ACTA ARITHMETICA
124.1 (2006)

On theta series vanishing at ∞ and related lattices

by

Christine Bachoc (Talence) and Riccardo Salvati Manni (Roma)

1. Introduction. In a recent paper [8], Imamoḡlu and Kohnen have studied the mth power of the Riemann theta function ϑ in relation with the number $r_m(n)$ of representations of a positive integer n as a sum of m integral squares. Their result is interesting, since, for each m, the computation of $r_m(n)$ does not require any pre-knowledge of $r_m(n')$ for $n' < n$. One of the main tools used in this proof was that ϑ^m has highest order of vanishing at one cusp or, better, that a translate of ϑ has highest order of vanishing at the cusp ∞; subsequently Kohnen and the second author extended the result to the integral representations of the lattice D_m^+ (see [9]).

In this paper we want to treat the problem of theta series with the highest order of vanishing at the cusp ∞. When the level is a power of 2, these theta series are the mth powers of a certain theta function with characteristic, related to the quadratic form $2^k 1_m$ or, in the language of lattices, to the lattice $\sqrt{2^k}\,\mathbb{Z}^m$. Instead if the level is a power of 3, these theta series are the $(m/2)$th powers of a theta series associated to the 2-dimensional root lattice A_2 with characteristic. These modular forms have also many representations as theta series related to different lattices.

Let L be an integral lattice of rank m. We denote by $(\cdot,\cdot)$ its associated scalar product, and we say as usual that L is *even* if $(x,x) \equiv 0 \bmod 2$. We define the dual lattice by

$$L' = \{x \in L \otimes \mathbb{Q} \mid (x,y) \in \mathbb{Z} \text{ for all } y \in L\}.$$

If L is even, we define the *level* of L as the minimal positive integer l such that the lattice $\sqrt{l}\,L'$ is an even lattice.

It is a standard method to exploit the properties of the theta series that can be attached to a lattice to derive some interesting arithmetic properties of the lattice. For example, one can derive bounds for the minimum, which turn out to be tight for small levels and dimension. Also the consideration

2000 *Mathematics Subject Classification*: 11H06, 11F11, 11F27.
Key words and phrases: theta series, lattices, codes.

of the shadow of odd lattices and of its theta series has led to interesting results, and the property that a lattice contains designs is controlled by theta series with spherical coefficients.

In this paper, we shall consider cosets of $L/2L$, $L/3L$ and their theta series. In the case of unimodular lattices, among the cosets of $L/2L$, there is a fundamental one, the so-called *canonical class* (cf. [11]), that is characterised by the property that all vectors w in this coset satisfy $(v, w) \equiv (v, v) \bmod 2$ for all $v \in L$. In this paper we shall consider more general cosets.

For any coset $2L + w$, we set

$$m(w) := \min_{x \in 2L+w} (x, x),$$

and for any coset $3L + v$, we set

$$n(v) := \min_{x \in 3L+v} (x, x).$$

We shall prove that for even lattices of level 2^k,

$$m(w) \leq m2^{k-1}.$$

Similarly for even lattices of level 3^k, we will get

$$n(v) \leq m3^k.$$

Both these estimates are sharp. Moreover, we shall characterise the lattices that have a coset reaching these bounds to be the lattices obtained from binary and ternary codes. For a fixed level, the theta series associated to this coset is the same for all these lattices, while their homogeneous theta series may of course vary.

Of special interest is the case of odd unimodular lattices; in this case we get $m(w) \leq m$ and this coset exists if and only if the lattice is isometric to $\mathbb{Z}^m$ and $2L + w$ is the canonical class. This extends the results of [4] and [5].

2. Some basic facts about modular forms. Let $\mathcal{H}$ be the upper complex half-plane. The group $\Gamma(1) := \mathrm{SL}(2, \mathbb{Z})$ acts on it by fractional linear transformations:

$$z \mapsto \sigma \cdot z := \frac{az + b}{cz + d}, \qquad \sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1).$$

For any positive integer N, we denote by $\Gamma(N)$ the subgroup of $\Gamma(1)$ defined by $\sigma \equiv 1_2 \bmod N$. The index of $\Gamma(N)$ in $\Gamma(1)$ is

$$i(N) := N^3 \prod_{p|N} (1 - p^{-2}).$$

We shall also use the intermediate subgroup $\Gamma_0(N)$ defined in $\Gamma(1)$ by the condition $c \equiv 0 \bmod N$ and its subgroup $\Gamma_1(N)$ defined in $\Gamma_0(N)$ by the conditions $a \equiv d \equiv 1 \bmod N$.

Let Γ, k and χ be respectively a subgroup of finite index of $\Gamma(1)$, a positive integer and a character of Γ. Then a *modular form* relative to Γ of weight k and character χ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that for all $\sigma \in \Gamma$,

$$f(\sigma \cdot z) = \chi(\sigma)(cz + d)^k f(z)$$

and f is holomorphic at the cusps. Such forms form a finite-dimensional vector space that we denote by $[\Gamma, k, \chi]$. The graded ring of modular forms

$$A(\Gamma, \chi) := \bigoplus_{k=0}^{\infty} [\Gamma, k, (\chi)^k]$$

is finitely generated and normal. We shall omit the character if it is trivial.

The projective variety associated to the ring of modular forms is the Satake compactification of $\mathcal{H}/\Gamma$. Set-theoretically this is the union of $\mathcal{H}/\Gamma$ and a finite set of cusps, denoted by $\mathcal{C}$. In the $\Gamma(N)$ case, the number of cusps is equal to the index of $\pm\Gamma_1(N)$ in $\Gamma(1)$. It is 1, 3 and $c(N) := i(N)/2N$, according as N is 1, 2 or > 2.

For $N = 1, 2, 4$, the ring $A(\Gamma(N))$ is generated by suitable polynomials in the theta functions with half-integral characteristics $\vartheta_{(a,b)}$ defined by

$$\vartheta_{(a,b)}(z) := \sum_{n \in \mathbb{Z}} e^{\pi i((n+a)^2 z + 2b(n+a))} \qquad (z \in \mathcal{H},\ a, b = 0, 1/2).$$

The theta function $\vartheta_{(1/2,1/2)}$ is identically zero. Only the theta function $\vartheta_{(1/2,0)}(z)$ vanishes at the cusp ∞, in fact it has the expansion

$$\vartheta_{(1/2,0)}(z) = 2e^{\pi i z/4} \sum_{n \geq 0} e^{2\pi i n(n+1)z/2} \qquad (z \in \mathcal{H}).$$

On the theta functions with half-integral characteristics acts the group $\Gamma(1)$. The action can be described on the generators by

$$\vartheta_{(a,b)}(-1/z) = \sqrt{z/i}\, \vartheta_{(b,-a)}(z) \tag{1}$$

where the square root is chosen to be positive on the positive imaginary axis. Moreover we have

$$\begin{cases} \vartheta_{(0,0)}(z+1) = \vartheta_{(0,1/2)}(z), \\ \vartheta_{(0,1/2)}(z+1) = \vartheta_{(0,0)}(z), \\ \vartheta_{(1/2,0)}(z+1) = e^{\pi i/4} \vartheta_{(1/2,0)}(z). \end{cases}$$

From these transformation formulae, it follows that $\vartheta_{(a,b)}(z)^4$ belongs to $[\Gamma(2), 2]$ (see [7]).

Any modular form f of weight k relative to $\Gamma(N)$ has a Fourier expansion of the form

$$f(z) = \sum_{n \geq 0} a(n) e^{2\pi i n z/N} \qquad (z \in \mathcal{H}).$$

For such modular forms we will define the *vanishing order at infinity* $v_\infty(f)$ putting

$$v_\infty(f) := \min_{a(n)\neq 0} (n/N).$$

Moreover we define the *slope* $\mathrm{sl}(f)$ setting

$$\mathrm{sl}(f) := k/v_\infty(f).$$

The following result is rather well known, but we repeat it for the sake of completeness:

PROPOSITION 2.1. *Let $f \in [\Gamma(N), k, \chi]$ with χ of finite order. Then f vanishes identically*:

(1) *if $N = 1$ and $\mathrm{sl}(f) < 12$,*
(2) *if $N = 2$ and $\mathrm{sl}(f) < 4$,*
(3) *if $N > 2$ and $\mathrm{sl}(f) < 12/c(N)$.*

Proof. This follows easily from the classical formula for the degree of the divisor associated to f. With the notations of [10], if $f \in [\Gamma(N), k]$ with k even is non-zero, then ([10, Theorem 2.3.3, Theorem 4.2.11])

$$\sum_{a\in\mathcal{H}/\Gamma(N)\cup\mathcal{C}} \nu_a(f) = \frac{kN}{12}\,|\mathcal{C}|. \tag{2}$$

This follows from the fact that $\mathcal{H}/\Gamma(2)$ and $\mathcal{H}/\Gamma(N)$ have respectively 3 and $c(N)$ cusps (with the definition of [10], $\nu_\infty(f) = Nv_\infty(f)$). In case the character χ is non-trivial (in our situation it is quadratic) or the weight is odd, we replace f by f^2 or by a suitable power of f. ∎

If $N = 1, 2, 4$, we have simple examples showing that these estimates are sharp: the modular form

$$\Delta(z) = (\vartheta_{(1/2,0)}(z)\vartheta_{(0,1/2)}(z)\vartheta_{(0,0)}(z))^8$$

is in $[\Gamma(1), 12]$ and $\mathrm{sl}(\Delta) = 12$, the modular form $\vartheta_{(1/2,0)}(z)^4$ is in $[\Gamma(2), 2]$ and has slope 4, and the modular form $\vartheta_{(1/2,0)}(2z)^2$ is in $[\Gamma(4), 1]$ and has slope 2. We could exhibit examples also for another few cases. In general these examples are not easy to obtain; in fact, theta functions or more generally theta series will not reach the sharp bound, since, geometrically speaking, they do not separate cusps. For example $\vartheta_{(1/2,0)}(4z)^2$ is in $[\Gamma(8), 1]$ and has slope 1 (instead of 1/2). However, as we shall see in the next section we can give a sharp bound for theta series.

3. Lattices and their associated theta series. For any lattice L we define the theta series

$$\vartheta_L(z) = \sum_{x\in L} e^{\pi i(x\cdot x)z} \qquad (z \in \mathcal{H}).$$

We shall also consider theta series with rational characteristic. We proceed as follows: for any $w \in L$, we set

$$\vartheta_{L,w/q} = \sum_{x \in L+w/q} e^{\pi i (x \cdot x) z} \quad (z \in \mathcal{H}).$$

Obviously this definition depends only on cosets $qL+w$, and clearly, $\vartheta_{\mathbb{Z},1}(z) = \vartheta_{(1/2,0)}(z)$. We will be mainly interested in the cases $q = 2, 3$. In the first case we will speak of theta series *with half-integral characteristic*

$$\vartheta_{L,w/2}(z) = \sum_{x \in L+w/2} e^{\pi i (x \cdot x) z} \quad (z \in \mathcal{H}).$$

In the second case we will speak of theta series *with one-third-integral characteristic*

$$\vartheta_{L,v/3}(z) = \sum_{x \in L+v/3} e^{\pi i (x \cdot x) z} \quad (z \in \mathcal{H}).$$

Let A_2 denote the 2-dimensional root lattice with Gram matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ in the basis (e_1, e_2) and let $e := e_1 + e_2$. We have

$$\vartheta_{A_2,e/3}(z) = e^{\pi i \frac{2}{3} z}(3 + 3e^{\pi i 2z} + 6e^{\pi i 4z} + 6e^{\pi i 8z} + \cdots). \tag{3}$$

From the inversion formula (cf. [1, p. 24]), we can calculate that

$$\vartheta_{A_2,e/3}\left(-\frac{1}{z}\right) = \frac{z}{i}\frac{1}{\sqrt{3}} \sum_{y \in A_2'} e^{2\pi i (y,e)} e^{\pi i (y,y) z} \tag{4}$$

$$= \frac{z}{i}\frac{1}{\sqrt{3}} (1 - 3e^{\pi i \frac{2}{3} z} + 6e^{\pi i 2z} + \cdots). \tag{5}$$

We now state our main theorems:

THEOREM 3.1. *Let L be an even lattice of rank m, of level 2^k, $k \geq 0$. Then $m(w) \leq 2^{k-1}m$. Moreover, if for some $w \in L$, $m(w) = 2^{k-1}m$, then $\vartheta_{L,w/2}(z) = \lambda \vartheta_{(1/2,0)}(2^{k-1}z)^m$ for some $\lambda \in \mathbb{R}^*$.*

THEOREM 3.2. *Let L be an even lattice of rank m, of level 3^k, $k \geq 0$. Then $n(v) \leq 3^k m$. Moreover, if for some $v \in L$, $n(v) = 3^k m$, then m is even, and $\vartheta_{L,v/3}(z) = \lambda \vartheta_{A_2,e/3}(3^{k-1}z)^{m/2}$ for some $\lambda \in \mathbb{R}^*$.*

Proof. The proofs of the two theorems are very similar. We shall give all details for Theorem 3.1. For Theorem 3.2 the same proof can be easily adapted. We can assume that the rank m is even, otherwise we replace L by $L \oplus L$. According to Theorem 1.3.13 in Andrianov's book [1, p. 23], when L is unimodular, $\vartheta_{L,w/2}(2z)$ is in $[\Gamma(2), m/2]$. Similarly if L is even of level N, then $\vartheta_{L,w}(z)$ belongs to $[\Gamma(N), m/2, \chi]$ for some quadratic character χ.

Assume that L is unimodular. Then $\vartheta_{L,w/2}(2z)$ has weight $m/2$ and vanishing order $m(w)/4$ at ∞, so from Proposition 2.1(1) we have

$$\mathrm{sl}(\vartheta_{L,w/2}(2z)) = \frac{2m}{m(w)} \geq 4.$$

Hence $m(w) \leq m/2$.

Now we assume that for some $w \in L$, $m(w) = m/2$. Then $\vartheta_{L,w/2}(z)$ and $\vartheta_{(1/2,0)}(z/2)^m$ have the same weight and vanishing order at ∞. Moreover $\vartheta^m_{(1/2,0)}$ does not have other zeros, so $\vartheta_{L,w/2}(z)/\vartheta_{(1/2,0)}(z/2)^m$ is a holomorphic modular function, also at the cusps, hence it is a constant.

The case of level 2 is exactly the same. For the levels $N = 2^k$ with $k > 1$, we need a sharper estimate for the slope of theta series. In the already cited theorem of [1], the transformation formula shows that the theta series $\vartheta_{L,w/2}$ vanishes not only at the cusp ∞, but also at all its $\Gamma_0(N)$-conjugates. Indeed, a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ transforms $L + w/2$ into $L + aw/2 = L + w/2$ because $ad \equiv 1 \bmod 2$, hence $a \equiv 1 \bmod 2$ (in the case of level 3 we have $L + aw/2 = L \pm w/2$). So the vanishing order is equal at all these cusps. The cardinality of the orbit of the cusp ∞ under the action of $\Gamma_0(N)$ is equal to the index of $\pm\Gamma_1(N)$ in $\Gamma_0(N)$, which is $\phi(N)/2 = 2^{k-2}$. Here ϕ is the Euler function.

Because of this result for theta series and again from (2) we have:

Proposition 3.1. *Let L be an even lattice of level 2^k and rank m, and let $f \in [\Gamma(2^k), m/2, \chi]$ be a theta series of the form $\vartheta_{L,w/2}(z)$. Then it vanishes identically if*

$$\mathrm{sl}(f) < \frac{6\phi(2^k)}{c(2^k)} = 2^{3-k}.$$

From this fact the proof of the theorem easily follows. ∎

Remark 3.1. As we wrote, the proof of Theorem 3.2 is similar. Also in this case a proposition similar to Proposition 3.1 holds. Obviously for the slope we get the bound

$$\frac{6\phi(3^k)}{c(3^k)} = 3^{2-k}.$$

Remark 3.2. These precise estimates can be obtained, since in both cases the theta series $\vartheta_{L,w/2}(z)$ and $\vartheta_{L,v/3}(z)$ have equal vanishing order at all cusps $\Gamma_0(q^k)$-conjugate to the cusp ∞, $q = 2, 3$. In all other cases, this is false since we have different vanishing orders, as the characteristics change by a factor $a \in (\mathbb{Z}/q\mathbb{Z})^*$. This is one of the main obstructions to further generalisations of the results of this paper.

Of special interest is the case of odd unimodular lattices. Replacing L by $\sqrt{2}\,L$, an odd unimodular lattice becomes an even lattice of level 4, so we have:

COROLLARY 3.1. *Let L be an odd unimodular lattice of rank m. Then $m(w) \le m$. Moreover, if for some $w \in L$, $m(w) = m$, then $\vartheta_{L,w/2}(z) = \lambda\vartheta_{(1/2,0)}(z)^m$ for some $\lambda \in \mathbb{R}^*$.*

There are well known lattices for which the estimate is sharp, namely $E_8, D_4, \mathbb{Z}^m, A_2$. They are special cases of a more general family of lattices described in the next sections.

Moreover, a natural question is to characterise the cases when this estimate is sharp. This is done in Sections 5 and 8.

4. Lattices from binary codes. We describe some lattices for which there exist elements w with the maximal value for $m(w)$ according to Theorem 3.1.

We recall what is usually meant by "a lattice constructed from a binary code". Let $C \subset \mathbb{F}_2^n$ be a linear binary code of length m. We denote by $\mathbf{1}$ the all-one word. We define

$$L_C := \{(x_1, \dots, x_m) \in \mathbb{Z}^n \mid (x_1, \dots, x_m) \bmod 2 \in C\}.$$

We have the following result:

THEOREM 4.1. *Let C be a binary code with $\mathbf{1} \in C$. Let $w := (1, \dots, 1) \in L_C$. Then $m(w) = m$ and*

$$\vartheta_{L_C,w/2}(z) = \frac{|C|}{2^m}\,\vartheta_{(1/2,0)}(z)^m.$$

Proof. Sending $0 \in \mathbb{F}_2$ to $0 \in \mathbb{Z}$ and $1 \in \mathbb{F}_2$ to $-1 \in \mathbb{Z}$, we define a lifting map $c \mapsto \widetilde{c}$ from $\mathbb{F}_2^m$ to $\mathbb{Z}^m$. We have

$$L_C + w/2 = \bigcup_{c\in C} (2\mathbb{Z})^m + \widetilde{c} + w/2.$$

The vectors $\widetilde{c} + w/2$ have all coordinates equal to $\pm 1/2$. Hence, for every c, a suitable isometry σ of the form $(x_1, \dots, x_m) \mapsto (\varepsilon_1 x_1, \dots, \varepsilon_m x_m)$ with $\varepsilon_i = \pm 1$ sends $(2\mathbb{Z})^m + \widetilde{c} + w/2$ to $(2\mathbb{Z})^m + w/2$. We derive

$$\vartheta_{L_C,w/2} = |C|\vartheta_{(2\mathbb{Z})^m,w/2}.$$

It is immediate that

$$\sum_{x\in 2\mathbb{Z}^n + w/2} e^{\pi i(x,x)z} = \Big(\sum_{n\in\mathbb{Z}} e^{\pi i(2n+1/2)^2}\Big)^m = 2^{-m}\vartheta_{(1/2,0)}(z)^m,$$

which gives the desired formula. ∎

REMARK 4.1. In the case $L = \mathbb{Z}^n$, $w = (1, \dots, 1)$ defines the only coset of norm m; this is not true for other lattices. For example, when $L = D_m$, $w' = (-1, 1, \dots, 1)$ satisfies $m(w') = m$ but $w' \neq w \bmod 2L$.

From the previous theorem, an easy way to construct a lattice L containing an element w with $m(w) = 2^{k-1}m$ is the following: take $L = \sqrt{2^{k-1}}\, L_C$ with C a binary code.

Let us discuss in which cases such a lattice L is even of level 2^k.

(1) $k = 0$. Then $L = (1/\sqrt{2})L_C$ is even unimodular if and only if $C = C^\perp$ and C is doubly even.
(2) $k = 1$. Then $L = L_C$ is even if and only if C is even.
(3) $k > 1$. Then $L = \sqrt{2^{k-1}}\, L_C$ is always even.

Moreover, we need that $2^k(x, x) \in 2\mathbb{Z}$ for all $x \in L'$. Since $L' = (1/\sqrt{2^{k-1}})L'_C$ and since $L'_C = \frac{1}{2}L_{C^\perp}$, we need $(x, x) \in 4\mathbb{Z}$ for all $x \in L_{C^\perp}$. This leads to the condition that $C^\perp$ is doubly even.

Let $\{e_1, \dots, e_m\}$ denote the canonical basis of $\mathbb{Z}^m$. If an even lattice L has the form $L = (1/\sqrt{2})L_C$, the elements $\{\sqrt{2}\, e_1, \dots, \sqrt{2}\, e_m\}$ provide pairwise orthogonal elements of norm 2 in L, also called *roots*.

Conversely, an even lattice L containing m pairwise orthogonal roots is easily seen to be isometric to a lattice of the form $L = (1/\sqrt{2})L_C$.

Standard examples are the following: $C = \mathbb{F}_2(1, \dots, 1)$ leads to $L = L_C = D_m$. The lattice E_8 arises from the extended Hamming code; the Golay code of length 24 leads to the even unimodular lattice in dimension 24 with root system A_1^{24}.

5. Lattices with the largest $m(w)$. Here we characterise all lattices that reach the bounds of Theorem 3.1.

THEOREM 5.1. *Let L be an even lattice of rank m and level 2^k, $k \geq 0$, such that there exists $w \in L$ with $m(w) = 2^{k-1}m$. Then $L = \sqrt{2^{k-1}}\, M$, and there exists a binary code C such that $M = L_C$. Moreover, C has the following properties*:

(1) *If $k = 0$, then $C = C^\perp$ and C is doubly even.*
(2) *If $k = 1$, then $C^\perp$ is doubly even and $\mathbf{1} \in C^\perp$.*
(3) *If $k > 1$, then $C^\perp$ is doubly even.*

In all cases, $w := \sqrt{2^{k-1}}(1, \dots, 1) \in L$ and $m(w) = 2^{k-1}m$.

Proof. From Theorem 3.1, we have $\vartheta_{L,w/2}(z) = \lambda \vartheta_{(1/2,0)}(2^{k-1}z)^m$ for some $\lambda \in \mathbb{R}^*$. We recall the inversion formula for $\vartheta_{L,w/2}(z)$ ([3, Prop. 3.1]):

$$\vartheta_{L,w/2}\left(-\frac{1}{z}\right) = \left(\sqrt{\frac{z}{i}}\right)^m \frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x,w/2)} e^{\pi i z(x,x)}. \tag{6}$$

Taking account of the inversion formula (1) for $\vartheta_{(1/2,0)}$ we obtain

$$\frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x,w/2)} e^{\pi i z(x,x)} = \frac{\lambda}{2^{(k-1)m/2}}\, \vartheta_{(0,1/2)}\left(\frac{z}{2^{k-1}}\right)^m. \tag{7}$$

Since the constant coefficients of the left and right hand side must be equal, we have in fact

$$\sum_{x\in L'} e^{2\pi i(x,w/2)} e^{\pi i z(x,x)} = \vartheta_{(0,1/2)}\left(\frac{z}{2^{k-1}}\right)^m. \tag{8}$$

It is worth noticing that this argument in fact calculates the value of λ. We have

$$\vartheta_{(0,1/2)}(z)^m = \Big(1 + 2\sum_{n\geq 1}(-1)^n e^{\pi i n^2 z}\Big)^m = 1 - 2me^{\pi i z} + \cdots.$$

Now we compare the second coefficient in (8). Set $L_i := \{x \in L \mid (x,x) = i\}$ and $S := L'_{1/2^{k-1}}$. We obtain

$$\sum_{x\in S} e^{\pi i(x,w)} = -2m. \tag{9}$$

The first easy consequence of (9) is that S is non-empty, but we need more: we want to prove that S contains m pairwise orthogonal elements. We first notice that, if x belongs to S, then (x,w) can take only the values $0, \pm 1, \pm 2$. Indeed, since L has level 2^k, we have $2^k x \in L$ and therefore $(w \pm 2^{k+1}x)^2 \geq w^2$, which leads to $|(x,w)| \leq 2$. We partition S into two subsets: $S_0 := \{x \in S \mid (x,w) = 0, \pm 2\}$ and $S_1 := \{x \in S \mid (x,w) = \pm 1\}$. The contribution of the first set to (9) is $+1$ and of the second is -1. Obviously, vectors go in pairs $\pm x$. So (9) tells us that S_1 contains at least $2m$ pairs of elements. Moreover, let us prove that, if $x \neq \pm x' \in S$, then $(x,x') = 0, \pm 1/2^k$. Since L has level 2^k, it follows that $2^{k-1}(y,y) \in \mathbb{Z}$ for any $y \in L'$. Hence, if $x \neq \pm x'$, then $(x \pm x')^2 \geq 1/2^{k-1}$, and therefore $|(x,x')| \leq 1/2^k$. Finally, $2^k x \in L$ implies $(x,x') \in 1/2^k\mathbb{Z}$.

Now assume $(x_1, \ldots, x_s)$ is a maximal chain of pairwise orthogonal elements in S_1. Of course $s \leq m$ and we want to prove that $s = m$. To any $x \in S_1$ not in this chain, we can associate an index i such that $(x, x_i) = \pm 1/2^k$ (from the previous discussion), otherwise we could increase the chain. If, without loss of generality, $(x, x_i) = -1/2^k$, then $x' = x - x_i$ is another element of S but this one belongs to S_0. So the pair (x, x') contributes 0 to the sum (9). Since the chain itself contributes $-2s$, this proves that we must have $s = m$.

We have found a sublattice of L' isometric to $((1/\sqrt{2^{k-1}})\mathbb{Z})^m$. This proves that (up to isometry) $L \subset (\sqrt{2^{k-1}}\,\mathbb{Z})^m$. In the case $k = 0$, i.e. for even unimodular lattices, we have found m pairwise orthogonal roots in $L = L'$, so we are in case (2) described in the previous section.

Assume $k > 0$. Let $M := (1/\sqrt{2^{k-1}})L$; then M is an integral lattice and $M \subset \mathbb{Z}^m$. Moreover, since $2^k L' \subset L$ and $((1/\sqrt{2^{k-1}})\mathbb{Z})^m \subset L'$, we also have $(2\mathbb{Z})^m \subset M$. This obviously means that $M = L_C$ for some binary code C.

The condition $2^k(x,x) \in 2\mathbb{Z}$ for all $x \in L'$ is equivalent to $2(x,x) \in 2\mathbb{Z}$ for all $x \in M'$. Since $M' = (L_C)' = \frac{1}{2}L_{C^\perp}$, this leads to the condition that $C^\perp$ is doubly even. When $k > 1$, L is automatically even; when $k = 1$, $L = L_C$ is even if and only if $\mathbf{1} \in C^\perp$.

In all cases, the code $C^\perp$ is doubly even, which guarantees that $\mathbf{1} \in C$, and hence $w := \sqrt{2^{k-1}}(1,\dots,1) \in L$. From Theorem 4.1, $m(w) = 2^{k-1}m$. ∎

As a consequence, in the case of unimodular lattices we obtain a strengthening of Elkies's result ([4]):

COROLLARY 5.1. *The lattice $\mathbb{Z}^m$ is the unique unimodular lattice of dimension m that contains a coset of minimal norm m. Moreover, this coset is the canonical class.*

Proof. Let U be such a unimodular lattice. From Theorem 3.1, U must be odd. Consider the lattice $L := \sqrt{2}\,U$, which is even of level 4. The assumption on U implies that L contains an element w with $m(w) = 2m$. From the previous theorem, $L = \sqrt{2}\,M$ with $M \subset \mathbb{Z}^m$. Hence $M = U = \mathbb{Z}^m$. ∎

6. Lower bound. In some cases we can give a lower bound for the maximum of the possible $m(w)$. For this purpose we need to introduce theta series with double characteristics. For $w \in L$ and $l \in L' \otimes \mathbb{Q}$, we set

$$\vartheta_{L,w/2,l}(z) = \sum_{x \in L + w/2} e^{\pi i[(x\cdot x)z + 2(x\cdot l)]} \quad (z \in \mathcal{H}).$$

Now let L be an even unimodular lattice such that $2L \subset \mathbb{Z}^m$ and a vector of the form $(1,\dots,1) + 2\mathbb{Z}^m$ is in $2L$. We shall denote this vector by w_0. We remark that all even unimodular 24-dimensional lattices have these properties.

Let d be the order of $\frac{1}{2}L'/\mathbb{Z}^m$. Then we have

$$\sum_{x \in (1/2)L'/\mathbb{Z}^m} e^{2\pi i(x\cdot(w_0/2))}\vartheta_{\mathbb{Z}^m,w_0,x}(z) = \sum_{x \in (1/2)L'/\mathbb{Z}^m} \sum_{y \in \mathbb{Z}^m} e^{\pi i[((y+w_0/2)\cdot(y+w_0/2))z + 2(x\cdot y)]}.$$

Using the orthogonality of characters we get

$$d \sum_{y \in 2L} e^{\pi i((y+w_0/2)\cdot(y+w_0/2))z} = d\vartheta_{2L,w_0}(z) \quad (z \in \mathcal{H}).$$

We know that the theta series $\vartheta_{\mathbb{Z}^m,w,x}(z)$ have vanishing order $m/8$ at the cusp ∞. For a linear combination the vanishing order cannot decrease, thus for the above described lattices, we have $m(w_0/2) \geq m/4$.

Unfortunately this estimate is not sharp, since we know that for even unimodular 24-dimensional lattices we have $\max m(w) \geq 8$. For the Leech lattice we have $\max m(a) = 8$.

7. Lattices from ternary codes. We describe some lattices for which there exist elements v with the maximal value for $n(v)$ according to Theorem 3.2.

Let $C \subset \mathbb{F}_3^n$ be a linear ternary code of length n. Using the isomorphism $A_2/3A_2' \simeq \mathbb{Z}/3\mathbb{Z}$, we can lift a ternary code to a sublattice of A_2^n:

$$L_C := \{(x_1, \dots, x_n) \in A_2^n \mid (x_1, \dots, x_n) \bmod (3A_2')^n \in C\}.$$

The resulting lattice is of dimension $m = 2n$, and is even since it is a sublattice of A_2^n. It has level 3, 9 or 27; the case of level 3 corresponds to $C^\perp \subset C$.

It is worth noticing that $e/3 \in A_2'$ and hence $(e, \dots, e) \in L_C$. We have the following result:

THEOREM 7.1. *Let C be a ternary code. Let $v := (e, \dots, e) \in L_C$. Then $n(v) = m$ and*

$$\vartheta_{L_C, v/3}(z) = \frac{|C|}{3^{m/2}}\, \vartheta_{A_2, e/3}(z)^{m/2}.$$

Proof. We fix a preimage $\widetilde{a} \in A_2$ of each element $a \in \mathbb{F}_3$ in the following way: $[\widetilde{0}, \widetilde{1}, \widetilde{2}] = [0, -e_1, -e_2]$, and define $\widetilde{c}$ for all $c \in \mathbb{F}_3^n$ in the obvious way. Then

$$L_C + v/3 = \bigcup_{c \in C} (v/3 + \widetilde{c} + (3A_2')^n).$$

The coordinates of $v/3 + \widetilde{c}$ belong to $\{e/3, e/3 - e_1, e/3 - e_2\}$. These three vectors have the same norm $2/3$, moreover they are transitively permuted by the automorphism group of A_2. Let $\sigma_i \in \mathrm{Aut}(A_2)$ be such that $e/3 = \sigma_i(e/3 + \widetilde{c_i})$ and let $\sigma := (\sigma_1, \dots, \sigma_n)$. Obviously, $\sigma \in \mathrm{Aut}((3A_2')^n)$, and hence $v/3 + \widetilde{c} + (3A_2')^n = \sigma(v/3 + (3A_2')^n)$. As a consequence, the classes $v/3 + \widetilde{c} + (3A_2')^n$ and $v/3 + (3A_2')^n$ have the same theta series, and

$$\vartheta_{L_C, v/3}(z) = |C| \vartheta_{3A_2', e}(z)^{m/2}.$$

Moreover, the decomposition $A_2 = 3A_2' \cup (3A_2' - e_1) \cup (3A_2' - e_2)$ and the transitive action of $\mathrm{Aut}(A_2)$ on $\{e/3, e/3 - e_1, e/3 - e_2\}$ show that

$$\vartheta_{A_2, e/3}(z) = 3\vartheta_{3A_2', e/3}(z),$$

which yields the desired formula. ∎

8. Lattices with the largest $n(v)$. Here we characterise all lattices that reach the bounds of Theorem 3.2.

THEOREM 8.1. *Let L be an even lattice of rank m and level 3^k, $k \geq 0$, such that there exists $v \in L$ with $n(v) = 3^k m$. Then $L = \sqrt{3^k}\, M$, and there exists a ternary code C such that $M = L_C$. Moreover, C has the following properties*:

(1) *If* $k = 0$, *then* $C = C^\perp$.
(2) *If* $k > 0$, *then* $C^\perp \subset C$.

Proof. From Theorem 3.2, we have $\vartheta_{L,v/3}(z) = \lambda \vartheta_{A_2,e/3}(3^{k-1}z)^{m/2}$ for some $\lambda \in \mathbb{R}^*$.

We recall the inversion formula for $\vartheta_{L,v/3}(z)$ ([3, Prop. 3.1]):

$$\vartheta_{L,v/3}\left(-\frac{1}{z}\right) = \left(\sqrt{\frac{z}{i}}\right)^m \frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x,v/3)} e^{\pi i z(x,x)}.$$

Taking account of the inversion formula (4) for $\vartheta_{A_2,e}$ we obtain

$$\frac{1}{\sqrt{\det(L)}} \sum_{x \in L'} e^{2\pi i(x,v/3)} e^{\pi i(x,x)z} = \frac{\lambda}{3^{m/2(k-1/2)}} \left(1 - \frac{3m}{2} e^{\pi i \frac{2}{3^k} z} + \cdots\right)$$

from which we obtain

$$\sum_{x \in (L')_{2/3^k}} e^{2\pi i(x,v/3)} = -\frac{3m}{2}. \tag{10}$$

Let $S := (L')_{2/3^k}$. Similar arguments to those in the case of level 2 show that $|(v,x)| \le 3$. We set for $i = 0, 1, 2$,

$$S_i := \{x \in S \mid (x,v) = i \bmod 3\}.$$

If $x \in S_0$, then $-x \in S_0$ and the pair $(x, -x)$ contributes 2 to (10); if $x \in S_1$, then $-x \in S_2$ and $(x, -x)$ contributes -1 (and similarly if $x \in S_2$).

Similar arguments to the case of level 2 show that the set $R := 3^{k/2}S$ satisfies $(r, r') = 0, \pm 1, \pm 2$ for all $r, r' \in R$ and hence is a root system. Defining R_0, R_1, R_2 in the obvious way, we let s be the maximal integer such that a chain A_2^s is contained in $R_1 \cup R_2$ (here A_2 denotes the root system, not the root lattice). The contribution of this A_2^s to (10) equals $-3s$. Our goal is to prove that $s = m/2$.

Let $x \in R_1 \cup R_2$, $x \notin \mathrm{A}_2^s$. There are two possibilities:

(1) x is orthogonal to all the elements of A_2^s.
(2) There exists one component A_2 and one root r in this component such that $(x, r) = -1$.

If several elements x are as in case (1), they can only be pairwise orthogonal since otherwise s would not be maximal. So this leads to a root system of type $A_2^s \perp A_1^t$ and $2s + t \le m$. The contribution to (10) is $-3s - t$. Since $-3s - t = (-2s - t) - s \ge -m - m/2$, it can reach $-3m/2$ only if $s = m/2$ and $t = 0$.

Now let us consider case (2). The component A_2 together with x generate a root lattice of dimension 3 which can only be isometric to A_3, and hence contains twelve roots. We need to discuss how many of these roots belong to R_0 and how many to $R_1 \cup R_2$. It is easy to exhaust all possibilities since these

roots are linear combinations of a given basis (r_1, r_2) of the component A_2 and of x, with $(x, r_1) = -1$ and $(x, r_2) = 0$. We have $(v, x), (v, r_1), (w, r_2) \in [1, -1, 2, -2]$ and they uniquely determine the other values (v, r) when r is one of these twelve roots. By the computation of all possibilities, after having eliminated irrelevant possibilities (e.g. $|(v, r)| > 3$ for some r), we find that the contribution of these twelve roots is either -3 or 0. The conclusion is that there is no hope that such a root x can make the value of the summation decrease. In order to have (10), we must have $s = m/2$.

The end of the argument is essentially the same: we have found a sublattice of L' isometric to $((1/\sqrt{3^{k-1}})A_2')^{m/2}$, which proves that up to isometry $L \subset (\sqrt{3^{k-1}}A_2)^{m/2}$. Let $M := (1/\sqrt{3^{k-1}})L$. The lattice M is a sublattice of $A_2^{m/2}$, hence is even. Moreover, $(3A_2')^{m/2} \subset M \subset (A_2)^{m/2}$, which means that M arises from a ternary code.

When $k = 0$, we want $L = (1/\sqrt{3})L_C$ to be unimodular, which is equivalent to $C = C^\perp$. When $k > 0$, L has level 3^k if and only if $M = L_C$ has level 3, which is equivalent to $C^\perp \subset C$. ∎

References

[1] A. Andrianov, *Quadratic Forms and Hecke Operators*, Grundlehren Math. Wiss. 286, Springer, Berlin, 1987.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren Math. Wiss. 290, Springer, Berlin, 1988.

[3] W. Ebeling, *Lattices and Codes*, Vieweg, Braunschweig, 1994.

[4] N. Elkies, *A characterization of the* $\mathbb{Z}^n$ *lattice*, Math. Res. Lett. 2 (1995), 321–326.

[5] —, *Lattices and codes with long shadows*, ibid., 643–651.

[6] E. Freitag, *Singular Modular Forms and Theta Relations*, Lecture Notes in Math. 1487, Springer, Berlin, 1991.

[7] J. Igusa, *Theta Functions*, Grundlehren Math. Wiss. 194, Springer, Berlin, 1972.

[8] O. Imamoḡlu and W. Kohnen, *Representations of integers as sums of an even number of squares*, Math. Ann. 333 (2005), 815–829.

[9] W. Kohnen and R. Salvati Manni, *On the theta series attached to* D_m^+*-lattices*, Int. J. Number Theory 2 (2006), 1–5.

[10] T. Miyake, *Modular Forms*, Springer, Berlin, 1989.

[11] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, Berlin, 1973.

Laboratoire A2X
Université Bordeaux I
351, cours de la Libération
33405 Talence, France
E-mail: bachoc@math.u-bordeaux1.fr

Dipartimento di Matematica
Università di Roma
Piazzale Aldo Moro, 2
I-00185 Roma, Italy
E-mail: salvati@mat.uniroma1.it

Received on 8.7.2005
and in revised form on 24.3.2006 (5029)