $E'/\mathbb{Q}$ isogenous to E. Since the L-function is unchanged by isogenies we may assume without loss of generality that $E' = E$.

Let K be an imaginary quadratic field of discriminant $D < -4$ in which N splits. Choose $b_* \in \mathbb{Z}$ such that $b_*^2 \equiv D \bmod N$; this is possible by the assumption that N splits in K. Note also that N does not divide b_*. We want to consider Heegner points on $X_0(N)$ of discriminant D. To define them concretely choose representatives $Q = (a, b, c)$ of the $h(D)$ classes of binary quadratic forms with $N \mid a$ and $b \equiv b_* \bmod N$. (For example, start with representatives (a, b, c) with $\gcd(a, N) = 1$ and compose them with the fixed form $(N, b_*, (b_*^2 - D)/2N)$.)

Then $z_Q := (-b + \sqrt{D})/2/a) \in X_0(N)$ is well defined and $P_D := \sum_Q \Phi(z_Q) \in E(K)$. Moreover, complex conjugation fixes P_D, by the assumption on the sign of the functional equation. Hence P_D actually is in $E(\mathbb{Q})$ (and is independent of the choice of b_*).

One consequence of the results of Gross–Zagier is the following [15],[4], [5]. By our assumption on $E(\mathbb{Q})$ we have $P_D = m_D P_0$ for some $m_D \in \mathbb{Z}$ and hence

$$L(E, D, 1) = \kappa_D m_D^2; \tag{8}$$

where κ_D is an explicit easily computable positive constant; i.e. we have a formula of type (1).

Usually one regards the Gross-Zagier formula as a way to compute a rational point P_D on E whose height is given in terms of $L(E, D, 1)L'(E, 1)$ and hence obtaining, when this value does not vanish, a confirmation of the predictions of the Birch–Swinnerton-Dyer conjecture. Here, instead, we are taking the point of view that the points of $E(\mathbb{Q})$ are known and use the Gross–Zagier formula as a means to computing $L(E, D, 1)$.

To calculate m_D in practice it is better to work on the $E(\mathbb{C}) = \mathbb{C}/L$ model of E rather than, say, a Weierstrass equation. Let $z_0 \in \mathbb{C}$ represent, modulo L, the point $P_0 \in E(\mathbb{Q})$. We first compute an approximation to

$$z_D := \sum_Q \sum_{n \geq 1} \frac{a_n}{n} e^{2\pi i n z_Q}.$$

Then we solve the linear equation below for integers n_1 and n_2

$$z_Q = m_D z_0 + n_1 \omega_1 + n_2 \omega_2,$$

where ω_1, ω_2 are a basis for L. (In fact, multiplying by 2 if necessary, we may assume that $\omega_1 \in \mathbb{R}$ and $\omega_1 \in i\mathbb{R}$ and hence by taking real parts solve only a three term equation instead.)

The result is a practical and reasonably efficient algorithm for computing m_D. The number m_D is the D-th Fourier coefficient of a weight 3/2 modular form g of level $4N$ which is in Shimura correspondence with f. It is interesting that we can compute the Fourier coefficients of g directly without any knowledge of the whole vector space of modular forms in which g lies; though we do, of course, start by knowing f itself. (We have only described the calculation for certain D's but there is analogous way to get all coefficients.)

Together with my student Ariel Pacetti we implemented the above algorithm in GP. The corresponding routines can be found at

`http://www.ma.utexas.edu/users/villegas/cnt/`

under Heegner points.

Here is a sample example. Let E be the curve $y^2 + y = x^3 - x$ of conductor $N = 37$ (this is the elliptic curve over $\mathbb{Q}$ of positive rank with smallest conductor). This case was described in detail in [15]. It is known that $E(\mathbb{Q}) = \langle (0,0) \rangle$.

```
? e=ellinit([0,0,1,-1,0]);  anvec=ellan(e,5000);
? for(d=5,100, if(isfundamental(-d) && kronecker(-d,37)==1,
          print(-d," ",ellheegnermult(e,-d,[0,0],0,anvec)[1])))

-7  -11 -40 -47 -67  -71 -83  -84 -95
 1   -1  -2   1  -6   -1   1    1   0
```

The first row is D, the second m_D (for typographical reasons we transposed the actual GP output). These values agree, fortunately, with Zagier's [15] formula (28) up to a global negative sign.

In our implementation at least the algorithm is not that well suited for computing $L(E, D, 1)$ for all $D < 0$ and $|D| < X$ for very large X; for this, it would be better to adapt (see §5) the ideas of (II) below but these have not been fully implemented as yet.

(II) Let B over $\mathbb{Q}$ be the (unique up to isomorphism) positive definite quaternion algebra ramified at ∞ and a prime N. Pick a maximal order R of B and let $I_1, \ldots, I_n$ be representatives for the (left) ideal classes of R. Let R_i be the right order of I_i for $i = 1, \cdots, n$. The class number n of R, in contrast with $h(D)$, has a simple formula and is roughly of size $N/12$.

For example, if $N \equiv 3 \bmod 4$ we can describe B as the algebra over $\mathbb{Q}$ with generators i, j such that $i^2 = -1, j^2 = -N$ and $ij = -ji$. Also in this case we can take $R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1}{2}(1+j) + \mathbb{Z}i\frac{1}{2}(1+j)$.

There are various ways to compute representatives $I_1, \cdots, I_n$ of the ideal classes (for algorithms for quaternion algebras see [11]). If $N \equiv 3 \bmod 4$ there is an algorithm which is completely analogous to that of Gauss §3 (I) for binary quadratic forms. It exploits the fact that our choice of R has an embedding of $\mathbb{Z}[i]$ and hence allows us to view R-left ideals as rank 2 modules over $\mathbb{Z}[i]$; then classes of R-ideals correspond to classes of positive definite binary Hermitian forms over $\mathbb{Z}[i]$ of discriminant $-N$. Instead of $\mathcal{H}$ we now need to work on hyperbolic 3-space where, as it turns out, the action of $SL_2(\mathbb{Z}[i])$ has a very simple fundamental domain. This yields an algorithm which is almost verbatim that of Gauss for binary forms over $\mathbb{Z}$. Details can be found in [12].

For example, if $N = 11$ then there are two classes of positive definite binary Hermitian forms of discriminant -11 over $\mathbb{Z}[i]$; namely, $(1, 1, 3)$ and $(2, 1 + 2i, 2)$ corresponding to the two ideals

$$I_0 := R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\tfrac{1}{2}(1 + j) + \mathbb{Z}i\tfrac{1}{2}(1 + j)$$

and

$$I_1 := 2\mathbb{Z} + \mathbb{Z}2i + \mathbb{Z}\tfrac{1}{2}(1 + 2i + j) + \mathbb{Z}i\tfrac{1}{2}(1 + 2i + j)$$

representing the $n = 2$ classes of left R-ideals.

Let $V_{\mathbb{Q}}$ be the $\mathbb{Q}$ vector space of functions on the set $\{I_0, \ldots, I_n\}$. For each $m \in \mathbb{Z}_{\geq 0}$ there is an operator $B(m)$ acting on $V_{\mathbb{Q}}$, the Brandt matrix of order m, which encodes the number of representations of m by certain quaternary quadratic forms (see [3] (1.4)). Let $\mathbb{B}$ be the algebra generated over $\mathbb{Z}$ by all the $B(m)$; it is commutative and $\mathbb{B} \otimes_{\mathbb{Z}} \mathbb{Q}$ is semisimple.

On the other hand, we have the space $M_{\mathbb{C}}$ of modular form of weight 2 on $\Gamma_0(N)$ (known to be of dimension n) and the Hecke operators T_m acting on $M_{\mathbb{C}}$. Let $\mathbb{T}$ be the algebra spanned by the T_m over $\mathbb{Z}$; like $\mathbb{B}$ it is commutative and $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ is semisimple. This algebra preserves the $\mathbb{Q}$ vector space $M_{\mathbb{Q}} \subset M_{\mathbb{C}}$ of dimension n consisting of those modular forms in $M_{\mathbb{C}}$ with Fourier coefficients in $\mathbb{Q}$.

These two setups are closely related and indeed we have a special case of the Jacquet–Langlands correspondence. Eichler proved that T_m and $B(m)$ have the same trace for all $m \in \mathbb{N}$. Hence, by semisimplicity of the algebras the map $T_m \mapsto B(m)$ induces a ring isomorphism $\mathbb{T} \simeq \mathbb{B}$. It follows that eigenspaces of $V_{\mathbb{Q}}$ and $M_{\mathbb{Q}}$, under the action of $\mathbb{B}$ and $\mathbb{T}$ respectively, correspond to each other. Since we also have multiplicity one these eigenspaces are one-dimensional.

In conclusion, given $f = \sum_{n \geq 0} a_n q^n \in M_{\mathbb{C}}$ an eigenform for all Hecke operators T_m (so that $T_m f = a_m f$) there is an $e_f \in V_{\mathbb{Q}} \otimes_{\mathbb{Z}} K$ unique up to scalars such that $B(m)e_f = a_m e_f$. (Here K denotes the field $\mathbb{Q}(a_0, a_1, \ldots)$ generated by the Fourier coefficients of f.)

In fact, this correspondence gives an efficient way to compute Fourier coefficients of eigenforms in $M_{\mathbb{C}}$ (see [11]). An implementation of the corresponding algorithms can be found in the above mentioned website (under `qalgmodforms`). Here is a sample GP session.

```
? R=qsetprime(11);

? brandt(R,2)~

[1 3]

[2 0]

? brandt(R,3)~

[2 3]

[2 1]
```

The first line defines R as a maximal order in the algebra ramified at 11 and ∞; the others compute the corresponding Brandt matrices. We find that these matrices have two eigenvectors: $e_E = (1/2, 1/3)$ and $e_f = (-1, 1)$ corresponding to an Eisenstein series and a cusp form, respectively.

The above implementation is intended for small to medium scale computations. For large scale computations one should use the *graph method* ideas of Mestre and Oesterlé [8], which exploit the sparse nature of the Brandt matrices.

Now following Gross we show how to associate a modular form of weight 3/2 to an eigenvector e_f. Let R_i be the right order of I_i and let $L_i \subset R_i$ be the ternary lattice defined by

$$L_i : \qquad w \in R_i, \qquad t(w) = 0, \qquad w \in \mathbb{Z} \bmod 2R_i.$$

Let g_i be the corresponding theta series

$$g_i(\tau) := \tfrac{1}{2} \sum_{w \in L_i} q^{n(w)}, \qquad q = e^{2\pi i \tau}.$$

Gross [3] prop. 12.9 describes precisely how the D-th coefficient $a_i(D)$ of g_i relates to the optimal embeddings of imaginary quadratic orders of $Q(\sqrt{D})$ into R_i.

These theta series are modular forms of weight 3/2 and level $4N$ and, in fact, belong to a certain subspace U defined by Kohnen. This subspace is determined by the condition that the coefficient of q^d of a form should be zero unless $D := -d$ is a discriminant, i.e., $D \equiv 0, 1 \bmod 4$, and $\left(\frac{D}{N}\right) \neq 1$. The weight 3/2 Hecke operators T_{m^2} preserve U.

Define

$$g := \sum_i e_f(i)\, g_i = \sum_D m_D\, q^{|D|} \in U.$$

This form is identically zero if the sign in the functional equation of f is -1. If g is non-zero it is a modular form in Shimura correspondence with f; i.e., $T_{m^2} g = a_m g$, where $T_m f = a_m f$. Moreover, we have the Waldspurger formula [3] 13.5

$$L(f, 1) L(f \otimes \chi_D, 1) = \kappa_f \frac{\delta_D}{\sqrt{|D|}}\, m_D^2, \tag{9}$$

where D is a fundamental discriminant with $\left(\frac{D}{N}\right) \neq 1$, χ_D is the associated quadratic character, $\kappa_f > 0$ is a constant depending only on f and $\delta_D := 2$ if $N \mid D$ and $\delta_D := 1$ otherwise.

Finally, let $E/\mathbb{Q}$ be an elliptic curve of prime conductor N and sign $+1$ in its functional equation. Let f and g be the corresponding modular forms of weight 2 and 3/2 respectively as above. Then if $L(f, 1) \neq 0$ we obtain from (9) a formula of type (1) with m_D the Fourier coefficient of g. As in §3 (II) to compute m_D for $|D| < X$ we could run through all $w \in L_i$ with $n(w) \leq X$ whose total number is $O(X^{3/2})$. Again various computational techniques could also be used to speed up the calculation of m_D. Note that in any case all computations are done with integer arithmetic.

Tables of m_D's for several curves and the routines to compute them can be found at G. Tornaría's website

`http://www.ma.utexas.edu/users/tornaria/cnt/`

among other goodies (an interactive version of Cremona's tables of elliptic curves and an interactive table of ternary quadratic forms).

5.

We conclude with some remarks about the general situation.

1. It follows from (9) that if $L(f,1)=0$ then the form g vanishes identically. In this case we naturally need to do something else.

In [7] we work out an extension of Gross's work introducing an auxiliary prime l; the theta series g_i, for example, are modified by introducing an appropriate weight function. The complexity of algorithms only increase by a factor essentially proportional to l.

2. If the level N is not prime but square-free the situation is not too different from the one described above. The downside is that $L(E,D,1)$ can be computed this way only for a certain fraction of D's (determined by local conditions). One needs to consider a quaternion algebra B ramified at ∞ and at primes $l \mid N$ for which the Atkin-Lehner involution acts as $f|_{w_l} = -f$ and an Eichler order in B of level the product of the remaining primes factors of N.

3. If the level is not square-free things become quite a bit more complicated; for example, the algebra $\mathbb{B}$ of Brandt matrices typically does not act with multiplicity one and some modular forms are simply missing. The arithmetic of the corresponding orders, which are no longer Eichler orders in general, also becomes more involved and, moreover, one needs to consider two types of orders: one for the weight 2 side and another for the weight 3/2 side; see [9], [10], [14] some work on this case.

4. To compute twists $L(f\otimes\chi_l,1)$ by *real* quadratic fields $\mathbb{Q}(\sqrt{l})$ one may consider a twist $f_D := f\otimes\chi_D$ by an auxiliary imaginary quadratic field $Q(\sqrt{D})$ and find a formula of type (1) for $L(f_D\otimes\chi_{Dl},1)$. The form f_D typically does not have square-free level so several corresponding difficulties ensue, see [14].

5. Forms of higher weight can also be handled using quaternion algebras by introducing harmonic polynomials as weight functions for the theta functions (both for the ideals I_i corresponding to forms of weight $2+2r$ and for the ternary lattices L_i corresponding to forms of weight $3/2+r$) see [6], [13].

References

[1] H. Cohen, *A course in computational algebraic number theory*, GTM **138**, Springer-Verlag, Berlin, (1993).

[2] L. Dickson, *History of the theory of numbers*, Chelsea Pub. Co., New York (1966).

[3] B. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., **7**, Amer. Math. Soc., Providence, RI, (1987).

[4] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

[5] B. Gross, W. Kohnen and D. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. **278** (1987), 497–562.

[6] R. Hatcher, *Heights and L-series*, Canad. J. Math. **42**,(1990), 533–560.

[7] Z. Mao, F. Rodriguez-Villegas, G. Tornaría, *Computation of central value of quadratic twists of modular L-functions*, To appear in “Ranks of Elliptic Curves and Random Matrix Theory” (2005).

[8] J.-F., Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), 217–242, Nagoya Univ., Nagoya, 1986.

[9] A. Pacetti and F. Rodriguez-Villegas (appendix by B. Gross), *Computing Weight* 2 *Modular forms of level* p^2 Math. Comp. **251**, (2004), 1545–1557.

[10] A. Pacetti, G. Tornaría, *Examples of Shimura correspondence for level* p^2 *and real quadratic twists* To appear in “Ranks of Elliptic Curves and Random Matrix Theory” (2005).

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

[12] F. Rodriguez-Villegas, *Explicit models of genus 2 curves with split CM* Algorithmic number theory (Leiden, 2000), 505–513, Lecture Notes in Comput. Sci., **1838**, Springer, Berlin, (2000).

[13] H. Rosson, G. Tornaría, *Central values of quadratic twists for a modular form of weight 4*, To appear in “Ranks of Elliptic Curves and Random Matrix Theory” (2005).

[14] A. Pacetti, G. Tornaría, *Shimura correspondence for level* p^2 *and the central values of L-series*, preprint (2005).

[15] D. Zagier, *Modular points, modular curves, modular surfaces and modular forms*, Workshop Bonn 1984 (Bonn, 1984), 225–248, Lecture Notes in Math., **1111**, Springer, Berlin, (1985).

Department of Mathematics
University of Texas at Austin,
TX 78712 USA

villegas@math.utexas.edu