SOME CONGRUENCES FOR SIEGEL THETA SERIES

RAINER SCHULZE-PILLOT

Abstract. We discuss an arithmetic approach to some congruence properties of Siegel theta series of even positive definite unimodular quadratic forms.

1. Introduction.

There has recently been some interest in congruence properties of Siegel modular forms. In particular, following Böcherer and Nagaoka [2], Siegel modular forms $f$ have been considered for which $\Theta(f) \equiv 0 \mod p$ for some prime $p$, where for $f(Z) = \sum a(f,T) \exp(2\pi i \text{tr}(TZ))$ one puts $\Theta(f)(Z) = \sum \det(T)a(f,T) \exp(2\pi i \text{tr}(TZ))$.

In this note we show that unimodular lattices with an automorphism of order $p$ give a quite natural series of examples for this behaviour. In particular, we recover the recent result of Nagaoka and Takemori from [6] for the theta series of the Leech lattice. I thank S. Böcherer for telling me about the problem and S. Nagaoka and S. Takemori for showing me their preprint [6].

2. Fixed space decomposition of lattices with an automorphism of prime order

In this section we recall and modify some results from [5, 8].

Let $V$ be an $m$-dimensional $\mathbb{Q}$-vector space with positive definite quadratic form $q$, let $M$ be an integral lattice (with respect to $q$) on $M$ having an automorphism $\sigma \in O(M,q)$ of order $p$, where $p \neq 2$ is a prime.

We denote by $\Pi = \langle \sigma \rangle$ the cyclic group generated by $\sigma$ and consider $M$ as a module over the group ring $\Lambda = \mathbb{Z}[\Pi]$.

We consider the $\mathbb{Z}$-linear embedding

$$\iota : \Lambda \rightarrow \Gamma = \mathbb{Z} \oplus \mathbb{Z}[\zeta_p]$$

given by $\iota(\sigma^i) = (1, \zeta_p^i)$; it is clearly an embedding of rings, which extends to an isomorphism

$$\iota : \mathbb{Q}[\Pi] \rightarrow \mathbb{Q}\Gamma = \mathbb{Q} \oplus \mathbb{Q}(\zeta_p);$$
Lemma 2.1. The lattice $M$ of $V$ again identifying $V$ on $M$. We denote by $\Lambda$ and $\iota$ that $\Lambda$ and $\iota$ in the sequel.

We have $\sum_{j=0}^{p-1} \sigma|_{V_i} = 0$, i.e., the $\mathbb{Q}[\Pi]$-module $V_1$ can be viewed via $\mathbb{Q}(\zeta_\rho) \cong \mathbb{Q}[X]/(X^{p-1} + \cdots + 1)$ as a $\mathbb{Q}(\zeta_\rho)$-vector space, and $(a, b) = (a, \sum_{i=1}^{p-1} \beta_i \zeta^i) \in \mathbb{Q}\Gamma = \mathbb{Q}\Lambda = \mathbb{Q}[\Pi]$ acts on $V_0$ by multiplication with $a$, on $V_1$ by multiplication with $b$, and split $\mathbb{Q}(\zeta_\rho)$ onto $\mathbb{Q}[\Pi]$ via $\iota$.

Lemma 2.2. With notations as above and $M_i = M \cap V_i$ one has $p\tilde{M}_i \subseteq M_i \subseteq \tilde{M}_i \subseteq M_i^\#$ for $i = 1, 2$.

Proof. $p\Gamma \subseteq \Lambda$ implies $p\tilde{M}_i \subseteq p\Gamma M \subseteq \Lambda M = M$ for $i = 1, 2$, so $p\tilde{M}_i \subseteq M \cap V_i = M_i$. $M_i \subseteq M = \Lambda M \subseteq \Gamma M$ implies $M_i \subseteq \tilde{M}_i$. The inclusion $\tilde{M}_i \subseteq M_i^\#$ is obvious.

Lemma 2.3. With notation as above one has $M = M_0 \perp M_1$ or $M_0$ has determinant divisible by $p$. 

we have then

$$\iota\left(\sum_{i=1}^{p-1} \alpha_i \sigma^i\right) = (a, \sum_{i=1}^{p-1} \beta_i \zeta^i)$$

with

$$p\alpha_0 = a + \text{Tr}_{\mathbb{Q}(\zeta_\rho)}(\sum_{i=1}^{p-1} \beta_i \zeta^i)$$

and $\alpha_i = \beta_i + \alpha_0$ for $1 \leq i \leq p - 1$.

In particular we have $I := p\mathbb{Z} \oplus (1 - \zeta)\mathbb{Z}[\zeta_\rho] \subseteq \iota(\Lambda)$. We will identify $\Lambda$ and $\iota(\Lambda)$ in the sequel.

We denote by $V_0$ the fixed space of $\sigma$ in $V$ and split $V = V_0 \perp V_1$, so that

$$\sum_{j=0}^{p-1} \sigma|_{V_i} = 0,$$

Lemma 2.1. The lattice $\Gamma M \subseteq V$ splits as $\Gamma M = \tilde{M}_0 \oplus \tilde{M}_1$, where $\tilde{M}_i = \pi_i(M)$ is the orthogonal projection of $M$ onto $V_i$ ($i = 1, 2$).

Proof. The splitting $\Gamma = \mathbb{Z} \oplus \mathbb{Z}[\zeta_\rho]$ induces corresponding splittings of $V$ and $\Gamma M$. In view of the remarks above on the action of $\mathbb{Q}\Gamma$ on $V_0$ and $V_1$ we see that the splitting of $V$ is indeed the splitting $V = V_0 \perp V_1$, we write $\Gamma M = \tilde{M}_0 \oplus \tilde{M}_1$. For $m_0 \in \tilde{M}_0$ we can write $m_0 = (1, 0) \cdot m$ with $m \in M$, then $m_1 = (0, 1)m \in \tilde{M}_1$ gives $m = m_0 + m_1$, so $m_0 = \pi_0(m) \in \pi_0(M)$, in the same way we see $\tilde{M}_1 \subseteq \pi_1(M)$. Conversely, given $m_i \in \pi_i(M)$, $m_i = \pi_i(m)$ with $m \in M$, we have $m_i = \epsilon_i m$, where $\epsilon_1 = (1, 0), \epsilon_2 = (0, 1) \in \Gamma$ are the orthogonal idempotents of $\Gamma$.

Lemma 2.2. With notations as above and $M_i = M \cap V_i$ one has $p\tilde{M}_i \subseteq M_i \subseteq \tilde{M}_i \subseteq M_i^\#$ for $i = 1, 2$.

Proof. $p\Gamma \subseteq \Lambda$ implies $p\tilde{M}_i \subseteq p\Gamma M \subseteq \Lambda M = M$ for $i = 1, 2$, so $p\tilde{M}_i \subseteq M \cap V_i = M_i$. $M_i \subseteq M = \Lambda M \subseteq \Gamma M$ implies $M_i \subseteq \tilde{M}_i$. The inclusion $\tilde{M}_i \subseteq M_i^\#$ is obvious.

Lemma 2.3. With notation as above one has $M = M_0 \perp M_1$ or $M_0$ has determinant divisible by $p$. 

Proof. If $M \neq M_0 \perp M_1$ one has $M_0 \subseteq \tilde{M}_0$, and $(\tilde{M}_0 : M_0)$ is a positive power of $p$ by $pM_0 \subseteq M_0 \subseteq \tilde{M}_0$. But then $\det(M_0) = (M_0 \# : M_0)$ is also divisible by a positive power of $p$. □

**Theorem 2.4.** With notation as above and $m_i = \dim V_i$ ($i = 1, 2$) one has:

If $M$ is indecomposable or decomposable with no proper orthogonal summand of rank $m_0$ and determinant prime to $p$, the $\sigma$-fixed sublattice $M_0 = M \cap V_0$ of $M$ has determinant divisible by $p$.

Proof. Clear from the lemmas above. □

### 3. Congruences of Theta series.

**Theorem 3.1.** Let $(M, q)$ be a positive definite even unimodular lattice on the $m$-dimensional vector space $V$ over $\mathbb{Q}$, having an automorphism of odd prime order $p$, let $V_0 \subseteq V$ be the fixed space of $\sigma$, $m_0 = \dim V_0$, let

$$F_M(Z) = \sum_{T \in M_{m_0}^{\text{sym}}(Z)} A(M, T) \exp(2\pi i \text{tr}(TZ)) \in M_{m/2}(Sp_{m_0}(Z))$$

denote the degree $m_0$ theta series of $(M, q)$, write

$$\Theta F_m(Z) = \sum_{T} \det(T) A(M, T) \exp(2\pi i \text{tr}(TZ)).$$

Then $\Theta F_M \equiv 0 \mod p$ unless $M$ is decomposable and has a proper orthogonal summand of rank $m_0$.

In particular, if $m_0$ is not divisible by 8, $\Theta F_M$ is congruent to zero modulo $p$.

Proof. If $T \in M_{m_0}^{\text{sym}}(Z)$ is a positive definite matrix with $A(M, T) \neq 0$, there are $x_1, \ldots, x_{m_0} \in M$ linearly independent with $b(x_i, x_j) = t_{ij}$ ($1 \leq i, j \leq m_0$), and the set of such $m_0$-tuples $x_1, \ldots, x_{m_0}$ can be split up into $\Pi$-orbits, where each non-trivial orbit has length divisible by $p$.

The orbits with one element consist of tuples $x_1, \ldots, x_{m_0} \in M_0$, these tuples (if there are any) have a Gram matrix $T$ whose determinant is divisible by the determinant of $M_0$. If the exceptional conditions given in the theorem are not satisfied, $\det M_0$ is divisible by $p$, so the assertion follows. □

**Examples 3.2.** a) The Leech lattice has automorphisms of orders 2, 3, 5, 7, 11, 13, 23. Of these, the automorphisms of order 11 and 23 do not act fixed point free. Since the Leech lattice is indecomposable, its theta series $F$ of degree $m_0$ satisfies $\Theta F \equiv 0 \mod p$ for $p = 11$ and for $p = 23$. For $p = 23$ we have $m_0 = 2$, and it is easily seen that the theta series of degree 2 itself has nondegenerate Fourier coefficients which are not divisible by 23 (the automorphism group of the binary fixed lattice $M_0$ has order
not divisible by 23). In fact, from [8] one sees that $M_0$ has Gram matrix

$$
\begin{pmatrix}
4 & 1 \\
1 & 6
\end{pmatrix}.
$$

For $p = 11$, inspection of the character table of the group $Co_1$ in [4] shows that $m_0 = 4$ holds in this case. Since the order of the automorphism group of a lattice of rank 4 can not be divisible by 11, it is again clear that the theta series of degree 4 has non degenerate Fourier coefficients not divisible by 11 and that 4 is the largest degree in which the theta series has this property (whereas the theta series of degree 5 or higher is singular mod $p$ in the terminology of [3]).

Ozeki [7] has recently computed part of the degree 4 theta series of the Leech lattice, he found that the Gram matrix

$$
\begin{pmatrix}
4 & 2 & 1 & 0 \\
2 & 4 & 1 & 1 \\
1 & 1 & 4 & 2 \\
0 & 1 & 2 & 4
\end{pmatrix}
$$

of determinant 121 (belonging to the unique non-principal ideal for a maximal order in the quaternion algebra ramified at $\infty$ and 11) is represented 1259323656192000 times by the Leech lattice (this number is equal to 1/660 times the order of the automorphism group $Co_0$ of the Leech lattice). Since this representation number is not divisible by 11 the lattice generated by a set of representing vectors must be contained in the fixed lattice $M_0$ of an automorphism of order 11, and since this lattice is maximal, it must be equal to $M_0$. We see that the Gram matrix above is indeed associated to the fixed lattice of such an automorphism, and the degree 4 theta series of the Leech lattice is congruent modulo 11 to the theta series of degree 4 of this quaternary lattice.

b) The automorphisms of order 13 of the Leech lattice act (see again the character table in the atlas) fixed point free. If we put $M = M_0 \perp M_1$, where $M_0$ is the $E_8$-lattice and $M_1$ is the Leech lattice, we have $m_0 = 8$, and the degree 8 theta series $F$ of $M$ has Fourier coefficient $|O(E_8)|$ at the Gram matrix $T$ of the $E_8$-lattice, so this coefficient, which is not divisible by 13, also appears in $\Theta F$.

c) Let $M_1$ be any even unimodular positive definite lattice having an automorphism of order $p$ (where $p \neq 2$ is prime) which acts fixed point free and let $M_0$ be any positive definite even unimodular lattice of rank $m_0$ whose automorphism group is trivial (such lattices are known to exist if the rank $m_0$ is at least 144 [1]). Then $m_0$ is the largest degree in which the theta series of $M$ is not singular modulo $p$ and the degree $m_0$ theta series of $M = M_0 \perp M_1$ is not annihilated by the theta operator.
Remark.  a) Theorem 2.4 would in principle also allow to study the action of the theta operator on theta series of non-unimodular lattices.  
b) The degree $m_0$ of the theta series considered in Theorem 3.1 is the maximal degree for which the non-degenerate Fourier coefficients are not forced to be divisible by the prime $p$ (so that the theta series of degree $m_0 + 1$ and higher are singular mod $p$).

References

[1] E. Bannai: Positive definite unimodular lattices with trivial automorphism groups, Mem. Amer. Math. Soc. 85 (1990), no. 429
[2] S. Böcherer, S. Nagaoka: On mod $p$ properties of Siegel modular forms, Mathematische Annalen 338 (2007), 421–433.
[3] S. Böcherer, T. Kikuta: On mod $p$ singular modular forms, Preprint 2013.
[4] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985
[5] I. Hambleton, C. Riehm: Splitting of Hermitian forms over group rings,. Invent. Math. 45 (1978), 19–33
[6] S. Nagaoka, S. Takemori: On theta series attached to the Leech lattice, Preprint 2014
[7] M. Ozeki: Siegel theta series of various degrees of the Leech lattice, Kyushu J. Math. 68 (2014), 63-91
[8] H.-G. Quebbemann: Zur Klassifikation unimodularer Gitter mit Isometrie von Primzahlordnung. J. Reine Angew. Math. 326 (1981)

Rainer Schulze-Pillot  
Fachrichtung 6.1 Mathematik, Universität des Saarlandes (Geb. E2.4)  
Postfach 151150, 66041 Saarbrücken, Germany  
email: schulzep@math.uni-sb.de