JOURNAL OF NUMBER THEORY 26, 1–7 (1987)

Theta Series of Ternary Quadratic Forms

D. C. HUNG

Department of Mathematics, State University of New York, Binghamton, New York 13901

Communicated by H. Zassenhaus

Received February 26, 1985; revised June 25, 1986

We establish the linear independence of the theta series arising from the classes of even positive definite ternary forms of discriminant $2p^2$ which have a nontrivial automorphism group. p is assumed to be an odd prime number. We also consider even positive ternary forms over $\mathbb{Z}[(1+\sqrt{p})/2]$ of discriminant 2. In the case $p \equiv 5 \pmod 8$, we show that those forms that represent 2 have independent generalized theta series. © 1987 Academic Press, Inc.

Unless otherwise indicated, we shall adopt the terminology and notations of [7]. All quadratic forms will be even positive definite and all genera will be uniquely determined by their discriminants. Let $G(n, d)$ denote the genus of n-ary quadratic forms over $\mathbb{Z}$ of discriminant d, and $\mathscr{G}(n, d)$ the corresponding genus over the ring of integers of $\mathbb{Q}(\sqrt{p})$, where p throughout will be an arbitrarily fixed prime $\equiv 1 \pmod 4$. In an earlier paper [1], Hsia and the author established a few results on the linear independence of theta series associated with certain classes of forms in $G(3, 2p)$ and $G(4, p)$. These genera, as it turns out, are not the only instances to which our arithmetic method applies, and similar results can be obtained (see [2]) for other genera as well as for theta series over number fields. The objective here is to investigate the theta series arising from the forms in the ternary genera $G(3, 2p^2)$ and $\mathscr{G}(3, 2)$.

Our approach is similar to that of [1, 2]. Some technical features must be overcome by analyzing the arithmetic structures of the forms in each genus. In the case of $G(3, 2p^2)$, this is accomplished by establishing a one-to-one correspondence between its classes and those in $G(3, 2p)$. Such a correspondence has been proved in [8] via the arithmetic of quaternion algebra. We present here a lattice-theoretic proof which will be useful to our study of the theta series. The second half of this paper is devoted to the study of the forms in $\mathscr{G}(3, 2)$ and their associated theta series. For this we make use of the known structures of the forms in $\mathscr{G}(4, 1)$, which was treated in [2]. We shall adopt the geometric language of quadratic spaces and lattices in the following discussion.

0022-314X/87 $3.00

1. Even Positive Definite Ternary Lattices of Discriminant $2p^2$

We fix a prime $p \equiv 1 \pmod 4$. Let K be an even positive definite ternary lattice of discriminant $2p^2$. Then K is $2\mathbb{Z}$-maximal and the Hasse symbol of $\mathbb{Q}K$ at 2 is -1. Since $S_r(\mathbb{Q}K) = 1$ for all primes $r \neq 2, p$, we have $S_p(\mathbb{Q}K) = -1$ also by the Hilbert reciprocity law. It follows that there is just one genus $G(3, 2p^2)$ of such ternary lattices. Locally at the prime p, we have

$$K_p \cong \langle -2\Delta \rangle \perp \langle p \rangle \perp \langle -\Delta p \rangle,$$

where Δ is a nonsquare p-adic unit.

Proposition 1.1. *Let $K \in G(3, 2p^2)$. Then K contains a unique sublattice $\bar{K}$ such that $[K: \bar{K}] = p$ and $n(\bar{K}_p) = p\mathbb{Z}_p$.*

Proof. Locally at p, $K_p = \mathbb{Z}_p x_1 \perp \mathbb{Z}_p x_2 \perp \mathbb{Z}_p x_3$, where $Q(x_1) = -2\Delta$, $Q(x_2) = p$, and $Q(x_3) = -\Delta p$. By lattice theory, there is a lattice $\bar{K}$ such that

$$\bar{K}_r = \begin{cases} K_r, & r \neq p, \\ \mathbb{Z}_p(px_1) \perp \mathbb{Z}_p x_2 \perp \mathbb{Z}_p x_3, & r = p. \end{cases}$$

Clearly, K contains $\bar{K}$ with $[K: \bar{K}] = p$ and $n(\bar{K}_p) = p\mathbb{Z}_p$. To show the uniqueness, let J be a sublattice of K with the stated properties. Then $J_r = K_r = \bar{K}_r$ for all $r \neq p$. It suffices to show that $J_p = \bar{K}_p$. If u is any vector in J_p, then $u = \alpha x_1 + \beta x_2 + \gamma x_3$ for some $\alpha, \beta, \gamma \in \mathbb{Z}_2$. Since $Q(u) = -2\Delta\alpha^2 + \beta^2 p - \Delta\gamma^2 p \in p\mathbb{Z}_p$, we have $\alpha \in p\mathbb{Z}_p$, hence $u \in \bar{K}_p$. It follows at once that $J = \bar{K}$.

Remark 1.2. If the lattice $\bar{K}$ is scaled by a factor p^{-1} then one obtains a lattice K' in $G(3, 2p)$. Conversely, given $K' \in G(3, 2p)$, we let $\bar{K} = (K')^p$. Then $\bar{K}$ has discriminant $2p^4$ and locally at p, $\bar{K}_p \cong \langle p \rangle \perp \langle -\Delta p \rangle \perp \langle -2\Delta p^2 \rangle$. By a construction which is the inverse process of that in Proposition 1.1, one obtains a unique lattice K in $G(3, 2p^2)$ containing $\bar{K}$ such that $[K: \bar{K}] = p$. We shall reserve the symbols K, $\bar{K}$ and K' for the lattices just mentioned.

Corollary 1.3. *The mapping $K \mapsto K'$ induces a one-to-one correspondence between the classes in $G(3, 2p^2)$ and those in $G(3, 2p)$.*

Remark 1.4. It is easy to see from the proof of Proposition 1.1 that any vector u in K of length $Q(u)$ which is divisible by p actually lies in $\bar{K}$. In particular, if $u \in K$ has length $2p$, then $u \in \bar{K}$, hence the number of representations of $2p$ by K (denoted by $a_K(2p)$) is the same as those by $\bar{K}$. On the other hand, it is clear that $a_{\bar{K}}(2p) = a_{K'}(2)$, since K' is just the lattice $\bar{K}$ scaled by p^{-1}. It follows therefore that $a_K(2p) = a_{K'}(2)$.

PROPOSITION 1.5. *Let* K, $\bar{K}$, K' *be as in Remark* 1.2. *Then* $O(K) = O(\bar{K}) = O(K')$.

Proof. Since $\bar{K}$ and K' have the same underlying lattice structure, it is clear that $O(\bar{K}) = O(K')$. To see that $O(K) = O(\bar{K})$, let $\sigma \in O(K)$. Since both $\sigma\bar{K}$ and $\bar{K}$ are sublattices of index p in K with their norms contained in $p\mathbb{Z}$, it follows by Proposition 1.1 that $\sigma\bar{K} = \bar{K}$. Conversely, if $\sigma \in O(\bar{K})$, then σK contains $\bar{K}$ as a sublattice of index p. Therefore $\sigma K = K$ by the uniqueness of such lattice (see Corollary 1.3).

Remark 1.6. It is now clear from the structure of $O(K')$ as given in [4] that $O(K)$ is generated by symmetries and ± 1. A typical symmetry of $O(K)$ is of the form S_u, where u is a vector in K of length $2p$. The order of $O(K)$ is determined by the number of such vectors of length $2p$. In particular, $|O(K)| = 2, 4, 8, 12$ accordingly as $a_K(2p) = 0, 2, 4, 6$, respectively.

In the following, $G'(n, d)$ will denote those lattices in $G(n, d)$ which have an improper automorphism. The same notation will also apply to the genus $\mathscr{G}(n, d)$. By Remark 1.6, $G'(3, 2p^2)$ are exactly those lattices in $G(3, 2p^2)$ which represent $2p$. In view of the close relationship between these lattices and their counterparts in $G'(3, 2p)$, we shall now examine their theta series. Specifically, we shall prove their linear independence. Recall in the proof of the independence for $G'(3, 2p)$ that a key ingredient is the existence of a prime q_i for each class K_i' such that $a_{\tilde{K}_i'}(q_i) \equiv 2 \pmod 4$ but $a_{\tilde{K}_j'}(q_i) \equiv 0 \pmod 4$ for $j \neq i$ (see [1, p. 155]), where $\tilde{K}'$ is the reciprocal of K' (i.e., the dual $(K')^{\#}$ scaled by the factor dK'/Ω, where Ω is the g.c.d. of the entries in the adjoint matrix of K'). It would now be sufficient, in order to prove the independence for $G'(3, 2p^2)$, to show that $a_{\tilde{K}_j'}(q_i) = a_{\tilde{K}_j}(p^2 q_i)$ for all i, j, where K_j' and K_j are corresponding classes in $G'(3, 2p)$ and $G'(3, 2p^2)$. This can be accomplished by linking the representations of an integer by a form to the representations of codimension 1 forms by its reciprocal. For a detailed statement of this classical duality, see Proposition I.2.3, [2]. In particular, if K', K are corresponding lattices in $G'(3, 2p)$ and $G'(3, 2p^2)$, and q a prime $\neq p$, then

$\frac{1}{2}a_{\tilde{K}'}(q) =$ the number of (primitive) binary sublattices of K' of discriminant q

and

$\frac{1}{2}a_{\tilde{K}}(p^2 q) =$ the number of primitive binary sublattices of K of discriminant $p^2 q$.

Our proof will be completed if we show that these two numbers coincide. It is clear that every binary sublattice of discriminant q in K' gives rise to a sublattice of discriminant p^2q in K by scaling. Conversely, every binary sublattice of discriminant p^2q in K comes from one of discriminant q in K':

PROPOSITION 1.7. *Let K, $\bar{K}$, K' be as in Remark 1.2. Suppose K contains a binary sublattice M of discriminant p^2q, where q is an odd prime $\neq p$. Then $M \subset \bar{K}$, hence K' contains the lattice $N = M^{p^{-1}}$.*

Proof. We first show that M_p is p-modular. Suppose this is not the case; then $M_p = \mathbb{Z}_p u \perp \mathbb{Z}_p v$, where $Q(u)$ is a p-adic unit and $Q(v) \in p^2\mathbb{Z}_p$. It follows that u splits K_p; hence $K_p = \mathbb{Z}_p u \perp B$ for some binary B. It is easy to see that B is p-modular and $\mathbb{Q}_p B$ is anisotropic. By [7, 63:15], B represents only elements of odd order. This is absurd, since $v \in B$. Now we have $nM \subseteq 2p\mathbb{Z}$, hence by Remark 1.4, $M \subset \bar{K}$.

Summarizing the above, we obtain:

THEOREM 1.8. *The theta series $\Theta_K(z)$ for lattices K coming from the classes in $G'(3, 2p^2)$ are linearly independent over $\mathbb{C}$.*

Remark 1.9. The results in this section remain valid for the case $p \equiv 3 \pmod 4$. The principal difference here is the existence of decomposable forms. Some modifications to the proof of Theorem 1.8 are therefore needed to deal simultaneously with such forms and the indecomposable ones.

2. EVEN POSITIVE DEFINITE TERNARY LATTICES OF DISCRIMINANT 2 OVER $\mathbb{Q}(\sqrt{p})$

Fix a prime $p \equiv 1 \pmod 4$. Let $F = \mathbb{Q}(\sqrt{p})$, $\mathcal{O}$ be the ring of integers of F and $\mathcal{O}^\times$ be the group of units of $\mathcal{O}$. Let V be a positive definite ternary space of discriminant 2 over F. We assume that V admits an even lattice K over $\mathcal{O}$ such that $K_\mathfrak{p}$ is unimodular at all nondyadic primes and $dK_\mathfrak{p} = 2$ for dyadic primes. Let $\mathcal{A}$ be the quaternion algebra of discriminant p^2 over $\mathbb{Q}$ and $\mathcal{A}_F = \mathcal{A} \otimes F$; then V is isometric to the pure part of $\mathcal{A}_F$, where the quadratic map on $\mathcal{A}_F$ is $2N(-)$, N the reduced norm. The $2\mathcal{O}$-maximal lattices K on V are free (see [5, Appendix]) and constitute a single genus $\mathcal{G}(3, 2)$. They are closely related to the unimodular lattices on $\mathcal{A}_F$, specifically, to those lattices $L \in \mathcal{G}'(4, 1)$ which contain a nontrivial root system. Some basic facts about these lattices may be found in [2]. A vector e will be called a minimal vector if it has quadratic length 2. By a standard construction of even quaternary lattices from even ternary ones (see Proposition I.1.1, [2]), there is associated to every $K \in \mathcal{G}(3, 2)$ a unique lattice L in $\mathcal{G}'(4, 1)$ containing $\mathcal{O}e \perp K$. Conversely, if $L \in \mathcal{G}'(4, 1)$ and e is a minimal vector in L, then $K=(\mathcal{O}e)^{\perp}\in\mathcal{G}(3,2)$ (here the orthogonal complement is taken in L). We shall assume in the following that $p>5$.

PROPOSITION 2.1. *Let L be any lattice in* $\mathcal{G}'(4,1)$; *then the minimal vectors in L are transitively permuted by its automorphism group* $O(L)$.

Proof. By the structures of 2-lattices over real quadratic integers as given in [6], any two minimal vectors e_1, e_2 in L are either orthogonal or they satisfy $B(e_1,e_2)=\pm 1$. If e_1 and e_2 are orthogonal, then there exist a vector u in $(\mathcal{O}e_1\perp\mathcal{O}e_2)^{\perp}$ and a principal prime ideal $\mathfrak{q}=\mathcal{O}\pi$ such that $Q(u)=2\pi$. It follows that $L\supset\mathcal{O}e_1\perp\mathcal{O}e_2\perp\mathcal{O}u\perp\mathcal{O}v$ for some vector v of length $Q(v)=2\pi$. The mapping σ defined by $\sigma(e_1)=e_2$, $\sigma(e_2)=e_1$, $\sigma(u)=v$ and $\sigma(v)=-u$ is an automorphism of L. If e_1 and e_2 are not orthogonal, then we may assume that $B(e_1,e_2)=1$. Clearly, the automorphism $S_{e_1-e_2}$ permutes e_1 and e_2.

It follows from Proposition 2.1 that the mapping $K\mapsto L\supset\mathcal{O}e\perp K$ induces a one-to-one correspondence between the classes in $\mathcal{G}(3,2)$ and those in $\mathcal{G}'(4,1)$. The type of roots system of K can be easily determined by the type of the corresponding lattice L. In fact, K is of type ϕ, A_1, A_2 or $A_1\oplus A_1\oplus A_1$ as the type of L is A_1 or A_2, $A_1\oplus A_1$, $A_2\oplus A_2$, or D_4, respectively.

PROPOSITION 2.2. *Let* $K\in\mathcal{G}(3,2)$ *and* $L\supset\mathcal{O}e\perp K$ *be the corresponding lattice in* $\mathcal{G}'(4,1)$; *then* $|O(K)|=\sqrt{|O(L)|}$.

Proof. Since $O(L)$ permutes the minimal vectors of L, we have for any minimal vector e' in L an automorphism $\sigma\in O(L)$ such that $\sigma(e)=e'$ and $\sigma K=K'$, where $K'=(\mathcal{O}e')^{\perp}$. Conversely, if η is an isometry of K onto K' and $\rho e=e'$, then $\sigma=\rho\perp\eta$ is an automorphism of L, since L is the only lattice in $\mathcal{G}'(4,1)$ containing $\mathcal{O}e'\perp K'$. Now the number of isometries from K onto K' is just $|O(K)|$, hence $|O(L)|=a_L(2)|O(K)|$. But $a_L(2)=\sqrt{|O(L)|}$ [2, Corollary II.2.6], hence, our results follows.

Remark 2.3. Let $K\in\mathcal{G}(3,2)$ be a lattice with an empty root system. Then K either comes from a lattice L of type A_1 or from one of type A_2. In the former case, the unit group of K is trivial by Proposition 2.2 and [2, Corollary II.2.6], whereas in the latter $|O(K)|=6$. It follows that the unit group of K is not necessarily determined by its roots system. We denote by $\mathcal{G}'(3,2)$ those lattices which contain a nontrivial root system. By [2, Corollary II.2.6], again, $|O(K)|=4$, 12 or 24 according as the type of K is A_1, A_2 or $A_1\oplus A_1\oplus A_1$.

Let K be a lattice in $\mathcal{G}'(3,2)$ and e a minimal vector of K. Denote by M the orthogonal complement of e in K. It is easy to show that M is free with discriminant 4 (see [5, Appendix]). Locally at each dyadic prime $\mathfrak{p}$, $M_{\mathfrak{p}}$ is proper $\mathfrak{p}$-modular. By Lemma 1.6, [3], there exist a vector u in M and a principal prime ideal $\mathfrak{q} = \mathcal{O}\pi$ of F such that $Q(u) = 2\pi$. The orthogonal complement of u in M is again a free lattice $\mathcal{O}v$ with $Q(v) = 2\pi$. Therefore we have $K \supset \mathcal{O}e \perp \mathcal{O}u \perp \mathcal{O}v$. Define an isometry τ on V by $\tau(e) = e$, $\tau(u) = v$ and $\tau(v) = -u$.

PROPOSITION 2.4. *Let* $p \equiv 5 \pmod 8$, *then there are four lattices in* $\mathcal{G}'(3, 2)$ *which contain* $\mathcal{O}e \perp \mathcal{O}u \perp \mathcal{O}v$, *and they are transitively permuted by* S_v *and* τ.

Proof. There is a unique dyadic prime $\mathfrak{p} = (2)$. Locally at $\mathfrak{p}$, there are two $2\mathcal{O}_\mathfrak{p}$-maximal lattices which contain $\mathcal{O}_\mathfrak{p} e \perp \mathcal{O}_\mathfrak{p} u \perp \mathcal{O}_\mathfrak{p} v$, namely

$$(\mathcal{O}_\mathfrak{p} e \perp \mathcal{O}_\mathfrak{p} u \perp \mathcal{O}_\mathfrak{p} v) + \mathcal{O}_\mathfrak{p} \tfrac{1}{2}(e + au)$$

and

$$(\mathcal{O}_\mathfrak{p} e \perp \mathcal{O}_\mathfrak{p} u \perp \mathcal{O}_\mathfrak{p} v) + \mathcal{O}_\mathfrak{p} \tfrac{1}{2}(e + av),$$

where $a \in \mathcal{O}_\mathfrak{p}^\times$. At the prime $\mathfrak{q} = \mathcal{O}\pi$, there are also two $\mathcal{O}_\mathfrak{q}$-maximal lattices which contain $\mathcal{O}_\mathfrak{q} e \perp \mathcal{O}_\mathfrak{q} u \perp \mathcal{O}_\mathfrak{q} v$. They are

$$(\mathcal{O}_\mathfrak{q} e \perp \mathcal{O}_\mathfrak{q} u \perp \mathcal{O}_\mathfrak{q} v) + \mathcal{O}_\mathfrak{q} \frac{1}{\pi}(u + bv)$$

and

$$(\mathcal{O}_\mathfrak{q} e \perp \mathcal{O}_\mathfrak{q} u \perp \mathcal{O}_\mathfrak{q} v) + \mathcal{O}_\mathfrak{q} \frac{1}{\pi}(u - bv), \qquad \text{where} \quad b \in \mathcal{O}_\mathfrak{q}^\times.$$

It is clear that there are four global lattices which contain $\mathcal{O}e \perp \mathcal{O}u \perp \mathcal{O}v$. One checks easily that they are permuted by S_v and τ.

Remark 2.5. Consider an even positive definite binary lattice M of discriminant $4p$ over $\mathbb{Z}$, $p \equiv 5 \pmod 8$. In [4], it was shown that there exist two ternary lattices K_1, K_2 in $G'(3, 2p)$ which contain $\mathbb{Z}e \perp M$, where e is a minimal vector. Moreover, K_1 and K_2 are inequivalent unless M has a nontrivial isometry. Proposition 2.4 shows that the "glueing" construction lifts K_1, K_2 to two isometric lattices over $\mathcal{O}$. The situation is not as clear if $p \equiv 1 \pmod 8$ since now there are eight lattices in $\mathcal{G}'(3, 2)$ which contain $\mathcal{O}e \perp \mathcal{O}u \perp \mathcal{O}v$ forming two sets of four lattices. Lattices in each set are isometric to one another, but not necessarily isometric to members of the other set.

Fix $p \equiv 5 \pmod 8$. We are now ready to prove the independence of the theta series arising from the lattices in $\mathcal{G}'(3, 2)$. Since our method is the same as in [2], we just indicate the changes. Let $K_1, \ldots, K_h$ be a full set of nonisometric lattices $\mathscr{G}'(3, 2)$. Each K_i contains a minimal vector e_i. As before, we consider a unary free lattice J_i in the orthogonal complement of e_i with discriminant $2\pi_i$, where $\mathfrak{q}_i = \mathcal{O}\pi_i$ is a principal prime ideal of F. If a_{ij} is the number of isometric embeddings of J_i into K_j, then

$$a_{ij} \equiv 0 \pmod{2^2}, \qquad i \neq j$$
$$a_{jj} \equiv 0 \pmod{2}, \qquad \text{but} \qquad a_{jj} \not\equiv 0 \pmod{2^2}$$

for the lattices K_j of type A_1 or A_2. If K_j is of the type $A_1 \oplus A_1 \oplus A_1$, then we have

$$a_{ij} \equiv 0 \pmod{2^3}, \qquad i \not\equiv j$$
$$a_{jj} \not\equiv 0 \pmod{2^3}.$$

Now let $\sum c_j \Theta_{K_j}(z) = 0$ be a nontrivial linear relation, where the coefficients c_j are relatively prime integers. By evaluating at each J_i and considering mod 2 and mod 2^2, we obtain $c_j \equiv 0 \pmod{2}$ for all j. This is a contradiction, and we have proved:

THEOREM 2.6. *Let $p \equiv 5 \pmod{8}$. The generalized theta series $\Theta_K(z)$ of degree one for lattices K coming from the classes in $\mathscr{G}'(3, 2)$ are linearly independent.*

REFERENCES

1. J. S. HSIA AND D. C. HUNG, Theta series of ternary and quaternary quadratic forms, *Invent. Math.* **73** (1983), 151–156.
2. J. S. HSIA AND D. C. HUNG, Theta series of quaternary quadratic forms over $\mathbb{Z}$ and $\mathbb{Z}[(1+\sqrt{p})/2]$, *Acta Arith.* **45** (1985), 75–91.
3. J. S. HSIA, Y. KITAOKA, AND M. KNESER, Representations of positive definite quadratic forms, *J. Reine Angew. Math.* **301** (1978), 132–141.
4. Y. KITAOKA, Quaternary even positive definite quadratic forms of prime discriminant, *Nagoya Math. J.* **52** (1973), 147–161.
5. Y. KITAOKA, Class numbers of quadratic forms over real quadratic fields, *Nagoya Math. J. ibid.* **66** (1977), 89–98.
6. Y. MIMURA, On 2-lattices over real quadratic integers, *Math. Sem. Notes* **7** (1979), 327–342.
7. O. T. O'MEARA, "Introduction to Quadratic Forms," Springer-Verlag, New York, 1963.
8. P. PONOMAREV, "Ternary Quadratic Forms and an Explicit Quaternary Correspondence," Queen's Paper on Pure and Applied Math., No. 46, pp. 361–371, 1977.