MATHEMATICS OF COMPUTATION
Volume 66, Number 218, April 1997, Pages 833–839
S 0025-5718(97)00821-1

RATIONAL EIGENVECTORS IN SPACES OF TERNARY FORMS

LARRY LEHMAN

Abstract. We describe the explicit computation of linear combinations of ternary quadratic forms which are eigenvectors, with rational eigenvalues, under all Hecke operators. We use this process to construct, for each elliptic curve E of rank zero and conductor $N < 2000$ for which N or $N/4$ is squarefree, a weight 3/2 cusp form which is (potentially) a preimage of the weight two newform ϕ_E under the Shimura correspondence.

Introduction

If E is a modular elliptic curve over $\mathbb{Q}$ with ϕ_E its associated weight two newform, an interesting problem is to construct explicitly a weight 3/2 cusp form which is sent to ϕ_E by the Shimura correspondence. Tunnell [19], Frey [8], Bungert [3], and the author [12] have used such cusp forms to provide information about the group of rational points on twists of specific elliptic curves. (Koblitz uses Tunnell's result as the motivation for an introduction to elliptic curves and modular forms, particularly those of half-integral weight, and we refer to his book [10] for more details on this problem.)

One method of constructing weight 3/2 modular forms, which the author employed in [12], uses quadratic forms in three variables. In [13], we demonstrated a practical method for finding all ternary quadratic forms associated with modular forms of a given level. In this article, we consider further the connection between quadratic forms, modular forms, and elliptic curves from the computational viewpoint. Our main result is the following: For every isogeny class of elliptic curves E having rank zero and conductor $N < 2000$ such that either N or $N/4$ is squarefree, there is an explicitly computed weight 3/2 cusp form, arising from the ternary quadratic forms in a genus which depends on invariants of E, which is a candidate for being a preimage of ϕ_E under the Shimura correspondence. (See Theorem 1 below and the remarks which follow it for a more precise expression of this result.)

1. Hecke operators on ternary forms and modular forms

In this section, we briefly recall the necessary background on ternary quadratic forms and their associated modular forms. We refer to a positive definite quadratic form $f(x, y, z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$ whose coefficients are integers having no common divisors as a *ternary form*. The *matrix* of f is $A = A_f = \begin{bmatrix} 2a & t & s \\ t & 2b & r \\ s & r & 2c \end{bmatrix}$. Following the conventions of [13], we define the *discriminant* of f to

Received by the editor January 17, 1995 and, in revised form, February 7, 1996.
1991 *Mathematics Subject Classification.* Primary 11E45; Secondary 11F37, 11G05.
Key words and phrases. Quadratic forms, modular forms, elliptic curves.

be $d = \det(A)/2$ and its *level* to be the unique integer N such that NA^{-1} is the matrix of a ternary form. Ternary forms f and g are said to be *equivalent over a ring* R if there is an R-unimodular matrix U (a matrix with entries in R whose determinant is a unit in R) such that $A_g = UA_fU^t$. Two ternary forms are in the same *class* if they are equivalent over $\mathbb{Z}$. They are in the same *genus* if they are equivalent over $\mathbb{Z}_p$ for all primes p and over the real numbers. This is the case if and only if the ternary forms have the same discriminant and level and the same collection of genus symbols. (See [13, p. 410] for the definition of genus symbols.)

Now consider a genus of ternary forms of level N, with $G = \{f_1, \ldots, f_n\}$ as class representatives. Let $\mathcal{M}$ be the complex vector space having G as a basis. Then there is a commutative family of linear operators on $\mathcal{M}$, $\mathcal{T} = \{T_p \mid p \text{ prime}, p \nmid N\}$, which we refer to as *Hecke operators*. We can define T_p as follows (see [1] for more details and references): For each $f \in G$, the congruence $f(x, y, z) \equiv 0 \pmod{p}$ is a nonsingular conic over $\mathbb{F}_p$, call it $S_p(f)$, and so contains $p + 1$ points. For each point P on $S_p(f)$, there is a $\mathbb{Z}$-unimodular matrix U such that the first row of U, viewed as a point in projective space over $\mathbb{F}_p$, is the same as P, and such that $UA_fU^t = \begin{bmatrix} 2p^2a & pt & s \\ pt & 2b & r \\ s & r & 2c \end{bmatrix}$ with a, $t \in \mathbb{Z}$. Then let $A_g = \begin{bmatrix} 2a & t & s \\ t & 2b & pr \\ s & pr & 2p^2c \end{bmatrix}$ be the matrix of a ternary form g. One can show that f and g are in the same genus and that the class of g depends only on the point P and the class of f. Denote the class of g by $P(f)$. So now we can define T_p by setting $T_p(f_i) = \sum_{P \in S_p(f_i)} P(f_i)$ for $1 \le i \le n$, and extending T_p to $\mathcal{M}$ by linearity.

We are interested in finding *rational eigenvectors* in $\mathcal{M}$, that is, eigenvectors which have rational eigenvalues under each of the Hecke operators. We note some useful facts about eigenvectors in the following two propositions.

Proposition 1. *Let $g = \sum_{i=1}^n \alpha_i f_i$ be an eigenvector of T_p (for some prime $p \nmid N$ as above) with eigenvalue λ. Then λ is an algebraic integer which is rational if each α_i is rational. Furthermore $|\lambda| \le p + 1$ and $\lambda = p + 1$ if $\sum_{i=1}^n \alpha_i \neq 0$.*

Proof. If $B = [b_{ij}]$ is the representation of T_p with respect to the basis G, then each b_{ij} is a nonnegative integer and for all j, $\sum_{i=1}^n b_{ij} = p + 1$. The first statement in Proposition 1 is then obvious. For the second, consider the sums $\sum_{i=1}^n |\lambda\alpha_i|$ and $\sum_{i=1}^n \lambda\alpha_i$. □

We will denote the subspace of $\mathcal{M}$ consisting of all $\sum_{i=1}^n \alpha_i f_i$ with $\sum_{i=1}^n \alpha_i = 0$ as $\mathcal{S}$ and refer to these as *cusp vectors* in $\mathcal{M}$. It is easy to see that $\mathcal{S}$ is invariant under all T_p. The fact that the Hecke operators in $\mathcal{T}$ commute allows us to conclude the following:

Proposition 2. *Let V be a subspace of $\mathcal{M}$ which is invariant under all operators in $\mathcal{T}$. For a specific prime p and some $\lambda \in \mathbb{C}$, let W be the λ-eigenspace of T_p in V. Then W is also invariant under $\mathcal{T}$.*

Proof. If w is any element in W, then for any prime q, $T_p(T_q(w)) = T_q(T_p(w)) = T_q(\lambda w) = \lambda T_q(w)$. Thus $T_q(w) \in W$ by definition. □

If f is a ternary form with level N and discriminant d, then the complex function on the upper half-plane defined by

$$\theta_f(z) = \sum_{(k,l,m) \in \mathbb{Z}^3} e^{2\pi i \cdot f(k,l,m)z} = \sum_{n=0}^{\infty} a_n q^n, \text{ where } q = e^{2\pi iz},$$

is a modular form of weight 3/2, level N, and character χ_d [17]. The latter expression is called the q-expansion of θ_f. Modular forms of the same weight, level, and character are equal if their q-expansions are identical for sufficiently many terms, depending on the level of the forms [15]. For any prime p, there is a Hecke operator $T(p^2)$ which takes a form θ_f to another modular form of the same weight, level, and character. For $p \mid N$, we can define $T(p^2)$ in terms of the q-expansion of θ_f by $T(p^2)\theta_f = \sum_{n=0}^{\infty} a_{p^2 n} q^n$. (See [10] for the more general definition of Hecke operators, and for more details on these terms.)

If $\mathcal{M}$ is spanned by a genus $G = \{f_1, \ldots, f_n\}$ of ternary forms of level N, then there is a linear map, which we will denote by Θ, from $\mathcal{M}$ into a space of modular forms, determined by sending each ternary form $f \in G$ to the modular form $\theta_f/2$. We will denote the image of $\mathcal{M}$ as M in general. Because $\theta_f - \theta_g$ is a cusp form if f and g are in the same genus [16], it is easy to see that the image of $\mathcal{S}$ under Θ, call it S, is the subspace of cusp forms in M. Results of Eichler [7] and Ponomarev [14] (see also [3, Prop. 4]) indicate that the Hecke operators T_p defined on $\mathcal{M}$ are essentially the same as $T(p^2)$ on M, that is, for primes $p \nmid N$ that $\Theta \circ T_p = T(p^2) \circ \Theta$. In particular, an eigenvector in $\mathcal{M}$ is mapped to an eigenform in M (or to zero, as noted in Theorem 1 below).

2. Rational eigenvectors associated to elliptic curves

We now note some connections between certain elliptic curves and eigenvectors in specific spaces of ternary forms. Let E be a representative of an isogeny class of modular elliptic curves over $\mathbb{Q}$ and let ϕ_E be its associated weight two newform. Suppose that E has even rank and that its conductor is of the form $N = 2^e Q$ where Q is an odd, squarefree integer and $0 \le e \le 3$. For each prime $p \nmid N$, let λ_p be the eigenvalue of ϕ_E under the Hecke operator $T(p)$. For $p \mid N$, let ε_p be the eigenvalue of ϕ_E under the W_p involution. Define a squarefree integer γ by saying that $p \mid \gamma$ if and only if $\varepsilon_p = -1$. We will say that γ is the *genus number* associated to the collection $\{\varepsilon_p\}$ (or to ϕ_E or to E). Since E has even rank, it is conjectured that $\prod \varepsilon_p = -1$ or equivalently that γ has an odd number of prime factors. (See [18] for more details on these operators.)

To E, we associate a genus of ternary forms in the following way. Let the level of the genus equal $2^r Q$ and the discriminant equal $2^s Q^2$ where r and s are as follows: If $e = 0$, then $r = 2$ and $s = 4$; if $e = 1$, then $r = 2$ and $s = 2$; if $e = 2$, then $r = 3$ and $s = 4$; and if $e = 3$, then $r = 4$ and $s = 5$. For a ternary form f of this level and discriminant, the relevant genus symbols are (f/p) for all $p \mid Q$, and if $e = 0$, $(f/4)$ (but in that case, $(f/4)$ must be -1) [13, Prop. 5]. In each case, choose (f/p) to be $\varepsilon_p(-2^s/p)$. Let $\mathcal{M}(N, \gamma)$ be the space spanned by all classes of ternary forms in the genus having level, discriminant, and genus symbols as defined here (with $\mathcal{S}(N, \gamma)$ its subspace of cusp vectors, and so forth).

In the case in which $e = 0$, the fact that $(f/4) = -1$ implies that any cusp form in $S(N, \gamma)$ has the form $\sum_{n=1}^{\infty} a_n q^n$, where $a_n = 0$ if $n \equiv 1$ or $2 \pmod 4$. Thus $S(N, \gamma)$ is a subspace of the space denoted as $S_{3/2}(N)$ in [11]. In general, this space is not invariant under the operator $T(2^2)$ as defined above, but Kohnen defines a revised operator, which we will denote by $T'(2^2)$, for this space (see [11, p. 42] for the definition of this operator).

We can now state our main result as follows:

Theorem 1. *For every isogeny class of elliptic curves E of even rank and conductor $N = 2^eQ < 2000$, with genus number γ, there is an explicitly computed rational eigenvector $g \in \mathcal{M}(N, \gamma)$, unique up to scalar multiplication, having eigenvalues the same as those of ϕ_E for small primes. Furthermore, $A = A(z) = \Theta(g)$ has the following properties:*

(1) *$A \neq 0$ if and only if E has rank zero.*
(2) *If $e = 0$, then $T'(2^2)A = \lambda_2 A$.*
(3) *If $e = 1$, then $T(2^2)A = -\varepsilon_2 A$.*
(4) *If $e = 2$, then $T(2^2)A = 0$.*
(5) *If $e = 3$, then $T(2^2)A(2z) = 0$.*
(6) *If an odd prime p divides γ, then $T(p^2)A = A$.*

Proof. The proof is mainly by direct computation, but we describe the general method used to establish this result. Let $G = \{f_1, \ldots, f_n\}$ be a basis for $V_0 = \mathcal{M}(2^eQ, \gamma)$. Writing the primes not dividing $2Q$ in increasing order as p_1, $p_2, \ldots$, let V_i be the λ_{p_i}-eigenspace of T_{p_i} in V_{i-1}, for $i > 0$. If B_i is the representation of T_{p_i} with respect to G, a basis for V_i can be found by solving the homogeneous system $(\lambda_{p_i} I_n - B_i)X = 0$. It is clear that each element in such a basis can be taken as a rational linear combination of G. By Proposition 2, each space V_i is invariant under all operators in $\mathcal{T}$. By direct computation, we have shown that for some $i > 0$, $\dim V_i = 1$ and so any nonzero element $g \in V_i$ is an eigenvector under all $T_p \in \mathcal{T}$, with a rational eigenvector in each case.

The first five statements about $A = \Theta(g)$ are also established computationally by calculating sufficiently many terms in the q-expansion of A. (Note that statement 5 says that each term of even exponent in that q-expansion has coefficient 0.) Statement 6 is shown without computation by establishing a one-to-one correspondence between solutions of $f(x, y, z) = n$ and of $f(x, y, z) = p^2 n$ if f is a ternary form for which the genus symbol (f/p) is equal to $-(2^s/p)$ (which is the case if $p \mid \gamma$). The details are omitted. □

Remarks. We used published [4] and unpublished [6] tables of Cremona for the elliptic curves of conductor less than 2000. The invariants ε_p and λ_p are easily calculated in terms of E—note in particular that since $\lambda_p = p + 1 - |E_p|$ [4], it follows that $|\lambda_p| < p + 1$ and thus that any eigenvector g obtained by this process must be a cusp vector. A basis G for $\mathcal{M}(N, \gamma)$ can be computed using the process outlined in [13]. The representation matrices B_i are found using an algorithm adapted from [1].

In general, the cusp form $A = \Theta(g)$ is, as stated in the introduction, merely a candidate for being a preimage of ϕ_E under the Shimura correspondence. But in any specific case, the remaining details could, in principle, be tested as follows: One could check by sufficient computation that A is an eigenform under $T(p^2)$ for any odd prime $p \mid N$ for which $p \nmid \gamma$. (Preliminary computations in our examples give strong evidence that $T(p^2)A = -A$ for each such prime.) If so, then A must be sent to some weight two newform ψ by the Shimura correspondence. If for sufficiently many primes, the eigenvalues of A agree with those of ϕ_E, it follows that $\psi = \phi_E$ [15]. In each of our examples, we have checked that the eigenvalues of A are the same as those of ϕ_E for all primes $p < 50$ for which $p \nmid N$.

We do not offer a proof that there is always some $i > 0$ for which $\dim V_i = 1$ (that is, for $N > 2000$). However, we note that results of Gross [9] when N is prime, and Böcherer and Schulze-Pillot [2] when N is squarefree indicate that a preimage

of ϕ_E under the Shimura correspondence is a linear combination of the theta series associated to ternary forms if and only if for the L-series of ϕ_E, $L(\phi_E, 1) \neq 0$. This is conjectured to be the case if and only if the rank of E is zero.

The particular choices of the level, discriminant, and genus symbols of the ternary forms which we associate to an elliptic curve E are based on extensive computation of all rational eigenvectors in spaces of ternary forms. By Proposition 1, there are only finitely many possible rational eigenvalues under a given Hecke operator T_p on a space of ternary forms $\mathcal{M}$. We have carried out a complete computation of all rational eigenvectors in a large number of spaces, and we present some results in the following:

Theorem 2. *Let $N = 2^e Q$ with Q odd and squarefree and $0 \leq e \leq 3$ as above. For each prime p dividing N, let ε_p be chosen as ± 1 such that $\prod \varepsilon_p = -1$, and let γ be the genus number associated to the collection $\{\varepsilon_p\}$. Let $\mathcal{S}(N, \gamma)$ be the space of cusp vectors generated by the genus of ternary forms as defined preceding Theorem 1. If D divides N, let $n(D, \gamma)$ be the number of weight two newforms of level D and genus number γ. (If $\gamma \nmid D$, then $n(D, \gamma) = 0$ by definition.) Then for all $N < 1000$,*

(1) $\dim \mathcal{S}(N, \gamma) = \sum_{D|N} n(D, \gamma)$.

(2) *There is a one-to-one correspondence between independent rational eigenvectors in $\mathcal{S}(N, \gamma)$ and isogeny classes of elliptic curves of even rank, conductor D dividing N, and genus number γ.*

(3) *If g is a rational eigenvector in $\mathcal{S}(N, \gamma)$, but g does not arise from an elliptic curve of conductor N as in Theorem 1, then there is at least one prime $p \mid N$ for which $\Theta(g)$ is not an eigenform under $T(p^2)$.*

Remark. The proof of Theorem 2 is again by direct computation. Statement 1 is proved by comparing our tables of ternary forms with tables of W-splits of weight two modular forms compiled by Cremona in an unpublished table [5].

3. Example

We conclude by presenting an example to illustrate the results of Theorems 1 and 2. This example is fairly typical, although in many cases, the space of ternary forms which we must consider has a substantially larger dimension than in this case.

Let E be given by $y^2 = x^3 - x^2 + 25158x - 775719$, an elliptic curve of rank 0 and conductor $924 = 2^2 \cdot 3 \cdot 7 \cdot 11$, denoted as curve 924A1 in [4]. By counting points on E reduced modulo various primes, we find that $\varepsilon_3 = 1$, $\varepsilon_7 = 1$, $\varepsilon_{11} = 1$, $\lambda_5 = -3$, $\lambda_{13} = 1$, etc. Since the rank of E is even, we may assume that $\varepsilon_2 = -\varepsilon_3\varepsilon_7\varepsilon_{11} = -1$, so the genus number of E is 2. (These values are confirmed by Table 3 in [4].)

Writing $N = 924$ as $2^e Q$ with $e = 2$ and $Q = 231$, we associate to E the genus of ternary forms having level $2^3 Q = 1848$, discriminant $2^4 Q^2 = 853776$, and genus symbols $(f/3) = \varepsilon_3(-2^4/3) = -1$, $(f/7) = -1$, and $(f/11) = -1$. Using the methods of [13], we find that there are ten classes of ternary forms in this genus, having representatives $f_1, \ldots, f_{10}$ as in the following table. Let $\mathcal{M}(924, 2)$ be the $\mathbb{C}$-vector space spanned by these ten forms.

Applying T_5 to $\mathcal{M}(924, 2)$, we find that the -3-eigenspace, V_1, has dimension 2, but in V_1, the 1-eigenspace of T_{13}, V_2, is one-dimensional. For some vector in V_2

TABLE 1. $\mathcal{M}(924,2)$ is spanned by the ternary forms $f_1,\ldots,f_{10}$. There are seven rational eigenvectors in $\mathcal{S}(924,2)$, each presented as a linear combination of the f_i's. (For example, $g_1 = f_1 - f_2 + \cdots + 6f_{10}$.)

	$\underline{f_1}$	$\underline{f_2}$	$\underline{f_3}$	$\underline{f_4}$	$\underline{f_5}$	$\underline{f_6}$	$\underline{f_7}$	$\underline{f_8}$	$\underline{f_9}$	$\underline{f_{10}}$	
a :	6	17	21	24	33	35	35	41	54	54	
b :	77	83	110	83	84	41	66	68	54	62	
c :	462	164	110	117	98	164	98	83	77	83	
r :	0	−52	−88	6	−84	32	0	−20	0	16	
s :	0	−8	0	12	0	28	−28	−26	0	36	
t :	0	−10	0	24	0	14	0	−8	−24	48	
g_1 :	1	−1	1	−1	3	1	−1	−5	−4	6	924A
g_2 :	1	0	1	2	1	−4	−2	0	1	0	154B
g_3 :	4	6	−1	−4	2	−6	6	0	−1	−6	132B
g_4 :	2	−2	2	−2	−1	2	−2	4	−1	−2	84B
g_5 :	1	0	−1	2	−1	0	0	0	−1	0	66B
g_6 :	1	4	1	−1	−2	1	−1	−5	1	1	44A
g_7 :	1	−4	1	2	1	4	2	−4	1	−4	42A

(g_1 in the table above), we calculate that

$$A_1 = \Theta(g_1) = q^6 - q^{17} + q^{21} + 3q^{33} - 4q^{41} + \ldots,$$

a cusp form of weight 3/2, level 1848, and trivial character. Forms in this space are equal if their q-expansions are identical to the term of q^{577} [15], so by direct calculation, we verify that $T(2^2)A_1 = 0$ and $T(p^2)A_1 = -A_1$ for $p = 3$, 7, and 11.

In $\mathcal{S}(924,2)$, there are seven independent rational eigenvectors, listed as $g_1,\ldots,g_7$ in the table above. By computing their eigenvalues for primes $p < 50$ which do not divide 924, it appears that there is a correspondence between these eigenforms and the isogeny classes of elliptic curves listed at the right of the table. These are all the elliptic curves of conductor dividing 924 which have genus number 2 [4]. However, if we let $A_i = \Theta(g_i)$ for $1 \le i \le 7$, we easily check that A_2, A_5, and A_7 are not eigenforms under $T(2^2)$; A_2 and A_6 are not eigenforms under $T(3^2)$; A_3, A_5, and A_6 are not eigenforms under $T(7^2)$; and A_4 and A_7 are not eigenforms under $T(11^2)$.

REFERENCES

1. B. J. Birch, *Hecke actions on classes of ternary quadratic forms*, Computational Number Theory, Walter de Gruyter & Co., Berlin, 1991, pp. 191–212. MR **93i:**11047
2. S. Böcherer and R. Schulze-Pillot, *The Dirichlet series of Koecher and Maass and modular forms of weight 3/2*, Math. Z. **209** (1992), 273–287. MR **93b:**11053
3. M. Bungert, *Construction of a cuspform of weight 3/2*, Arch. Math. **60** (1993), 530–534. MR **94f:**11035
4. J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, England, 1992. MR **93m:**11053
5. ———, *Dimensions and W-splits of cusp forms of level $N \le 1000$*, Unpublished table (1990).
6. ———, *Modular elliptic curves: conductors from 1001 to 2000*, Unpublished table (1993).
7. M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Springer-Verlag, Berlin, 1952. MR **14:**540a
8. G. Frey, *Der Rang der Lösungen von $y^2 = x^3 \pm p^3$ über $\mathbb{Q}$*, Manuscripta Math. **48** (1984), 71–101. MR **86g:**11033

9. B. H. Gross, *Heights and the special values of L-series*, Number Theory, Montreal 1985 (CMS Conf. Proc.), vol. 7, Amer. Math. Soc., Providence, 1987, pp. 115–187. MR **89c:**11082
10. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984. MR **86c:**11040
11. W. Kohnen, *Newforms of half-integral weight*, J. reine angew. Math. **333** (1982), 32–72. MR **84b:**10038
12. L. Lehman, *Rational points on elliptic curves with complex multiplication by the ring of integers in* $\mathbb{Q}(\sqrt{-7})$, J. Number Theory **27** (3) (1987), 253–272. MR **89a:**11059
13. ———, *Levels of positive definite ternary quadratic forms*, Math. Comp. **58** (197) (1992), 399–417. MR **92f:**11057
14. P. Ponomarev, *Ternary quadratic forms and Shimura's correspondence*, Nagoya Math. J. **81** (1981), 123–151. MR **83a:**10043
15. B. Schoeneberg, *Elliptic Modular Functions, An Introduction*, Springer-Verlag, New York, 1974. MR **54:**236
16. R. Schulze-Pillot, *Thetareihen positiv definiter quadratischer Formen*, Invent. Math. **75** (1984), 283–299. MR **86d:**11042
17. G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), 440–481. MR **48:**10989
18. H. P. F. Swinnerton-Dyer and B. J. Birch, *Elliptic curves and modular functions*, Lecture Notes in Mathematics, vol. 476, Springer-Verlag, Berlin, 1975. MR **52:**5685
19. J. B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. **72** (1983), 323–334. MR **85d:**11046

Department of Mathematics, Mary Washington College, Fredericksburg, Virginia 22401

E-mail address: llehman@mwc.edu