The Shadow Theory of Modular and Unimodular Lattices

E. M. Rains and *N. J. A. Sloane*

Information Sciences Research, AT&T Labs-Research
180 Park Avenue, Florham Park, NJ 07932-0971, U.S.A.

Apr. 27, 1998

ABSTRACT

It is shown that an n-dimensional unimodular lattice has minimal norm at most $2[n/24]+2$, unless $n=23$ when the bound must be increased by 1. This result was previously known only for even unimodular lattices. Quebbemann had extended the bound for even unimodular lattices to strongly N-modular even lattices for N in

$$\{1,2,3,5,6,7,11,14,15,23\}\ , \tag{$*$}$$

and analogous bounds are established here for odd lattices satisfying certain technical conditions (which are trivial for $N=1$ and 2). For $N>1$ in $(*)$, lattices meeting the new bound are constructed that are analogous to the "shorter" and "odd" Leech lattices. These include an odd associate of the 16-dimensional Barnes-Wall lattice and shorter and odd associates of the Coxeter-Todd lattice. A uniform construction is given for the (even) analogues of the Leech lattice, inspired by the fact that $(*)$ is also the set of square-free orders of elements of the Mathieu group M_{23}.

1. Introduction

The study of unimodular lattices (i.e. integral lattices of determinant 1) is an important chapter in the classical theory of quadratic forms. Another way to characterize a unimodular lattice is that it is equal to its dual. A *modular* lattice (the term was introduced by Quebbemann [38]; see also [39], [40]) is an integral lattice which is geometrically similar to its dual.

In other words, an n-dimensional integral lattice Λ is *modular* if there exists a similarity σ of $\mathbb{R}^n$ such that $\sigma(\Lambda^*) = \Lambda$, where Λ^* is the dual lattice. If σ multiplies norms by N, Λ is said to be *N-modular*. For example, the sporadic root lattices E_8, $F_4(\cong D_4)$, $G_2(\cong A_2)$ are respectively 1-, 2- and 3-modular. In the last two cases the modularity maps short roots to long roots.

If N is a composite number, a *strongly N-modular* lattice [39] satisfies certain additional conditions given in Section 3.

To date the study of N-modular lattices for $N > 1$ has focused on even lattices, but in the present paper we remove this restriction and also consider odd lattices.

The simplest example of an N-modular lattice for N prime is the two-dimensional lattice $C^{(N)} = \mathbb{Z} \oplus \sqrt{N}\mathbb{Z}$. The similarity σ takes (x, y) to $(\sqrt{N}y, \sqrt{N}x)$, and maps $C^{(N)*}$ to $C^{(N)}$. More generally, for any positive integer N,

$$C^{(N)} = \sum_{d|N} \sqrt{d}\mathbb{Z}$$

is a strongly N-modular lattice of dimension equal to $d(N)$, the number of divisors of N.

The main goal of this paper is to prove Theorems 1 and 2.

Theorem 1. *An n-dimensional unimodular lattice has minimal norm*

$$\mu \le 2\left[\frac{n}{24}\right] + 2 \ , \tag{1}$$

unless $n = 23$ when $\mu \le 3$.

Remarks. (1) The form of (1) suggests that dimension 24 may be special, and of course it is: there is a unique 24-dimensional lattice meeting the bound, the Leech lattice Λ_{24} (cf. [15]). The best odd lattice in dimension 24 is the "odd Leech lattice" O_{24} of minimal norm 3, and the exception to the bound in dimension 23 is necessary because of the existence of the "shorter Leech lattice" O_{23}, which also has minimal norm 3.

(2) Theorem 1 is the strongest upper bound presently known for unimodular lattices. For *even* unimodular lattices this was already known [26], but for odd unimodular lattices it was known only that

$$\mu \leq \left[\frac{n+6}{10} \right]$$

for all sufficiently large n [13].

(3) For self-dual codes the situation is similar. For doubly-even self-dual codes it was shown in [26], [27] that the minimal distance d of a code of length n satisfies

$$d \leq 4 \left[\frac{n}{24} \right] + 4 \ , \tag{2}$$

and for singly-even self-dual codes

$$d \leq 2 \left[\frac{n+6}{10} \right] \ ,$$

unless $n = 2$, 8, 12, 22, 24, 32, 48 and 72 when the bound must be increased by 2 [14]. The analogue of Theorem 1 is given in [41], where it is shown that (2) holds for all self-dual codes, unless $n \equiv 22 \pmod{24}$ when the upper bound must be increased by 2.

So in the coding analogue to Theorem 1 there are infinitely many exceptions, not just one. However, it seems very likely that equality can hold in (1) and (2), and in the bounds of Theorem 2, for only finitely many values of n (compare [26]).

(4) In the coding analogue of Theorem 1, it can be shown that any self-dual code of length $n \equiv 0 \pmod{24}$ meeting the bound in (2) must be doubly-even. We conjecture that if $n \equiv 0 \pmod{24}$ any unimodular lattice meeting the bound of Theorem 1 must be even, although we have so far not succeeded in proving this.

(5) Krasikov and Litsyn [25] have recently shown that for doubly-even self-dual codes of length n, where n is large, (2) can be improved to

$$d \leq 0.166315 \ldots n + o(n), \quad n \to \infty \ .$$

No analogous result is known for even unimodular lattices.

(6) Theorem 1 is included in Theorem 2, but is stated separately because of the importance of the unimodular case.

For strongly N-modular lattices we will restrict our attention to values of N from the set

$$\{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\} \ , \tag{3}$$

for which the corresponding *critical dimensions* $D_N = 24d(N)/\prod_{p|N}(p+1)$ are respectively

$$\{24, 16, 12, 8, 8, 6, 4, 4, 4, 2\} \ . \tag{4}$$

Theorem 2. *For N in (3), an n-dimensional strongly N-modular lattice which is rationally equivalent to the direct sum of $n/\dim C^{(N)}$ copies of $C^{(N)}$ has minimal norm*

$$\mu \leq 2\left[\frac{n}{D_N}\right] + 2 \ , \tag{5}$$

unless N is odd and $n = D_N - \dim C^{(N)}$ when

$$\mu \leq 3 \ . \tag{6}$$

Remarks. (1) The form of (5) suggests that dimension D_N may be special, and indeed in each case there is a unique lattice in that dimension meeting the bound (see Section 2).

(2) We will say that an n-dimensional strongly N-modular lattice Λ that meets the appropriate bound from Theorems 1 or 2 is *extremal.* This definition agrees with the historical usage for even lattices, but for odd unimodular lattices extremal has generally meant minimal norm $[n/8]+1$. There are just 11 such lattices with the latter property (SPLAG, Chap. 19). In view of Theorem 1 the more uniform definition proposed here seems preferable. A lattice satisfying the hypothesis of Theorem 2 is *optimal* if it has the highest minimal norm of any such lattice with the same n and N. An extremal lattice is *a priori* optimal.

(3) We conjecture that any extremal lattice of dimension a multiple of D_N must be even (compare Remark (4) above).

(4) The bound of Theorem 2 for $N \geq 11$ is quite weak, even for moderate values of n. If $N = 23$, for example, extremal lattices almost certainly do not exist in dimensions above 4. (Of course the analogous bounds for even lattices [39] are also weak.)

Section 2 gives a number of examples, some of which (the odd versions of the Barnes-Wall and Coxeter-Todd lattices, and the shorter Coxeter-Todd lattice, for instance) appear to be new.

In Section 3 we study certain Gauss sums $\gamma_\Pi(\Lambda)$ associated with a lattice Λ, show how Atkin-Lehner involutions act on theta series, and define the concept of strong modularity. Section 4 studies the shadow of a lattice. For example, Theorem 7 shows that the norm of every vector in the shadow of an odd lattice is congruent to (oddity Λ)/4 modulo $2\mathbb{Z}_2$. In Section 5 it is shown that the theta series of a lattice and its shadow are (essentially) invariant under the action of a certain modular group $\frac{1}{2}\Gamma_0(4N)^+$. The main result of this section is Corollary 3.

Section 6 contains the proofs of Theorems 1 and 2 (which make use of Corollary 2 from Section 3, Eq. (16) from Section 4, and Theorem 9 and Corollary 3 from Section 5), as well as some identities for modular functions that may be of independent interest.

In Section 7 we briefly discuss bounds for N-modular lattices not covered by Theorem 2. In the Appendix we prove a general result about the nonexistence of modular lattices in certain genera. Among other things this implies that any 7- or 23-modular lattice must satisfy the hypothesis of Theorem 2.

2. Examples of extremal modular lattices

Many examples of modular lattices meeting the bounds of Theorems 1 and 2 (and of the analogous bounds in Section 7) can be found for instance in [2], [15], [28], [31], [32], [34], [37], [38], [39]. Other examples will be constructed here. Some nonexistence results are given in [35] and [43] (see also [44], [45]).

For unimodular lattices, the highest possible minimal norm is known for dimensions $n \leq 33$ and 40–48 [13], [17], and in this range the bound of Theorem 1 is achieved precisely for $n = 8, 12, 14-24, 32$ and 40–48.

For $N = 2$, lattices achieving the bound of Theorem 2 are known (see e.g. [2] and [37]) in dimensions n = 4, 8–16, 20, 24, 28, 32, 36, 40, 44, 48, and do not exist for n = 2, 6, 18, 34; the existence for n = 22, 26, 30, 38, 42, 46 is open.

For $N = 3$, lattices meeting the bound of Theorem 2 are known (cf. [2], [32] and the present paper) for n = 4–12, 16–24, 28, 32, and do not exist for n = 2, 14, 26 and 50.

Less is known for larger values of N, for which we refer the reader to the table in [48]. (This table also has further information about many of the above lattices.)

We begin our discussion of specific constructions by noting the following generalization of a construction given in [15, Chap. 7, Theorem 26] and [2]: if C is an additive (but not necessarily linear) trace self-dual[1] code over $\mathbb{F}_4$ of length n and minimal distance d, then "Construction A"[2] produces a 3-modular lattice in dimension $2n$ with minimal norm $\mu = \min\{4, d\}$. If C

[1] That is, self-dual with respect to the inner product $Tr(u \cdot \overline{v})$ [9], [42].

[2] In other words, take the real form of the complex lattice $\{u \in \mathbb{Z}[\omega]^n : u \bmod 2 \in C\}$, where ω is a primitive cube root of unity.

is even so is the lattice (and if C is odd the shadow of the lattice is obtained by lifting the shadow of the code).

Since all lattices arising in this way share the common sublattice $(\sqrt{2}A_2)^n$, they are rationally equivalent to $(C^{(3)})^N$, where $C^{(3)} = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z}$ arises from the code C with generator matrix [1]. Thus these lattices all satisfy the hypothesis of Theorem 2. In particular, the hexacode (with $n = 6$, $d = 4$) [15, p. 82] gives rise to the Coxeter-Todd lattice K_{12}. There are two related additive self-dual codes, the shorter $(n = 5, d = 3)$ and odd $(n = 6, d = 3)$ hexacodes [9], [20], [42]. The latter can be taken to be the additive code generated by all cyclic shifts of $1\omega1000$. Under Construction A these codes become the shorter and odd Coxeter-Todd lattices $S^{(3)}$ and $O^{(3)}$ (see Theorem 3). Other examples of good additive codes over $\mathbb{F}_4$ from [9], [42] lead to optimal 3-modular lattices in dimensions $n \leq 22$, including possibly new lattices in dimensions 14, 18 and 22. Construction A applied to the dodecacode ($n = 12$, $d = 6$, [9], [20], [42]) gives rise to a neighbor of Nebe's 24-dimensional extremal 3-modular lattice [31], which has minimal norm 6 rather than 4.

As remarked above, for each N in (3) there is an especially interesting extremal strongly N-modular even lattice $E^{(N)}$ in the critical dimension D_N, having minimal norm 4. There is also a D_N-dimensional strongly N-modular *odd lattice* $O^{(N)}$ of minimal norm 3, and, when $N = 1, 3, 5, 7, 11$, a *shorter lattice* $S^{(N)}$ of dimension $D_N - 1$ (if $N = 1$) or $D_N - 2$ (if $N > 1$), also with minimal norm 3 (see Table 1). The even lattices are well known, see [38], [39]. It turns out that there is a uniform construction for all the above lattices (except for $O^{(N)}$ when N is even).

Theorem 3. *Consider the Mathieu group M_{23} acting on the Leech lattice Λ_{24}, and let $g \in M_{23}$ have order $N > 1$. (There is essentially only one class of elements of each order.) Then the sublattice Λ_g of Λ_{24} fixed by g is strongly N-modular. If N is in (3) then Λ_g is extremal of dimension D_N.*

Proof. A straightforward case-by-case verification. (The Λ_g are also described in [19], [22], [23].) ∎

Remarks. (1) We were led to this result by Quebbemann's observation in [38] (following [11]) that the function field of $\Gamma_0(p)^+$ for p prime has genus 0 exactly when p divides the order of the Monster group. Our investigations had suggested the group $\frac{1}{2}\Gamma_0(4p)^+$ and the list of

Table 1: Extremal strongly N-modular even lattice $E^{(N)}$ in the critical dimension D_N and its odd ($O^{(N)}$) and shorter ($S^{(N)}$) associates in dimensions D_N and D_N-dim $C^{(N)}$ respectively.

N	D_N	$E^{(N)}$	$O^{(N)}$	$S^{(N)}$
1	24	Λ_{24}	$O^{(1)} = O_{24}$	$S^{(1)} = O_{23}$
2	16	BW_{16}	$O^{(2)}$	—
3	12	K_{12}	$O^{(3)}$	$S^{(3)}$
5	8	$Q_8(1)$	$O^{(5)}$	$Q_6(4)^{+2}$
6	8	$G_2 \otimes F_4$	$O^{(6)}$	—
7	6	$A_6^{(2)}$	$O^{(7)}$	$\begin{bmatrix} 3 & 1 & 0 & -1 \\ 1 & 3 & 1 & 0 \\ 0 & 1 & 3 & 1 \\ -1 & 0 & 1 & 3 \end{bmatrix}$
11	4	$\begin{bmatrix} 4 & 1 & 0 & -2 \\ 1 & 4 & 2 & 0 \\ 0 & 2 & 4 & 1 \\ -2 & 0 & 1 & 4 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix} \oplus \begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix}$
14	4	$\begin{bmatrix} 4 & 1 & 0 & -1 \\ 1 & 4 & 1 & 0 \\ 0 & 1 & 4 & 1 \\ -1 & 0 & 1 & 4 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 5 \end{bmatrix} \oplus \begin{bmatrix} 3 & 1 \\ 1 & 5 \end{bmatrix}$	—
15	4	$\begin{bmatrix} 4 & 2 & 2 & 1 \\ 2 & 4 & 1 & 2 \\ 2 & 1 & 6 & 3 \\ 1 & 2 & 3 & 6 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 & 0 & -1 \\ 1 & 3 & 1 & 0 \\ 0 & 1 & 6 & 2 \\ -1 & 0 & 2 & 6 \end{bmatrix}$	—
23	2	$\begin{bmatrix} 4 & 1 \\ 1 & 6 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 8 \end{bmatrix}$	—

primes 2, 3, 5, 7, 11, 23. It was natural to conjecture that these primes also arose from some finite simple group, the obvious candidates being M_{23}, M_{24} and Co_2. The theta series of the sublattices Λ_g given by Koike [22] then suggested the theorem.

(2) It has been observed ([18], [23], [24]) that the theta series of the fixed sublattices Λ_g for $g \in Co_0$ transform nicely under Atkin-Lehner involutions. For $g \in M_{23}$ this can be independently deduced from the modularity of Λ_g, using Corollary 2 (this does not seem to have been noticed before). Indeed, it turns out that every relation between these theta series under Atkin-Lehner involutions can be explained by an appropriate modularity.

(3) There are two conjugacy classes of M_{23} with orders not in (3), those of orders 4 and 8. For order 4 the fixed sublattice is the 10-dimensional 4-modular lattice called Q_{10} in [16], [19]. For order 8 it is a 6-dimensional 8-modular even lattice with minimal norm 4 and automorphism group of order 384 [19].

Theorem 4. *(a) Consider M_{23} acting on the odd Leech lattice O_{24}, and suppose $g \in M_{23}$ has odd order $N > 1$. The fixed sublattice Λ_g is a strongly N-modular D_N-dimensional lattice $O^{(N)}$ of minimal norm 3. (b) Consider M_{23} acting on $O_{23} \oplus \mathbb{Z}$. Again supposing that N is odd, the fixed sublattice has the form $C^{(N)} \oplus D$, where D has dimension 0 if $N = 15$ or 23, and otherwise is an N-modular lattice $S^{(N)}$ of dimension $D_N - \dim C^{(N)}$ and minimal norm 3.*

Proof. Again a case-by-case verification. ∎

Since there is no exceptional case in Theorem 2 when N is even, the shorter lattices $S^{(N)}$ do not exist. There are however odd lattices $O^{(N)}$ for $N = 2$, 6 and 14, although the construction of Theorem 4 does not work. The most interesting of these cases is $N = 2$, for which $S^{(2)}$ can be constructed as follows.

Let L denote the 16-dimensional 2-modular lattice BW_{16}, with minimal norm 4, and take $v \in L$ with $v \cdot v = 6$, $w \in L^*$ with $w \cdot w = 3$. Then $O^{(2)} = \langle L', w \rangle$ where $L' = \{u \in L : u \cdot v \in 2\mathbb{Z}\}$.

In fact all the $O^{(N)}$ and $S^{(N)}$ in Table 1 can be found by a similar neighboring process, starting from the even lattice $E^{(N)}$. In each case there are four equivalence classes of $E^{(N)}/2E^{(N)}$ under the action of $\mathrm{Aut}(E^{(N)})$, with minimal norms 0, 4, 6, 8. Relative to a vector of norm 4, the even neighbor is $E^{(N)}$ again, and the odd neighbor is $C^{(N)} \oplus S^{(N)}$. Relative to a vector of norm 8, the even neighbor is an analog of the Niemeier lattice of type A_1^{24}, while the odd neighbor is $O^{(N)}$.

All the lattices in Table 1 are unique, although we only discuss the uniqueness of $O^{(N)}$ and $S^{(N)}$ here. It can be shown that if Λ is any N-modular lattice of norm 3 in the same dimension as $S^{(N)}$, then the even neighbors of $C^{(N)} \oplus S^{(N)}$ must be extremal; this implies the uniqueness of $S^{(N)}$. A similar argument (based on the fact that the analogue of A_1^{24} has the minimal nonzero number of roots) shows the uniqueness of $O^{(N)}$ for N odd. For N even, one can show (see Theorem 8) that the even neighbor of such a lattice must be extremal, and again the uniqueness of $O^{(N)}$ follows.

Finally, we comment on some of the other entries in Table 1. The 5-modular lattices $Q_8(1)$ and $Q_6(4)^{+2}$ are connected with the ring of icosian integers — see [12] (and [36]). $O^{(5)}$, $O^{(6)}$ and $O^{(7)}$ may be new: they have minimal norm 3, automorphism groups of orders 384, 96 and 48, respectively, and 16, 16 and 8 minimal vectors (see [48]). The remaining entries are self-explanatory.

3. Modular lattices and Atkin-Lehner involutions

A lattice Λ is *rational* (resp. *integral*) if $u \cdot v \in \mathbb{Q}$ (resp. $\mathbb{Z}$) for all $u, v \in \Lambda$. Let Π be a (possibly infinite) set of rational primes. The Π-*dual* $\Lambda^{*\Pi}$ of Λ consists of the vectors $v \in \Lambda \otimes \mathbb{Q}$ such that $v \cdot \Lambda \subseteq \mathbb{Z}_p$ for $p \in \Pi$ and $v \cdot \Lambda^* \subseteq \mathbb{Z}_p$ for $p \notin \Pi$.

In particular, with Ω the set of all rational primes,

$$\Lambda^{*\emptyset} = \Lambda, \quad \Lambda^{*\Omega} = \Lambda^*, \quad (\Lambda^{*\Pi})^{*\Pi} = \Lambda \ ,$$

and, more generally,

$$(\Lambda^{*\Pi_1})^{*\Pi_2} = \Lambda^{*(\Pi_1 \Delta \Pi_2)}$$

where Δ denotes a symmetric difference. (We will also need the notion $\overline{\Pi} = \Omega \setminus \Pi$, and when there is no possibility of confusion we abbreviate $\Pi = \{p\}$ to p.) Furthermore,

$$\Lambda^{*\Pi} \otimes \mathbb{Z}_p = \begin{cases} \Lambda^* \otimes \mathbb{Z}_p, & p \in \Pi \ , \\ \Lambda \otimes \mathbb{Z}_p, & p \notin \Pi \ . \end{cases}$$

We also define

$$\begin{aligned} \det_{\Pi}(\Lambda) &= (\det \Lambda / \det \Lambda^{*\Pi})^{1/2} \\ &= [\Lambda^{*\Pi} : \Lambda \cap \Lambda^{*\Pi}]/[\Lambda : \Lambda \cap \Lambda^{*\Pi}] \ , \end{aligned}$$

which is equal to the Π-part of $\det \Lambda$.

Suppose now that Λ is integral. The *level* of Λ is the smallest number l' such that $\sqrt{l'}\Lambda^*$ is integral. If Λ is even, the *even-level* of Λ is the smallest number l such that $\sqrt{l}\Lambda^*$ is even. The Π-levels l'_Π and l_Π are defined analogously, replacing Λ^* by $\Lambda^{*\Pi}$.

Quebbemann [39] associates certain Gauss sums with Λ. We do the same, but in a slightly more explicit fashion. Let

$$\gamma_2(\Lambda) = \xi^{\mathrm{oddity}(\Lambda)}, \quad \gamma_p(\Lambda) = \xi^{-p\text{-excess}(\Lambda)} \ ,$$

for an odd prime p, where $\xi = e^{\pi i/4}$ and the oddity and p-excess are as in Chap. 15 of [15], and define

$$\gamma_\Pi(\Lambda) = \prod_{p \in \Pi} \gamma_p(\Lambda) \ . \tag{7}$$

In particular, the product (or oddity) formula [15, Chap. 15, Eq. (30)] becomes

$$\gamma_\Omega(\Lambda) = \xi^{\dim \Lambda} \ .$$

The following lemma shows that $\gamma_\Pi(\Lambda)$ agrees with Quebbemann's Gauss sum.

Lemma 1. *For an even lattice* Λ*,*

$$\gamma_\Pi(\Lambda) = (\det_\Pi\ \Lambda)^{-1/2} \sum_{v \in \Lambda^{*\Pi}/\Lambda} e^{\pi i v \cdot v}\ . \tag{8}$$

Proof. From [46, Chap. 5], the right-hand side of (8) is multiplicative under direct sums of lattices and disjoint unions of prime sets, and is invariant under rational equivalence of lattices. It suffices therefore to consider only the cases where Π is a singleton and $\Lambda = \sqrt{a}\mathbb{Z}$, where a ranges over $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$. This is a straightforward problem involving one-dimensional Gauss sums. ∎

It is classical (cf. [30]) that if Λ is a lattice of even-level N, then its theta series Θ_Λ is a modular form for $\Gamma_0(N)$ with respect to an appropriate character. Kitaoka [21] describes how a somewhat larger subset of $SL_2(\mathbb{Z})(z)$ acts on Θ_Λ, up to an unspecified constant. Quebbemann [39] has determined this constant, but only for one representative from each coset of $\Gamma_0(N)$. We shall make use of the following more explicit result. Here $\Pi(m)$ denotes the set of primes dividing m, and $(\frac{m}{n})$ denotes the Kronecker-Jacobi symbol [10, p. 28].

Theorem 5. *Let* Λ *be an even lattice of even-level* N*, and let* $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be any element of* $SL_2(\mathbb{Z})$ *such that* cd *is a multiple of* N*. Then*

$$\Theta_\Lambda((az+b)/(cz+d)) = (\det_{\Pi(d)}\ \Lambda)^{-1/2} \chi_{c,d}(\Lambda) \left(\sqrt{cz+d}\right)^{\dim\Lambda} \Theta_{\Lambda^{*\Pi(d)}}(z), \tag{9}$$

where in both cases the square root is that with positive real part, and $\chi_{c,d}(\Lambda)$ *is equal to*

$$\gamma_{\Pi(d)}(\Lambda)^{-1} \left(\frac{c}{\det_{\Pi(d)}\ \Lambda}\right) \left(\frac{d}{\det_{\Pi(c)}\ \Lambda}\right)$$

multiplied either by

$$\left(\frac{d}{|c|}\right)^{\dim\Lambda} \left(\frac{\left(\frac{-1}{c}\right)}{\det\ \Lambda}\right) \xi^{-(c-1)\dim\Lambda} \tag{10}$$

if c *is odd, or by*

$$\left(\frac{c}{d}\right)^{\dim\Lambda} \left(\frac{\left(\frac{-1}{d}\right)}{\det\ \Lambda}\right) \xi^{(d-1)\dim\Lambda}. \tag{11}$$

if c *is even.*

For the proof, we need a lemma describing how Gauss sums behave as a lattice is rescaled.

Lemma 2. *Let Λ be a rational lattice, and let Π be any set of primes. Let t be any positive integer, with Π-part t_1 and $\overline{\Pi}$-part t_2. If $2 \notin \Pi$, then*

$$\gamma_\Pi(\sqrt{t}\Lambda)/\gamma_\Pi(\Lambda) = \left(\frac{t_1}{\det_{\overline{\Pi}} \Lambda}\right)\left(\frac{t_2}{\det_\Pi \Lambda}\right)\left(\frac{t_2}{t_1}\right)^{\dim\Lambda}\left(\frac{\left(\frac{-1}{t_1}\right)}{\det \Lambda}\right)\xi^{-(t_1-1)\dim\Lambda}, \qquad (12)$$

and if $2 \in \Pi$, then

$$\gamma_\Pi(\sqrt{t}\Lambda)/\gamma_\Pi(\Lambda) = \left(\frac{t_1}{\det_{\overline{\Pi}} \Lambda}\right)\left(\frac{t_2}{\det_\Pi \Lambda}\right)\left(\frac{t_1}{t_2}\right)^{\dim\Lambda}\left(\frac{\left(\frac{-1}{t_2}\right)}{\det \Lambda}\right)\xi^{(t_2-1)\dim\Lambda}. \qquad (13)$$

Proof. It follows from the definition of the p-excess that if p is any odd prime and t is relatively prime to p then

$$\gamma_p(\sqrt{t}\Lambda)/\gamma_p(\Lambda) = \left(\frac{t}{\det_p \Lambda}\right).$$

Furthermore, if p does not divide $\det \Lambda$, then

$$\begin{aligned}\gamma_p(\sqrt{p}\Lambda)/\gamma_p(\Lambda) &= \xi^{-(p-1)\dim\Lambda}\left(\frac{\det \Lambda}{p}\right)\\ &= \xi^{-(p-1)\dim\Lambda}\left(\frac{\left(\frac{-1}{p}\right)}{\det \Lambda}\right)\left(\frac{p}{\det \Lambda}\right),\end{aligned}$$

by reciprocity.

For $p = 2$ and t odd, the result clearly depends only on the congruence class of t mod 8. Consequently, we may assume that t is a prime not dividing $\det \Lambda$. Then

$$\begin{aligned}\gamma_2(\sqrt{t}\Lambda)/\gamma_2(\Lambda) &= (\gamma_t(\sqrt{t}\Lambda)/\gamma_t(\Lambda))^{-1}(\gamma_{\overline{\{2,t\}}}(\sqrt{t}\Lambda)/\gamma_{\overline{\{2,t\}}}(\Lambda))^{-1}\\ &= \xi^{(t-1)\dim\Lambda}\left(\frac{\left(\frac{-1}{t}\right)}{\det \Lambda}\right)\left(\frac{t}{\det \Lambda}\right)\left(\frac{t}{\det_{\overline{\{2,t\}}} \Lambda}\right)\\ &= \xi^{(t-1)\dim\Lambda}\left(\frac{\left(\frac{-1}{t}\right)}{\det \Lambda}\right)\left(\frac{t}{\det_2 \Lambda}\right).\end{aligned}$$

We can now write, for $2 \notin \Pi$:

$$\gamma_\Pi(\sqrt{t}\Lambda)/\gamma_\Pi(\Lambda) = (\gamma_\Pi(\sqrt{t_1 t_2}\Lambda)/\gamma_\Pi(\sqrt{t_1}\Lambda))(\gamma_\Pi(\sqrt{t_1}\Lambda)/\gamma_\Pi(\Lambda)).$$

The first ratio is

$$\left(\frac{t_2}{\det_\Pi(\sqrt{t_1}\Lambda)}\right) = \left(\frac{t_2}{t_1}\right)^{\dim\Lambda}\left(\frac{t_2}{\det_\Pi \Lambda}\right)$$

while the second is

$$\begin{aligned}
\gamma_\Pi(\sqrt{t_1}\Lambda)/\gamma_\Pi(\Lambda) &= (\gamma_{\overline{\Pi}}(\sqrt{t_1}\Lambda)/\gamma_{\overline{\Pi}}(\Lambda))^{-1} \\
&= (\gamma_2(\sqrt{t_1}\Lambda)/\gamma_2(\Lambda))^{-1}(\gamma_{\overline{\Pi\cup\{2\}}}(\sqrt{t_1}\Lambda)/\gamma_{\overline{\Pi\cup\{2\}}}(\Lambda))^{-1} \\
&= \xi^{-(t_1-1)\dim\Lambda}\left(\frac{\left(\frac{-1}{t_1}\right)}{\det\Lambda}\right)\left(\frac{t_1}{\det_2\Lambda}\right)\left(\frac{t_1}{\det_{\overline{\Pi\cup\{2\}}}\Lambda}\right) \\
&= \xi^{-(t_1-1)\dim\Lambda}\left(\frac{\left(\frac{-1}{t_1}\right)}{\det\Lambda}\right)\left(\frac{t_1}{\det_{\overline{\Pi}}\Lambda}\right).
\end{aligned}$$

This establishes (12). (13) then follows from the oddity formula. ∎

Proof of Theorem 5. We first suppose $c > 0$. Quebbemann [39] shows that when $a = 1$ and $c|N$,

$$\Theta_\Lambda((z+b)/(cz+d)) = (\det_{\Pi(d)}\Lambda)^{-1/2}\xi^{-\dim\Lambda}\gamma_{\Pi(c)}(\sqrt{c}\Lambda)\left(\sqrt{cz+d}\right)^{\dim\Lambda}\Theta_{\Lambda^{*\Pi(d)}}(z).$$

(To be precise, [39] has $\gamma_{\Pi(c)}(\sqrt{c}\Lambda^{*\Pi(c)})$, but since Λ and $\Lambda^{*\Pi(c)}$ are rationally equivalent, this is the same as $\gamma_{\Pi(c)}(\sqrt{c}\Lambda)$.) The argument in [39] never uses the fact that c divides N, and can be easily modified to show that for arbitrary $a > 0$,

$$\Theta_\Lambda((az+b)/(cz+d)) = (\det_{\Pi(d)}\Lambda)^{-1/2}\xi^{-\dim\Lambda}\gamma_{\Pi(c)}(\sqrt{ac}\Lambda)\left(\sqrt{cz+d}\right)^{\dim\Lambda}\Theta_{\Lambda^{*\Pi(d)}}(z).$$

If c is odd, the lemma implies

$$\begin{aligned}
\xi^{-\dim\Lambda}\gamma_{\Pi(c)}(\sqrt{ac}\Lambda) &= \left(\xi^{-\dim\Lambda}\gamma_{\Pi(c)}(\Lambda)\right)\left(\frac{c}{\det_{\overline{\Pi(c)}}\Lambda}\right)\left(\frac{a}{\det_{\Pi(c)}\Lambda}\right)\cdot \\
&\qquad\cdot\left(\frac{a}{c}\right)^{\dim\Lambda}\left(\frac{\left(\frac{-1}{c}\right)}{\det\Lambda}\right)\xi^{-(c-1)\dim\Lambda}\cdot \\
&= \gamma_{\Pi(d)}(\Lambda)^{-1}\left(\frac{c}{\det_{\Pi(d)}\Lambda}\right)\left(\frac{d}{\det_{\Pi(c)}\Lambda}\right)\cdot \\
&\qquad\cdot\left(\frac{d}{c}\right)^{\dim\Lambda}\left(\frac{\left(\frac{-1}{c}\right)}{\det\Lambda}\right)\xi^{-(c-1)\dim\Lambda},
\end{aligned}$$

where the second step follows from the oddity formula and the fact that $ad \bmod c = 1$. For $a \le 0$, we use the fact that Λ is even, so the result can depend only on the value of $a \bmod c$.

For c even, we do not, in general have $\left(\frac{a}{2}\right) = \left(\frac{d}{2}\right)$, so the above argument fails. However, again using the fact that the result only depends on the value of $a \bmod c$, we can arrange that $a \equiv d \pmod 8$, and then an analogous argument can be used.

For c negative ($c = 0$ is trivial), we apply the result to $-S$, and use the fact that $\sqrt{-cz-d} = i\sqrt{cz+d}$. For c odd,

$$i^{\dim\Lambda}\chi_{-c,-d}(\Lambda) = \chi_{c,d}(\Lambda)\left(-i\left(\frac{-1}{c}\right)\xi^{2c}\right)^{\dim\Lambda},$$

while for c even,

$$i^{\dim\Lambda}\chi_{-c,-d}(\Lambda) = \chi_{c,d}(\Lambda)\left(i\left(\frac{-1}{d}\right)\xi^{-2d}\right)^{\dim\Lambda}.$$

But for odd integers n, $\left(\frac{-1}{n}\right)\xi^{2n} = i$, so in either case,

$$\chi_{c,d}(\Lambda)\left(\sqrt{cz+d}\right)^{\dim\Lambda} = \chi_{-c,-d}(\Lambda)\left(\sqrt{-cz-d}\right)^{\dim\Lambda},$$

and so the above formulae also hold if c is negative. ∎

Remarks. (1) There is an apparent inconsistency in (9). Since

$$\Theta_{\Lambda^{*\Pi(d)}}\left(z + \frac{N}{\gcd(c,N)}\right) = \Theta_{\Lambda^{*\Pi(d)}}(z),$$

$\chi_{c,d}(\Lambda)$ must be periodic in d of period $cN/\gcd(c,N)$. For c odd or $c \equiv 0 \pmod 8$ this is manifestly true, but otherwise (11) appears to have the wrong period. For instance, for $c \equiv 4 \pmod 8$,

$$\chi_{c,d+(cN/\gcd(c,N))}(\Lambda) = (-1)^{\lambda+\dim\Lambda}\ \chi_{c,d}(\Lambda),$$

where $\lambda = \log_2(\det_2\Lambda)$. However, since $N|cd$, it follows that in the 2-adic Jordan decomposition of Λ the forms of levels 1 and 4 are both Type II and so have even dimension. This implies that $\lambda \equiv \dim\Lambda \pmod 2$.

Similarly, for $c \equiv \pm 2 \pmod 8$, the correct period is restored by the identities

$$\lambda \equiv \dim\Lambda \equiv 0 \pmod 2,$$
$$\left(\frac{-1}{\det\Lambda}\right) = (-1)^{(\dim\Lambda)/2}.$$

If both c and d are odd (so Λ has odd even-level), then similar reasoning allows us to simplify $\chi_{c,d}(\Lambda)$ to

$$\chi_{c,d}(\Lambda) = \gamma_{\Pi(d)}(\Lambda)^{-1}\left(\frac{c}{\det_{\Pi(d)}\Lambda}\right)\left(\frac{d}{\det_{\Pi(c)}\Lambda}\right).$$

(2) When N divides c, the usual formula [30, Theorem 4.9.3] for the action of $\Gamma_0(N)$ on the theta series of lattices of even-level N can be recovered with the help of the identity

$$\xi^{(t-1)} = \epsilon_t\left(\frac{-2}{t}\right) = \epsilon_t^{-1}\left(\frac{2}{t}\right),$$

for odd t, where $\epsilon_t = 1$ if $t \equiv 1 \pmod 4$ and $\epsilon_t = i$ if $t \equiv 3 \pmod 4$.

If Λ is any integral lattice of level N, $\sqrt{2}\Lambda$ is an even lattice of even-level dividing $4N$. We can apply Theorem 5 to obtain:

Corollary 1. *Let Λ be an integral lattice of level N, and let $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be any element of $SL_2(\mathbb{Z})$ such that cd is a multiple of $2N$. Then (9) holds if either d is odd and b is even, or c is odd and a is even.*

A *modularity* σ of an integral lattice Λ is a similarity mapping $\Lambda^{*\Pi}$ to Λ for some set of primes Π. We say that σ has *level* N (or is an N*-modularity*) if σ multiplies norms by N; Π is then the set of primes dividing N. A 1-modularity is just an automorphism of Λ.

Corollary 2. *Suppose Λ has even-level N and admits an m-modularity. Then for any matrix*

$$W_m = m^{-1/2} \begin{pmatrix} ma & b \\ mc & d \end{pmatrix} \tag{14}$$

of determinant 1*, with d a multiple of m and mc a multiple of N, we have*

$$\Theta_\Lambda|_{W_m} = \chi_{c,d}(\Lambda)\Theta_\Lambda.$$

Proof. Note that

$$\det{}_{\Pi(m)} \Lambda = \left(\frac{\det \Lambda}{\det \Lambda^{*\Pi(m)}}\right)^{1/2} = \det \sigma = m^{(\dim \Lambda)/2},$$

and $\sqrt{m}\Lambda^{*\Pi(m)}$ is isometric to Λ, where the isometry is $\sigma/\sqrt{m}$. Applying Theorem 5, we find

$$\begin{aligned} \Theta_\Lambda((amz+b)/(cmz+d)) &= (\det{}_{\Pi(d)}\Lambda)^{-1/2}\chi_{c,d}(\Lambda)\left(\sqrt{cmz+d}\right)^{\dim\Lambda}\Theta_{\Lambda^{*\Pi(d)}}(mz) \\ &= m^{-(\dim\Lambda)/4}\chi_{c,d}(\Lambda)\left(\sqrt{cmz+d}\right)^{\dim\Lambda}\Theta_{\sqrt{m}\Lambda^{*\Pi(m)}}(z) \\ &= \chi_{c,d}(\Lambda)\left(\sqrt{m^{1/2}cz+m^{-1/2}d}\right)^{\dim\Lambda}\Theta_\Lambda(z). \qquad \blacksquare \end{aligned}$$

The matrix W_m in (14) is called an *Atkin-Lehner involution* [1] of order m. The next result combines known properties of these involutions with a slight generalization of a result of Nebe [33] on modularities. We omit the proof.

Theorem 6. *If W_{m_1} and W_{m_2} are Atkin-Lehner involutions then $W_{m_1}W_{m_2}$ is an Atkin-Lehner involution of level $m_1m_2/gcd(m_1,m_2)^2$. Moreover, W_m^{-1} is an Atkin-Lehner involution of level m. If σ_1 is an m_1-modularity and σ_2 is an m_2-modularity then $\sigma_1\sigma_2/gcd(m_1,m_2)$ is a modularity of level $m_1m_2/gcd(m_1,m_2)^2$. Moreover, if σ is an m-modularity then so is $m\sigma^{-1}$.*

It follows from Theorem 6 that the number of distinct levels of modularities of a lattice is a power of 2, and indeed the levels have a natural elementary abelian 2-group structure. Moreover, the total number of modularities is equal to the number of levels of modularity times $|\operatorname{Aut}\Lambda|$.

We will say that an integral lattice Λ is $\{l_1, l_2, \ldots\}$-*modular* if it has modularities of levels $l_1, l_2, \ldots$. Two special cases warrant a shorthand notation. (i) Λ is N-*modular* if its level divides N and Λ is $\{1, N\}$-modular. (ii) Λ is *strongly* N-*modular* if its level divides N and Λ is $\{m : m \| N\}$-modular, where $a\|b$ means $a|b$ and $gcd(a, b/a) = 1$.

Corollary 2 states that if Λ is an even $\{l_1, l_2, \ldots\}$-modular lattice of even-level N, then its theta series is an automorphic form for the group $\Gamma_0(N)^{+\{l_1,l_2,\ldots\}}$, i.e. the group generated by $\Gamma_0(N)$ together with all its Atkin-Lehner involutions of levels $l_1, l_2, \ldots$. For ease in discussing strongly modular lattices we abbreviate $\Gamma_0(N)^{+\{m:m\|N\}}$ to $\Gamma_0(N)^+$.

If Γ is any modular group, $\frac{1}{2}\Gamma$ will denote the group $\left\{ \begin{pmatrix} a & 2b \\ c/2 & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \right\}$.

Corollary 1 implies that if Λ is an $\{l_1, l_2, \ldots\}$-modular lattice of level N, then its theta series is an automorphic form for the group

$$\frac{1}{2}\Gamma_0(4N)^{+\{4,l_1,l_2,\ldots\}}, \quad \text{if } N \text{ is odd} . \tag{15}$$

The initial 4 arises because $\sqrt{2}\Lambda$ has an obvious 4-modularity. As a special case, the theta series of any lattice of odd level is an automorphic form for $\frac{1}{2}\Gamma_0(4N)^{+\{4\}}$ (a subgroup of $\Gamma_0(N)$). If N is even, (15) must be replaced by

$$\frac{1}{2}\Gamma_0(4N)^{+\{4e_1,4e_2,\ldots,d_1,d_2,\ldots\}} ,$$

where $e_1, e_2, \ldots$ are the even l_i's and d_1, $d_2, \ldots$ are the odd l_i's.

4. Shadows

Let Λ be an integral lattice, or more generally a 2-integral lattice (i.e. $u \cdot v \in \mathbb{Z}_2$ for all $u, v \in \Lambda$), and set $\Lambda_0 = \{u \in \Lambda : u \cdot u \in 2\mathbb{Z}_2\}$. If Λ is even, $\Lambda = \Lambda_0$; otherwise Λ_0 is a sublattice of index 2. Λ_0 is called the even sublattice of Λ.

Following [13], [14], we define the *shadow* $S(\Lambda)$ to be Λ^* if Λ is even, $(\Lambda_0)^* \setminus \Lambda^*$ if Λ is odd. Equivalently,

$$S(\Lambda) = \{v \in \Lambda \otimes \mathbb{Q} \ : \ 2u \cdot v \equiv u \cdot u \pmod{2\mathbb{Z}_2} \quad \text{for all} \quad u \in \Lambda\} .$$

Also

$$\Theta_{S(\Lambda)}(z) = (\det\ \Lambda)^{1/2} \left(\frac{\xi}{\sqrt{z}}\right)^{\dim \Lambda} \Theta_\Lambda \left(1 - \frac{1}{z}\right) \ . \tag{16}$$

We also define the Π-*shadow* $S_\Pi(\Lambda)$: if $2 \in \Pi$,

$$S_\Pi(\Lambda) = S(\Lambda^{*_{\overline{\Pi}}}) \ ,$$

and if $2 \notin \Pi$,

$$S_\Pi(\Lambda) = \sqrt{l_2'} S(\sqrt{l_2'} \Lambda^{*_{\overline{\Pi}}})$$

where l_2' is the 2-level of Λ. The Π-shadow is a coset of the Π-dual Λ^{*_Π}, and in fact $v \pm w \in \Lambda^{*_\Pi}$ for $v, w \in S_\Pi(\Lambda)$. In particular, $S_\Omega(\Lambda) = S(\Lambda)$ is a coset of Λ^*, and $S_\emptyset(\Lambda)$ is a coset of Λ. The theta-series of $S_\Pi(\Lambda)$ may be computed from Corollary 1 and (16).

It is clear from the definition of $S(\Lambda)$ that any two vectors in the same coset of Λ in $S(\Lambda)$ have the same norm modulo $2\mathbb{Z}_2$. If Λ has odd determinant, we can say more.

Theorem 7. *Let Λ be a 2-integral lattice of odd determinant and let Π be a set of rational primes. Then every vector in $S_\Pi(\Lambda)$ has norm $\equiv$ (oddity $\Lambda)/4 \pmod{2\mathbb{Z}_2}$.*

Proof. We give three proofs. It suffices to consider $\Pi = \Omega$, since $\Lambda^{*_{\overline{\Pi}}}$ satisfies the hypotheses and has the same oddity.

First proof. By scaling Λ we may assume Λ is integral. Since Λ has odd determinant, $\Lambda^{*_2} = \Lambda$. Applying Corollary 1, we have

$$\Theta_\Lambda \Big|_{\begin{bmatrix} 1+N^2 & -N^2 \\ N^2 & 1-N^2 \end{bmatrix}} = \chi_{N^2, 1-N^2}(\Lambda) \Theta_{\Lambda^{*_2}} \ .$$

Now $\chi_{N^2,1-N^2}(\Lambda) = \gamma_2(\Lambda)^{-1}$. Since

$$\begin{bmatrix} 1+N^2 & -N^2 \\ N^2 & 1-N^2 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -N^2 \\ 0 & 1 \end{bmatrix} \ ,$$

we have

$$\Theta_{S(\Lambda)}(z - N^2) = \gamma_2(\Lambda)^{-1} \Theta_{S(\Lambda)}(z) \ .$$

In other words,

$$e^{-\pi i N^2 v \cdot v} = e^{-\frac{2\pi i}{8}\ \mathrm{oddity}\Lambda}$$

for all $v \in S(\Lambda)$.

Second proof. Since the desired result is purely 2-adic, we may localize at the prime 2. Because $S(\Lambda_1 \oplus \Lambda_2) = S(\Lambda_1) \oplus S(\Lambda_2)$, the result is preserved under direct summation, so it suffices to consider indecomposable 2-adic quadratic forms. It is straightforward to verify that the theorem holds for each of the six classes of 1- or 2-dimensional forms of unit determinant.

Third proof. Assume Λ is integral and odd (Λ even is trivial). Since $\Lambda_0 \subseteq \Lambda$ and oddity is a rational invariant,

$$\begin{aligned}
\gamma_2(\Lambda) = \gamma_2(\Lambda_0) &= (\det_2 \Lambda_0)^{-1/2} \sum_{v \in \Lambda_0^{*2}/\Lambda_0} e^{\pi i v \cdot v} \\
&= \frac{1}{2} \sum_{v \in \Lambda/\Lambda_0} e^{\pi i v \cdot v} + \sum_{v \in S_2(\Lambda)/\Lambda} e^{\pi i v \cdot v} \ .
\end{aligned}$$

The first sum is $1 - 1 = 0$, so $e^{\pi i u \cdot v} = e^{\pi i \text{ oddity}/4}$. ∎

Remarks. (1) For unimodular lattices, Theorem 7 together with the product formula implies that for $v \in S(\Lambda)$, $v \cdot v \equiv (\dim \Lambda)/4 \pmod 2$, a result that has been rediscovered several times (see [3], [4], [13], [29], [47]). (2) The third proof can be used to extend Lemma 1 to integral lattices, since it proves that

$$\gamma_2(\Lambda) = (\det_2 \Lambda)^{-1/2} \sum_{v \in S_2(\Lambda)/\Lambda} e^{\pi i v \cdot v} \ .$$

Genus of Λ_0. Assume Λ is odd. Since the even sublattice Λ_0 is defined 2-adically, its genus can be computed from that of Λ. (There is no change in the p-adic genus for $p \neq 2$.) Indeed, the change in the genus depends only on the unit form in the 2-adic Jordan decomposition of Λ.

When the oddity is not zero, the existence conditions for 1- and 2-dimensional forms [15, Theorem 11 of Chap. 15] and the fact that oddity is a rational invariant leave just one possibility. When the oddity is zero, Λ_0 has a form at level 2, which from the existence conditions could be either Type I or II. But by Theorem 7, every vector in Λ_0^* has integral norm. It follows that the form at level 2 must be Type II. We thus obtain the list of transforms shown in Table 2 (using the notation of [15, Chap. 15]).

To avoid undue proliferation of parentheses we adopt the conventions that the operation $\Lambda \to \Lambda_0$ takes precedence over $\Lambda \to \Lambda^{*2}$, and both take precedence over $\Lambda \to \sqrt{2}\Lambda$. Thus $\sqrt{2}\Lambda_0^{*2}$ means $\sqrt{2}((\Lambda_0)^{*2})$.

Table 2: Genus of Λ_0 in terms of genus of Λ.

genus (Λ)	genus (Λ_0)
$[1^{\pm n}]_0$	$1^{\pm(n-2)} : 2^2$
$[1^{\pm n}]_1$	$1^{\pm(n-1)} : [4^1]_1$
$[1^{\pm n}]_2$	$1^{\pm(n-2)}[2^2]_2$
$[1^{\pm n}]_3$	$1^{\mp(n-1)} : [4^{-1}]_3$
$[1^{\pm n}]_4$	$1^{\mp(n-2)} : 2^{-2}$
$[1^{\pm n}]_5$	$1^{\mp(n-1)} : [4^{-1}]_5$
$[1^{\pm n}]_6$	$1^{\pm(n-2)}[2^2]_6$
$[1^{\pm n}]_7$	$1^{\pm(n-1)} : [4^1]_7$

Theorem 8. *Let Λ be an odd $\{2\}$-modular lattice with dimension and oddity o both divisible by 4. Then $\Lambda' = \sqrt{2}\Lambda_0^{*_2}$ is an integral lattice, and $\Lambda'' = (\Lambda')'$ is an even $\{2\}$-modular lattice, rationally equivalent to Λ. In fact, every modularity of Λ is a modularity of Λ''.*

We call Λ'' the *even neighbor* of Λ.

Proof. The 2-adic genus of Λ must be $[1^{n/2}\, 2^{n/2}]_o$. From Table 2, the genera of Λ_0 and Λ' are respectively $1^{(n-4)/2}\, [2^{(n+4)/2}]_o$ and $[1^{(n+4)/2}]_o\, 2^{(n-4)/2}$, and so Λ' is integral. Then $(\Lambda')_0$ has 2-adic genus $1^{n/2} : 2^{n/2}$ if $o = 0$ and $1^{-n/2} : 2^{-n/2}$ if $o = 4$. So Λ'' is even.

If σ is a modularity of Λ of odd level, then it is still a modularity at each step of the construction. If σ is a 2-modularity, then $\Lambda'' = \sigma(\sigma\Lambda_0^{*_2})_0^{*_2}$. But then $\Lambda_0 \subseteq \Lambda'' \subseteq \sigma\Lambda_0^{*_2}$, and $\Lambda_0 \subseteq \sigma(\Lambda'')^{*_2} \subseteq \sigma\Lambda_0^{*_2}$. Since there is only one even lattice between Λ_0 and $\sigma\Lambda_0^{*_2}$, and both Λ'' and $\sigma(\Lambda'')^{*_2}$ are even (from the genus of Λ''), it follows that they are the same lattice, and thus σ is a 2-modularity of Λ''.

The remaining modularities carry over to Λ' by Theorem 6. Since $\Lambda \cap \Lambda'' = \Lambda_0$, Λ and Λ'' are clearly rationally equivalent. ■

The theta series of Λ'' is

$$\frac{1}{2}\{\Theta_\Lambda(z) + \Theta_\Lambda(z+1) + \Theta_{S_\emptyset(\Lambda)}(z) + \Theta_{S_\emptyset(\Lambda)}(z+1)\} .$$

In particular, if Λ is a 16-dimensional 2-modular lattice of minimal norm 3, Λ'' has minimal norm 4 and so (by [38]) must be the Barnes-Wall lattice. This forces the construction for the odd Barnes-Wall lattice given in Section 2.

5. Theta series of strongly modular lattices

Throughout this section we assume that Λ is a strongly N-modular lattice for N in (3). As remarked in Section 3, if Λ is even then $\Theta_\Lambda(z)$ is invariant under $\Gamma_0(N)^+$ with respect to a certain character depending only on the rational equivalence class of Λ. In all cases $\Theta_\Lambda(z)$ is invariant under $\frac{1}{2}\Gamma_0(4N)^+$, again with respect to some character. In order to prove Theorems 1 and 2 it is necessary to study the space of modular forms for $\frac{1}{2}\Gamma_0(4N)^+$.

Let $\chi^{(N)}$ be the character of $\frac{1}{2}\Gamma_0(4N)^+$ with respect to which $\Theta_{C^{(N)}}(z)$ is invariant, and let $w^{(N)}$ be the weight of $\Theta_{C^{(N)}}(z)$. Then a lattice satisfying the hypotheses of Theorem 2 has theta series in the space

$$\mathcal{M}_{kw^{(N)}}\left(\frac{1}{2}\Gamma_0(4N)^+, (\chi^{(N)})^k\right) .$$

Of course $\Theta_{C^{(N)}}(z)^k$ is in this space.

In the sequel, we define the divisor of a modular form $f(z)$ in $\mathcal{M}_k(\Gamma,\chi)$ to be

$$\frac{1}{n}\mathrm{div}(f(z)^n),$$

where $\chi^n = 1$, and the divisor of a form with trivial character is defined as in [30, p. 51].

Lemma 3. *For any square-free N, the divisor of $\Theta_{C^{(N)}}(z)$ with respect to $\frac{1}{2}\Gamma_0(4N)^+$ is*

$$\frac{1}{8}\sum_{d|N} d\cdot\mathbf{1}, \quad \textit{if } N \textit{ odd}\ , \quad \frac{1}{6}\sum_{d|N} d\cdot\mathbf{1}, \quad \textit{if } N \textit{ even}\ .$$

Proof. The modular form

$$\eta(z) = q^{1/12}\prod_{m=1}^{\infty}(1-q^{2m}), \quad q = e^{\pi i z},$$

is zero only at $\mathbb{Q}\ \cup\ \{\infty\}$. It follows that any product or quotient of functions $\eta(az+b)$ for rational a and b has no zeros or poles outside $\mathbb{Q}\ \cup\ \{\infty\}$. In particular, since $\Theta_{\mathbb{Z}}(z) = \theta_3(z) = \eta(z)^5/(\eta(z/2)\eta(2z))^2$, the same is true for $\Theta_{C^{(N)}}(z)$ ($\theta_2(z)$, $\theta_3(z)$, and $\theta_4(z)$ are the familiar Jacobi theta series). Since $C^{(N)}$ is a lattice, $\Theta_{C^{(N)}}(z)$ does not have a zero at ∞. Consequently,

$$\mathrm{div}(\Theta_{C^{(N)}}(z)) = \deg(\Theta_{C^{(N)}}(z))\cdot\mathbf{1}\ .$$

We may compute the right-hand side using the following result, which can be deduced from the proof of Theorem 2.4.3 of [30]. Let f be a modular form of weight k for a Fuchsian group Γ commensurate with $SL_2(\mathbb{Z})$. Then

$$\deg(f) = \frac{k}{12}\cdot\frac{[SL_2(\mathbb{Z}) : \Gamma\cap SL_2(\mathbb{Z})]}{[\Gamma : \Gamma\cap SL_2(\mathbb{Z})]}\ .$$

This determines $\deg(\Theta_{C^{(N)}}(z))$. ■

From now on let N be a fixed number from (3). Define

$$g_1(z) = \Theta_{C^{(N)}}(z) ,$$

and let $g_2(z)$ be a modular function for $\frac{1}{2}\Gamma_0(4N)^+$ with divisor $\infty - \mathbf{1}$ (which exists since $\frac{1}{2}\Gamma_0(4N)^+$ has genus 0). To be precise, let

$$\eta^{(N)}(z) = \prod_{d|N} \eta(dz) .$$

Then (cf. [11, Table 3]) if N is odd we take

$$g_2(z) = \left\{ \frac{\eta^{(N)}\left(\frac{z}{2}\right) \eta^{(N)}(2z)}{\eta^{(N)}(z)^2} \right\}^{D_N / \dim C^{(N)}} ,$$

and if N is even we take

$$g_2(z) = \left\{ \frac{\eta^{(N/2)}\left(\frac{z}{2}\right) \eta^{(N/2)}(4z)}{\eta^{(N/2)}(z)\eta^{(N/2)}(2z)} \right\}^{D_N / \dim C^{(N)}} .$$

Theorem 9. *Any element $f(z)$ of*

$$\mathcal{M}_{kw^{(N)}}\left(\frac{1}{2}\Gamma_0(4N)^+, (\chi^{(N)})^k\right)$$

can be written uniquely as

$$f(z) = g_1(z)^k \sum_{i=0}^{\lfloor k \ \mathrm{ord}_1(g_1) \rfloor} c_i g_2(z)^i . \tag{17}$$

For a cusp form, $c_0 = 0$, and if $k \ \mathrm{ord}_1(g_1)$ is an integer then that coefficient must also be zero.

Proof. $f(z)/g_1(z)^k$ is a modular function for $\frac{1}{2}\Gamma_0(4N)^+$ with the trivial character, and therefore can be written as a rational function in $g_2(z)$. But, since $f(z)$ has no poles, the only pole of $f(z)/g_1(z)^k$ is at the cusp class 1, which is also the pole of $g_2(z)$. It follows that $f(z)/g_1(z)^k$ is a polynomial in $g_2(z)$. The remaining statements follow by considering the order of $f(z)$ at the two cusp classes. ■

There is an expression similar to (17) for the theta series of the $\emptyset$-shadow. Let $s = D_N/\dim C^{(N)}$, and set

$$\begin{aligned} s_1(z) &= \left(\frac{n}{\sqrt{\sqrt{N}z}}\right)^{\dim C^{(N)}} g_1\left(1 - \frac{1}{Nz}\right) = \prod_{d|N} \theta_2(dz) = 2^{d(N)} \frac{\eta^{(N)}(2z)^2}{\eta^{(N)}(z)} , \\ s_2(z) &= g_2\left(1 - \frac{1}{Nz}\right) = -2^{-D_N/2} \left\{ \frac{\eta^{(N)}(z)}{\eta^{(N)}(2z)} \right\}^s . \end{aligned}$$

Corollary 3. *If Λ is a strongly N-modular lattice that is rationally equivalent to $(C^{(N)})^k$ then its theta series can be written in the form (17), and its $\emptyset$-shadow S has theta series*

$$\Theta_S(z) \;=\; s_1(z)^k \sum_i c_i s_2(z)^i \;. \tag{18}$$

Proof. This follows from Corollary 2, Theorem 9 and Equation (16). ∎

The proofs of Theorems 1 and 2 use only the nonnegativity of the coefficients of certain theta series. In some cases stronger bounds may be obtained by using the facts that the coefficients must also be integers, or, more precisely, that Θ_Λ and Θ_S must have nonnegative integer coefficients and satisfy $\Theta_\Lambda \equiv 1 \pmod 2$ and $\Theta_S \equiv 0$ or $1 \pmod 2$; and if Λ is odd with minimal norm μ then

$$\#\{v \in S_\emptyset(\Lambda) : \; v \cdot v < \mu/4\} = 0 \;,$$
$$\#\{v \in S_\emptyset(\Lambda) : \; v \cdot v < \mu/2\} \le 2 \;.$$

For example, let us prove that there is no 14-dimensional 3-modular lattice meeting the bound of Theorem 2 (and satisfying the hypothesis of that theorem). For such a lattice, Corollary 3 would imply that

$$\begin{aligned} \Theta_\Lambda &= g_1^7(c_0 + c_1 g_2 + c_2 g_2^2 + c_3 g_2^3) \\ &= 1 + O(q^4) \;, \\ \Theta_S &= s_1^7(c_0 + c_1 s_2 + c_2 s_2^2 + c_2 s_2^3) \;. \end{aligned}$$

From the first equation we find that $c_0 = 1$, $c_1 = -14$, $c_2 = 28$, $c_3 = -56$, so $\Theta_\Lambda = 1 + 602q^4 + 1344q^5 + 4032q^6 + \cdots$, and then $\Theta_S = \frac{7}{2}q + \frac{147}{2}q^3 + \cdots$, which is impossible.

The nonexistence results for $N = 2$ and 3 mentioned at the beginning of Section 2 (and further results given in the table in [48]) were obtained in this way.

6. The proofs of Theorems 1 and 2

We begin by stating a series of identities that relate g_1, g_2, s_1 and s_2. (We include more than are needed, because of their intrinsic interest.) For N odd, we have

$$g_2(z)^2 g_1(z)^s = \eta^{(N)}(z)^s \;, \tag{19}$$

$$g_2(z) g_1(z)^s = -\eta^{(N)}\left(\frac{z+1}{2}\right)^s \;, \tag{20}$$

$$s_2(z)^2 s_1(z)^s = \eta^{(N)}(z)^s \ , \tag{21}$$

$$s_2(z) s_1(z)^s = -2^{D_N/2} \ \eta^{(N)}(2z)^s \ , \tag{22}$$

$$g_2(z) g_2(z+1) s_2(z) = 2^{-D_N/2} \ , \tag{23}$$

$$\frac{1}{g_2(z)} + \frac{1}{g_2(z+1)} + \frac{1}{s_2(z)} = 2s \ , \tag{24}$$

$$g_1(z) g_1(z+1) s_1(z) = 2^{\dim C^{(N)}} \eta^{(N)}(z)^3 \ , \tag{25}$$

$$g_1(z)^{s/2} - g_1(z+1)^{s/2} - s_1(z)^{s/2} = 2s\eta^{(N)}(z)^{s/2} \ . \tag{26}$$

For $N = 2$, s_1 and s_2 are given by

$$\begin{aligned} s_1(z) &= \frac{2\eta(z)^5 \eta(4z)^2}{\eta\left(\frac{z}{2}\right)^2 \eta(2z)^3} \ , \\ s_2(z) &= -\frac{1}{16} \frac{\eta\left(\frac{z}{2}\right)^8 \eta(2z)^{16}}{\eta(z)^{16} \eta(4z)^8} \ . \end{aligned}$$

Then we have

$$g_1(z)^8 g_2(z)^2 = \eta(z)^8 \eta(2z)^8 \ , \tag{27}$$

$$s_1(z)^4 s_2(z)^2 = \frac{1}{16} \theta_4(z)^4 \theta_3(2z)^4 \ , \tag{28}$$

$$s_1(z)^8 s_2(z)^2 = \eta(z)^8 \eta(2z)^8 \ , \tag{29}$$

$$g_2(z) s_2(z+1) = g_2(z+1) s_2(z) = \frac{1}{16} \ , \tag{30}$$

$$g_2(z) g_2(z+1) s_2(z) s_2(z+1) = \frac{1}{256} \ , \tag{31}$$

$$\frac{1}{g_2(z)} + \frac{1}{g_2(z+1)} + \frac{1}{s_2(z)} + \frac{1}{s_2(z+1)} = 16 \ . \tag{32}$$

To show (23), for example, we observe that $f(z) = g_2(z) g_2(z+1) s_2(z)$ is invariant under $\Gamma_0(N)^+$, which is transitive on cusps, and so the order of $f(z)$ at every cusp is the same. On the other hand every pole and zero of $f(z)$ is at a cusp, and since $f(z)$ is a modular function the number of zeros must equal the number of poles. Therefore $f(z)$ has no zeros or poles, and must be constant. We leave the proofs of the other identities to the reader.

Proof of Theorem 1. Let Λ be a unimodular lattice of minimal norm μ in dimension $n = 8t + o = 24m - l$, where $0 \le o \le 7$, $1 \le l \le 24$. We must show that $\mu \le 2m$ except when $m = l = 1$. From Corollary 3,

$$\Theta_\Lambda = g_1^n \sum_{i=0}^{t} c_i g_2^i = \sum_{j=0}^{\infty} a_j q^j, \quad \text{(say)} \ , \tag{33}$$

and the theta series of the $\emptyset$-shadow of Λ is

$$\Theta_S = s_1^n \sum_{i=0}^{t} c_i s_2^i = q^{\frac{o}{4}} \sum_{j=0}^{\infty} b_j q^{2j}, \quad \text{(say)} . \tag{34}$$

Suppose, seeking a contradiction, that $\mu \geq 2m+1$. Then $\Theta_\Lambda = 1+O(q^{2m+1})$. This determines c_i for $0 \leq i \leq 2m$. In particular, as we show below, $c_{2m} \leq 0$, with equality only when $n = 23$. On the other hand, we will also write c_{2m} as a linear combination of b_j for $0 \leq j \leq t-2m$ with nonnegative coefficients, and thus $c_{2m} \geq 0$, which is a contradiction unless $n = 23$.

To compute c_{2m} we divide both sides of (33) by g_1^n to obtain

$$g_1^{-n} + O(q^{2m+1}) = \sum_{i=0}^{\infty} c_i g_2^i ,$$

where we adopt the convention that $c_i = 0$ for $i > t$. From the Bürmann-Lagrange theorem [49] we deduce

$$c_i = -\frac{n}{i} \text{ coefft. of } q^i \text{ in } q\ g_1'\ g_1^{-n-1} \left(\frac{q}{g_2}\right)^i ,$$

for $0 \leq i \leq 2m$. For $i = 2m$ this simplifies to

$$-\frac{24m-l}{2m} \text{ coefft. of } q^{2m} \text{ in } q\ g_1'\ g_1^{l-1}\ q^{2m}\ \eta^{-24m} ,$$

using (19). Now $g_1' g_1^{l-1}$ (the derivative of a theta series) has nonnegative coefficients, and $q^{2m}\eta^{-24m}$ has nonnegative coefficients and positive coefficients at even powers of q. So as long as $qg_1'g_1^{l-1}$ has a nonzero coefficient of even degree $\leq 2m$, it follows that $c_{2m} < 0$. Since g_1 has a linear term and g_1' has a cubic term, the only way c_{2m} can equal zero is if $m = l = 1$, i.e. if $n = 23$.

On the other hand, from (34) we have

$$\sum_{i=0}^{t} c_{t-i} s_2^{-i} = s_1^{-n} s_2^{-t} q^{o/4} \sum_{j=0}^{\infty} b_j q^{2j}$$

and thus

$$c_i = \sum_{j=0}^{t-j} \beta_{i,j} b_j$$

where

$$s_1^{-n} s_2^{-t} q^{o/4+2j} = \sum_{i=0}^{\infty} \beta_{t-i,j} s_2^{-i} .$$

Again using Bürmann-Lagrange we find

$$\beta_{i,j} = -\text{ coefft. of } q^{2t-2i-2j} \text{ in } 2\ \frac{qs_2'}{s_2}\ q^{2t-2i+o/4}\ s_2^{-i}\ s_1^{-n} . \tag{35}$$

From the product expansion for s_2 we immediately deduce that all coefficients of qs_2'/s_2 are nonpositive. From (22) (with $s = 24$) and the fact that s_1 has nonnegative coefficients, the remaining factor in (35) has nonnegative coefficients as long as $24i \geq n$. In particular, this is certainly true for $i = 2m$, and thus $\beta_{2m,j} \geq 0$, which produces the desired contradiction. ∎

Proof of Theorem 2. Theorem 1 covers the case $N = 1$, and the other cases when N is odd are analogous. The proof for $N = 2$ is given below, the remaining cases 6 and 14 again being analogous. We begin with a lemma.

Lemma 4. *If $N = 2$ then (i) all coefficients of $s_1^{-2a}s_2^{-2b}$ are nonnegative whenever $2b \leq a \leq 4b$, and (ii) all coefficients of the logarithmic derivative of $q^c s_1^{-2a} s_2^{-2b}$ are nonnegative whenever $2b \leq a \leq \min\{2b + c, 4b\}$.*

Proof. We write

$$q^c s_1^{-2a} s_2^{-2b} = q^{2b+c-a}(q^2 s_1^{-8} s_2^{-2})^{a/2-b}(s_1^{-4}s_2^{-2})^{2b-a/2} ,$$

in which the exponents $2b - a/2$, $a/2 - b$ and $2b + c - a$ are positive by hypothesis, and consider each factor separately. First, q and its logarithmic derivative (q^{-1}) are both nonnegative. The other two terms may be expanded as

$$\frac{q^2}{s_1^8 s_2^2} = \frac{q^2}{(\eta^{(2)})^8} = \prod_{m=1}^{\infty}(1-q^m)^{-8}(1-q^{2m})^{-8} \tag{36}$$

and, using (28),

$$s_1^{-4}s_2^{-2} = 16\prod_{m=1}^{\infty}\{(1+q^{2m-1})(1-q^{2m-1})^{-2}\}^4(1-q^{4m})^{-8}(1-q^{8m-4})^{-8} . \tag{37}$$

Each factor of (36) and (37) has nonnegative coefficients and nonnegative logarithmic derivative. ∎

Proof of Theorem 2 for $N = 2$. Let Λ be a 2-modular lattice of minimal norm μ in dimension $n = 4t + o = 16m - 2l$, where $o = 0$ or 2, $1 \leq l \leq 8$. Then

$$\begin{aligned}\Theta_\Lambda &= g_1^{n/2}\sum_{i=0}^{t} c_i g_2^i = \sum_{j=0}^{\infty} a_j q^j ,\\ \Theta_S &= s_1^{n/2}\sum_{i=0}^{t} c_i s_2^i = q^{o/2}\sum_{j=0}^{\infty} b_j q^j ,\end{aligned}$$

say. That $c_{2m} \leq 0$ follows as in the proof of Theorem 1, but since g'_1 now has a linear term there is no exception and $c_{2m} < 0$.

On the other hand, defining $\beta_{i,j}$ as before, we find

$$\beta_{2m,j} = \frac{1}{2m} \text{ coefft. } q^{t-2m-j} \text{ in } \mathcal{L}\{q^{j+o/2} s_1^{-n/2} s_2^{-t}\} q^{n/4-2m} s_1^{-n/2} s_2^{-2m} ,$$

where $\mathcal{L}$ denotes the logarithmic derivative. By the lemma, the first factor has nonnegative coefficients when $0 \leq o/2 \leq t$, and the second factor has nonnegative coefficients when $8m \leq n \leq 16m$. This proves the desired result for $n \geq 8$. The remaining three cases, $n = 2, 4$ and 6, can be checked directly. ∎

We end this section with an analogue of Theorem 1 for codes over $\mathbb{Z}/4\mathbb{Z}$. This is a generalization of a bound established by Bonnecaze et al. [5] for self-dual codes over $\mathbb{Z}/4\mathbb{Z}$ in which all Euclidean norms are divisible by 8.

Theorem 10. *Suppose C is a self-dual code over $\mathbb{Z}/4\mathbb{Z}$ of length n. The minimal Euclidean norm of C is at most*

$$8 \left[\frac{n}{24} \right] + 8 ,$$

unless $n \equiv 23 \pmod{24}$ when the bound must be increased by 4.

Proof. As in [5] we construct a unimodular lattice Λ from C using "Construction A". Λ has theta series

$$\theta_3(4z)^n + O(q^{\mu/4}) ,$$

where μ is the minimal Euclidean norm of C. The argument used to prove Theorem 1 now establishes the desired result. The identity

$$q\ (\theta_3(4z)\ \theta'_3(z) \ - \ \theta'_3(4z)\ \theta_3(z)) \ = \ \eta(2z)^6$$

is needed. ∎

7. Genera not covered by Theorem 2

We can say less about the minimal norm μ of a strongly N-modular lattice Λ not rationally equivalent to a direct sum of copies of $C^{(N)}$. If $N = 1$ or 2, local considerations show that no such lattices exist, nor can they exist for $N = 7$ or 23, although then a more involved argument appears to be needed (see the Appendix).

For $N = 3, 5, 6$ and 11, the numerical evidence suggests that

$$\mu \le 2 \left[\frac{n - \dim C^{(N)}}{D_N} \right] + 2 \ . \tag{38}$$

For $N = 3$ and 11 we further conjecture that if equality holds and $n \equiv 2 \pmod{D_N}$ then Λ must be even. These conjectures have been verified for $n \le 56$ for $N = 3, 5, 6$ and for $n \le 32$ for $N = 11$.

For $N \le 14$ we conjecture that

$$\mu \le 2 \left[\frac{n}{4} \right] + 2, \quad n \neq 2 \ ;$$

this has been verified for $n \le 30$. For $N = 15$ there is no obvious pattern. In the critical dimension 4, for example, the lattice defined below in (39) has minimal norm 4, which actually coincides with the bound of Theorem 2.

Acknowledgement. The computer language Magma [6], [7], [8] has been helpful in studying particular lattices, testing for modularity, etc.

Appendix

For $N = 7$ and 23, every N-modular lattice must satisfy the hypotheses of Theorem 2. This a consequence of the following result.

Theorem 11. *If N is a positive integer congruent to 7 mod 8, then any even $\{N\}$-modular lattice of even-level $4N$ has oddity 0.*

We begin with two lemmas. When we say that a power series reduces to 1 mod 2, this includes the assertion that the coefficients are algebraic integers, and the corresponding number field is unramified at 2.

Lemma 5. *Let Λ be an even lattice of even-level $2^k N$, with N odd. Then for any element t of $\Gamma_0(2^k)$, there exists a constant C such that $C\Theta_\Lambda|_t$ reduces to 1 mod 2.*

Proof. The analysis of [21] can be extended to show that there exists a function $T(v)$ on Λ^* such that

$$\Theta_\Lambda|_t = \sum_{v \in \Lambda^*} T(v) q^{v \cdot v}.$$

Moreover $T(v) = T(-v)$ and $T(v)/T(0)$ is either 0 or a root of unity of odd order. Taking $C = T(0)^{-1}$, the result follows immediately. ∎

Lemma 6. *Let g be a modular function for $\Gamma(2)$. If all poles of g occur at the cusp 1, and the expansion of g at ∞ reduces to 1 mod 2, then all zeros of g occur at points z such that $16\lambda(z)^{-1}$ is an algebraic integer with even norm, where $\lambda(z) = (\theta_2(z)/\theta_3(z))^4$.*

Proof. Let $\ell(z)$ be the function $\lambda(z)/16$. Then $\ell(z)$ has integer coefficients, with leading coefficient equal to 1. Since the unique pole of ℓ is at 1, g can be expressed as a polynomial p in ℓ, with algebraic integer coefficients. Clearly, then, g reduces to 1 mod 2 just when p reduces to 1 mod 2. But this implies that all roots of p have 2-adic valuation greater than 1, which is the desired result. ∎

Proof of Theorem 11. Let Λ be an n-dimensional even $\{N\}$-modular lattice of even-level $4N$, with theta series $\Theta_\Lambda(z)$, and let K be the $\{4, N\}$-modular lattice $\sqrt{2}\mathbb{Z} \times \sqrt{2N}\mathbb{Z}$, with theta series $\Theta_K(z) = \theta_3(2z)\theta_3(2Nz)$. Then $f(z) = \Theta_\Lambda(z)/\Theta_K(z)^{n/2}$ is a modular function for

$\Gamma_0(4N)$ (with trivial character, since $\dim \Lambda$ is even and thus $\det_2 \Lambda$ is a square). Furthermore, since $\theta_3(2z)\theta_3(2Nz)$ has zeros only at cusps, it follows that f has poles only at cusps.

If Λ had oddity 4 (the only other possibility), then f would satisfy the relation

$$f|_{W_N} = -f,$$

since both Λ and $K^{n/2}$ are $\{N\}$-modular, and K has oddity 0. As a consequence, f has at least one zero at every point of $\Gamma_0(4N)$ fixed by W_N. Also, since f is the ratio of two theta series, its expansion around ∞ has integer coefficients, and reduces to 1 mod 2.

Let T be a set of (right) representatives for $\Gamma_0(4)/\Gamma_0(4N)$. Then

$$g = \prod_{t \in T} f|_t$$

is a modular function for $\Gamma_0(4)$ (g can also be thought of as the norm of f from $\Gamma_0(4N)$ to $\Gamma_0(4)$). Moreover, up to a constant factor, the expansion of g around ∞ reduces to 1 mod 2, since by Lemma 5 the same is true for each $f|_t$.

Since $g(z)$ is invariant under $\Gamma_0(4)$, $g(z/2)$ is invariant under $\frac{1}{2}\Gamma_0(4) = \Gamma(2)$. Moreover, since the poles of $g(z)$ are at the cusps, and neither ∞ nor 0 are poles of $g(z)$, it follows that the only pole (which may, of course, be a multiple pole) of $g(z)$ is at the cusp 1.

To finish the proof, we invoke Lemma 6. We obtain a contradiction if we can demonstrate the existence of some point z of $\Gamma_0(4N)$ fixed by W_N such that $16\lambda(z/2)$ has odd norm. Let x be the point $(1+\sqrt{-N})/4$ of $\Gamma_0(N)$. If x' is any image of x in $\Gamma_0(N) \cap \Gamma(2)$, then $2x'$ is a point of $\Gamma_0(4N)$ fixed by W_N. Now $j(x)$ has odd norm. (The elliptic curve corresponding to x has complex multiplication by an order of $\mathbb{Q}(\sqrt{-N})$ of odd conductor. A CM curve always has integral j-invariant, so has good reduction over a suitable extension of $\mathbb{Q}$. The reduction mod 2 cannot be supersingular, so the j-invariant cannot reduce to 0.) We have

$$j = \frac{(\ell^2 - 16\ell + 256)^3}{\ell^2(\ell - 16)^2} \equiv \ell^2 \pmod 2,$$

so for two of the six images, ℓ must have odd norm. ∎

Remarks. (1) The assumption that N is congruent to 7 mod 8 is critical; for N congruent to 1 mod 4, there are no points fixed by W_N other than cusps, while for N congruent to 3 mod 8, the points fixed by W_N correspond to curves with supersingular reduction mod 2. (2) The hypothesis that the even-level be $4N$ can be relaxed to say that the even-level is $4MN$, where M is an odd integer, relatively prime to N, such that $-N$ has a square root mod M and $\det_{\Pi(M)}\Lambda$ is a square; in that case, the conclusion is that $\gamma_{\Pi(4M)}(\Lambda) = 1$. The existence of a square root of $-N$ is necessary to allow the existence of suitable CM curves.

Corollary 4. *If N is an integer congruent to 7 mod 8, then any N-modular lattice has oddity 0, as does any $\{2, N\}$-modular lattice of dimension a multiple of 4.*

Proof. If Λ is an N-modular lattice, then $\sqrt{2}\Lambda$ is $\{4, N\}$-modular, and has the same oddity (since $\det\Lambda$ is 1 or 7 mod 8). Therefore $\sqrt{2}\Lambda$ satisfies the hypotheses of Theorem 11, and must have oddity 0.

Similarly, a $\{2, N\}$-modular even lattice has oddity 0. If Λ is a $\{2, N\}$-modular odd lattice, then the even neighbor of Λ (recall Theorem 8) is a $\{2, N\}$-modular even lattice with the same oddity. ∎

The following is immediate:

Corollary 5. *All p-modular lattices, for p prime and congruent to 7 mod 8, are rationally equivalent to the direct sum of some number of copies of $C^{(p)}$. A strongly 14-modular lattice must be rationally equivalent to the direct sum of some number of copies of $\begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix}$. A strongly 15-modular lattice is rationally equivalent to the direct sum of some number of copies of $C^{(15)}$, possibly together with a copy of*

$$\begin{pmatrix} 4 & 0 & 2 & 1 \\ 0 & 4 & 1 & 2 \\ 2 & 1 & 5 & 1 \\ 1 & 2 & 1 & 5 \end{pmatrix}. \tag{39}$$

References

[1] A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160.

[2] C. Bachoc, Applications of coding theory to the construction of modular lattices, *J. Combin. Theory* **A 78** (1997), 92–119.

[3] F. van der Blij, An invariant of quadratic forms mod 8, *Indag. Math.* **21** (1959), 291–293.

[4] H. Braun, Geschlecter quadratischer Formen, *J. reine angewandte Math.* **182** (1940), 32–49.

[5] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Information Theory* **43** (1997), 969–976.

[6] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Sydney, 1995.

[7] W. Bosma, J. Cannon, and G. Mathews, Programming with algebraic structures: Design of the Magma language, in *Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation*, M. Giesbrecht, Ed., Association for Computing Machinery, 1994, 52–57.

[8] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.* **24** (1997), 235–265.

[9] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Information Theory* **44** (1998), to appear.

[10] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, NY, 1996.

[11] J. H. Conway and S. P. Norton, Monstrous moonshine, *Bull. London Math. Soc.* **11** (1979), 308–339.

[12] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices II: subgroups of $GL(n,\mathbb{Z})$, Proc. Royal Soc. London, **A 419** (1988), 29–68.

[13] J. H. Conway and N. J. A. Sloane, A new upper bound for the minimum of an integral lattice of determinant one, *Bull. Amer. Math. Soc.* **23** (1990), 383–387. Erratum: **24** (1991), 479.

[14] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Information Theory* **36**, (1990), 1319–1333.

[15] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 2nd edition, 1993.

[16] J. H. Conway and N. J. A. Sloane, On lattices equivalent to their duals, *J. Number Theory* **48** (1994), 373–382.

[17] J. H. Conway and N. J. A. Sloane, A note on optimal unimodular lattices, *J. Number Theory*, to appear.

[18] K. Harada and M. L. Lang, Some elliptic curves arising from the Leech lattice, *J. Alg.* **125** (1989), 298–310.

[19] K. Harada and M. L. Lang, On some sublattices of the Leech lattice, *Hokkaido Math. J.* **19** (1990), 435–446.

[20] G. Höhn, Self-dual codes over the Kleinian four group, preprint, August 1996.

[21] Y. Kitaoka, A remark on the transformation formula of theta functions associated to positive definite quadratic forms, *J. Number Theory* **12** (1980), 224–229.

[22] M. Koike, Mathieu group M_{24} and modular forms, *Nagoya Math. J.* **99** (1985), 147–157.

[23] T. Kondo and T. Tasaka, The theta functions of sublattices of the Leech lattice, *Nagoya Math. J.* **101** (1986), 151–179.

[24] T. Kondo and T. Tasaka, The theta functions of sublattices of the Leech lattice II, *J. Fac. Sci. Univ. Tokyo, Sec* **IA**, **34** (1987), 545–572.

[25] I. Krasikov and S. Litsyn, Linear programming bounds for doubly-even self-dual codes, *IEEE Trans. Information Theory* **43** (1997), 1238–1244.

[26] C. L. Mallows, A. M. Odlyzko and N. J. A. Sloane, Upper bounds for modular forms, lattices and codes, *J. Algebra* **36** (1975), 68–76.

[27] C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, *Information and Control* **22** (1973), 188–200.

[28] J. Martinet, *Les Réseaux Parfaits des Espaces Euclidiens*, Masson, Paris, 1996.

[29] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer-Verlag, NY, 1973.

[30] T. Miyake, *Modular Forms*, Springer-Verlag, NY, 1989.

[31] G. Nebe, Finite subgroups of $GL_{24}(\mathbb{Q})$, *Experimental Math.* **5** (1996), 163–195.

[32] G. Nebe, Finite subgroups of $GL_n(\mathbb{Q})$ for $25 \le n \le 31$, *Commun. Algeb.* **24** (1996), 2341–2397.

[33] G. Nebe, The normaliser action and strongly modular lattices, *L'Enseign. Math.* **43** (1997), 67–76.

[34] G. Nebe and W. Plesken, *Finite Rational Matrix Groups*, Memoirs Amer. Math. Soc., Vol. **116** (No. 556), 1995.

[35] G. Nebe and B. B. Venkov, *Non-existence of extremal lattices in certain genera of modular lattices*, *J. Number Theory*, **60** (1996), 310–317.

[36] W. Plesken and M. Pohst, On maximal finite irreducible subgroups of $GL(n, \mathbb{Z})$: IV, remarks on even dimensions with applications to $n = 8$, *Math. Comp.* **34** (1980), 259–275.

[37] H.-G. Quebbemann, Lattices with theta-functions for $G(\sqrt{2})$ and linear codes, *J. Alg.* **105** (1987), 443–450.

[38] H.-G. Quebbemann, Modular lattices in Euclidean spaces, *J. Numb. Theory* **54** (1995), 190–202.

[39] H.-G. Quebbemann, Atkin-Lehner eigenforms and strongly modular lattices, *L'Enseign. Math.*, **43** (1997), 55–65.

[40] H.-G. Quebbemann, A shadow identity and an application to isoduality, preprint, 1998.

[41] E. M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Information Theory* **44** (1998), 134–139.

[42] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, ed. V. Pless et al., Elsevier, Amsterdam, 1998, to appear.

[43] R. Scharlau and B. Hemkemeier, *Classification of integral lattices with large class number*, preprint 94–102, Univ. Bielefeld, 1994.

[44] R. Scharlau and B. B. Venkov, The genus of the Barnes-Wall lattice, *Comm. Math. Helv.* **69** (1994), 322–333.

[45] R. Scharlau and B. B. Venkov, The genus of the Coxeter-Todd lattice, preprint, 1995.

[46] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag, New York, 1985.

[47] J.-P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France, Paris, 1970; English translation, Springer-Verlag, NY, 1973.

[48] N. J. A. Sloane and G. Nebe, *Catalogue of Lattices*, published electronically at http://www.research.att.com/∼njas/lattices/.

[49] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge Univ. Press, 4th ed., 1963.