ACTA ARITHMETICA
XVII (1970)

Cyclic overlattices, I

by

A. J. JONES (Cambridge)

1. Introduction. In 1967 Davenport and Schinzel ([2]) related a curious problem of Diophantine approximation to a conjecture of R. M. Robinson ([5]) concerning sums of three roots of unity. If $\|\theta\|$ denotes the distance from θ to the nearest integer their approximation problem was as follows. Let $a_1, \ldots, a_k, q$ be given integers with

$$(a_1, \ldots, a_k, q) = 1.$$

Then can we find an integer n with $(n, q) = 1$ for which

$$\max_{1 \leqslant i \leqslant k} \|na_i/q\| < \delta,$$

where δ is a small positive number? (The particular case $k = 2$ is relevant to Robinson's conjecture.)

In discussing this question their method was partly analytical and the step from $k = 2$ to general positive integral k involved no special complications (see their elegant Theorem 3, [2]). However one of the drawbacks of their approach was that it became effective only for comparatively large q, for example in the case $k = 2$ with $\delta \sim 1/7$ they required $q \geqslant 4 \times 10^{10}$ which left a finite (but large) number of cases in Robinson's conjecture undecided.

In 1968 ([3]) I was able to settle Robinson's conjecture by considering the same question of Diophantine approximation (for $k = 2$ only) but this time using techniques from the Geometry of Numbers (see also [4]). It was natural to ask if these techniques could be generalised to produce a result, similar to that of Davenport and Schinzel, for general k. In fact the step from $k = 2$ to general k was not straight-forward and involved proving several other related results beforehand. These results, on what I have called *cyclic overlattices*, form the substance of this paper. In fact the proof of a somewhat improved version of the Davenport–Schinzel theorem will be postponed for a second paper concerned with applications of the cyclic overlattice theory.

I would like to record here my gratitude to the late Professor Davenport who having given much helpful advice during the early stages of this work sadly never saw its completion. I would also like to thank Professor Cassels, to whom I am greatly indebted, for many stimulating conversations and much encouragement.

2. Some basic notions. Let M be any k dimensional lattice of determinant $d(\mathsf{M}) = 1$. (The assumption of unit determinant is merely to avoid a factor $d(\mathsf{M})$ continually occuring in subsequent formulae.) Suppose further that $\mathsf{M} \subset \Lambda$, where Λ is another k dimensional lattice such that Λ/M is a finite cyclic group. In other words Λ is obtained from M by taking some point $\boldsymbol{a} \notin \mathsf{M}$, having the property that $q\boldsymbol{a} \in \mathsf{M}$ for some integer q (naturally we take q to be the least such positive integer), and then considering all points $\boldsymbol{m}+t\boldsymbol{a}$ where $\boldsymbol{m} \in \mathsf{M}$ and t is any integer. In this situation we say that Λ is a *cyclic overlattice* of M and refer to such points $\boldsymbol{a}$ as *generating points* of Λ over M.

For any two lattices M, Λ, where $\mathsf{M} \subset \Lambda$, the index of M in Λ, written $[\Lambda:\mathsf{M}]$, is defined as the ratio $d(\mathsf{M})/d(\Lambda)$. It is of course a positive integer. There is another characterisation of $[\Lambda:\mathsf{M}]$ which is often useful. We say that two vectors $\boldsymbol{c}, \boldsymbol{d}$ of Λ are in the same class with respect to M if $\boldsymbol{c}-\boldsymbol{d}$ is in M. Then $[\Lambda:\mathsf{M}]$ is precisely the number of distinct classes in Λ with respect to M (see for example Cassels [1], I, Lemma 1).

If Λ is a cyclic overlattice of M the above observation has a useful implication. Put

$$\boldsymbol{c} = \boldsymbol{m}_1 + t_1\boldsymbol{a}, \quad \boldsymbol{d} = \boldsymbol{m}_2 + t_2\boldsymbol{a},$$

where $\boldsymbol{m}_i \in \mathsf{M}$, t_i is an integer $(i = 1, 2)$ and $\boldsymbol{a}$ is a generating point of Λ over M. Then $\boldsymbol{c}-\boldsymbol{d}$ is in M if and only if $t_1 \equiv t_2 \pmod{q}$ where q is defined as before. Consequently the number of distinct classes in Λ with respect to M is q, so that

$$q = [\Lambda:\mathsf{M}] = d(\mathsf{M})/d(\Lambda)$$

whence

$$d(\Lambda) = 1/q. \tag{1}$$

Let F be a distance function defined in the space of M and Λ and associated with a bounded convex body. Then $F(\boldsymbol{x}) \neq 0$ if $\boldsymbol{x} \neq \boldsymbol{0}$ and

$$F(\boldsymbol{x}+\boldsymbol{y}) \leqslant F(\boldsymbol{x}) + F(\boldsymbol{y})$$

(see for example Cassels [1], IV, § 2–3). Let M^*, Λ^* and F^* be the duals of M, Λ and F respectively, so that

$$\Lambda^* \subset \mathsf{M}^*, \quad [\mathsf{M}^*:\Lambda^*] = q, \tag{2}$$

and F^* is convex since F is. *In much of what follows we make the following condition* :

CONDITION C. $F^*(\boldsymbol{x}^*) \geqslant 1$ *for all* $\boldsymbol{x}^* \in \mathsf{M}^*$, $\boldsymbol{x}^* \neq \boldsymbol{0}$.

For our purposes this is a necessary but quite reasonable restriction on F^*.

Let $D > 1$ be any given real number and consider the set $\mathscr{S}_D$ of points $\boldsymbol{x}^* \in \Lambda^*$ with $F^*(\boldsymbol{x}^*) < D$. This set is always non-empty since $\boldsymbol{0} \in \mathscr{S}_D$ and it spans a (possibly trivial) subspace W_D^*, say, of the dual space. Put

$$\Lambda_D^* = W_D^* \cap \Lambda^*, \quad \mathsf{M}_D^* = W_D^* \cap \mathsf{M}^*. \tag{3}$$

Then Λ_D^* and M_D^* are lattices and

$$\Lambda_D^* \subset \mathsf{M}_D^*. \tag{4}$$

Consider the following elegant result which is due to Professor J. W. S. Cassels and appears here for the first time with his kind permission.

THEOREM 1 (Cassels). *Suppose that* $\Lambda_D^* \neq \mathsf{M}_D^*$. *Then*

$$F(\boldsymbol{a}) > 1/D \tag{5}$$

for every $\boldsymbol{a} \in \Lambda$ *which generates* Λ *over* M.

Proof. We denote the canonical pairing by (,). Let $\boldsymbol{a}$ generate Λ over M and let $\boldsymbol{x}^* \in \mathscr{S}_D$. Then $(\boldsymbol{x}^*, \boldsymbol{a}) \in \boldsymbol{Z}$, where $\boldsymbol{Z}$ denotes the set of integers, from the definition of a dual lattice.

If $(\boldsymbol{x}^*, \boldsymbol{a}) \neq 0$, we have

$$|(\boldsymbol{x}, \boldsymbol{a})| \geqslant 1$$

and so (see for example Cassels [1], IV, Theorem III, Corollary 1)

$$F^*(\boldsymbol{x})F(\boldsymbol{a}) \geqslant 1,$$

that is

$$F(\boldsymbol{a}) \geqslant 1/F^*(\boldsymbol{x}^*) > 1/D$$

since $\boldsymbol{x}^* \in \mathscr{S}_D$.

Hence the conclusion of the theorem holds unless

$$(\boldsymbol{x}^*, \boldsymbol{a}) = 0 \quad (\text{all } \boldsymbol{x}^* \in \mathscr{S}_D).$$

But then

$$(\boldsymbol{x}^*, \boldsymbol{a}) = 0 \quad (\text{all } \boldsymbol{x}^* \in W_D^*)$$

which implies

$$(\boldsymbol{x}^*, \boldsymbol{a}) = 0 \quad (\text{all } \boldsymbol{x}^* \in \mathsf{M}_D^*). \tag{6}$$

Now any $x \in \Lambda$ is of the form $x = m + ta$ where $m \in M$ and $t \in Z$. So for any $x^* \in M_D^*$ we have

$$(x^*, x) = (x^*, m+ta) = (x^*, m) + t(x^*, a) = (x^*, m)$$

by (6). Now $(x^*, m) \in Z$ since $m \in M$ and $x^* \in M_D^*$ which is a subset (but not necessarily a sub-lattice) of M^*. Thus (6) implies that for any $x^* \in M_D^*$

$$(x^*, x) \in Z \quad (\text{all } x \in \Lambda).$$

Hence $x^* \in \Lambda^*$. But $x^* \in W_D^*$ so that x^* must be a point of Λ_D^*. Therefore $M_D^* \subset \Lambda_D^*$ and so by (4) $\Lambda_D^* = M_D^*$ which is contrary to hypothesis.

Our first objective is to show that this theorem has a good converse (cf. § 4, Theorem 2), originally conjectured in a slightly weaker form by Professor Cassels.

3. Two preliminary lemmas.

LEMMA 1. *Let V be a k dimensional vector space with dual V^* and let Λ, M be any lattices in V such that*

$$M \subset \Lambda \quad \text{and} \quad [\Lambda : M] < \infty.$$

Let W be a $k-r$ dimensional subspace of V such that $W \cap \Lambda$ contains $k-r$ linearly independent points (i.e., is a lattice). Let Λ^*, M^* be the dual lattices and define $\hat{W}$, an r dimensional subspace of V^*, by

(7) $$\hat{W} = \{\hat{w} \in V^* \,|\, (\hat{w}, w) = 0 \ \forall w \in W\},$$

then

(8) $$[W \cap \Lambda : W \cap M][\hat{W} \cap M^* : \hat{W} \cap \Lambda^*] = [\Lambda : M] \quad (= [M^* : \Lambda^*]).$$

Proof. Let φ be the projection $V \to V/W = \varphi(V)$ onto the quotient space. The kernel of φ is just W and so

(9) $$[\Lambda : M] = [W \cap \Lambda : W \cap M][\varphi(\Lambda) : \varphi(M)].$$

But $\varphi(V) = V/W$ is r dimensional and the duality between V and V^* clearly induces a duality between $\varphi(V)$ and $\hat{W}$, for $\varphi(V)^* = (V/W)^*$ is the set of all functionals on V which vanish over W and this is isomorphic to $\hat{W}$ in the obvious way. Clearly $\varphi(\Lambda)$ is the dual lattice to $\hat{W} \cap \Lambda^*$ and similarly for M. Hence

$$[\varphi(\Lambda) : \varphi(M)] = [\hat{W} \cap M^* : \hat{W} \cap \Lambda^*],$$

and this together with (9) gives (8).

Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the successive minima of Λ with respect to F. Then

(10) $$\lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_k$$

and by a classical theorem of Minkowski

(11) $$2^k d(\Lambda)/k! \leqslant \lambda_1 \lambda_2 \ldots \lambda_k V_F \leqslant 2^k d(\Lambda)$$

where V_F is the volume of the bounded convex set $\{x |\ F(x) < 1\}$. If $\mu_1, \mu_2, \ldots, \mu_k$ are the successive minima of Λ^* with respect to the distance function F^* dual to F then by a well known theorem of Mahler we have

(12) $$1 \leqslant \lambda_j \mu_{k+1-j} \leqslant k! \quad (1 \leqslant j \leqslant k).$$

Further we may choose a basis $x_1, x_2, \ldots, x_k$ of Λ so that, if $x_1^*, x_2^*, \ldots, x_k^*$ is the basis of Λ^* defined by

(13) $$(x_j^*, x_i) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

the following three conditions are satisfied. Firstly

(14) $$\begin{cases} F^*(x_k^*) = \mu_1, \\ 2F^*(x_j^*) \leqslant (k+1-j)\mu_{k+1-j} \quad (k-1 \geqslant j \geqslant 1). \end{cases}$$

Secondly if $a_1^*, a_2^*, \ldots, a_k^*$ is a fixed set of minimal points for Λ^* so that

(15) $$F^*(a_j^*) = \mu_j \quad (1 \leqslant j \leqslant k),$$

then $x_k^*, x_{k-1}^*, \ldots, x_{k+1-r}^*$ $(1 \leqslant r \leqslant k)$ form a basis for the subspace spanned by the first r of the previously chosen minimal points (note that in general this subspace really does depend on the a_j^* since the minimal points are not necessarily unique). Finally

(16) $$F(x_j) F^*(x_j^*) \leqslant (\tfrac{1}{2})^{k-1}(k!)^2 \quad (1 \leqslant j \leqslant k).$$

(For this result see Cassels [1], VIII, Theorem VII, Corollary, where we have interchanged the lattice and its dual.)

Observe that this choice of basis of Λ has the consequence that

(17) $$F(x_j) \leqslant (\tfrac{1}{2})^{k-1}(k!)^2 \lambda_j \quad (1 \leqslant j \leqslant k).$$

For it follows from the definition of μ_j that $F^*(x_j^*) \geqslant \mu_{k+1-j}$ so that (16) implies

$$F(x_j) \leqslant (\tfrac{1}{2})^{k-1}(k!)^2 \mu_{k+1-j}^{-1}$$

whence (17) on using the left-hand inequality in (12).

If a is a fixed generating point of Λ over M and x is any point of Λ we write as usual

(18) $$x = m + ta$$

where $m \in \mathsf{M}$ and $t \in \mathbf{Z}$. Let $m_1, m_2, \ldots, m_k$ be any basis for M. The basis x_j for Λ may be written as

$$(19)\qquad \begin{aligned} x_1 &= \sum_{i=1}^{k} u_{1i} m_i + t_1 a, \\ &\ldots\ldots\ldots\ldots \\ x_k &= \sum_{i=1}^{k} u_{ki} m_i + t_k a, \end{aligned}$$

where the u_{ij} and the t_j are all integers. The integers t_j will assume considerable importance in what follows.

Next define integers $\tau_1, \tau_2, \ldots, \tau_k$ by

$$(20)\qquad \begin{aligned} \tau_1 &= (t_1, q), \\ \tau_2 &= (t_1, t_2, q), \\ &\ldots\ldots\ldots\ldots \\ \tau_k &= (t_1, t_2, \ldots, t_k, q). \end{aligned}$$

We observe that $\tau_k = 1$. For every point of Λ is expressible in the form

$$x = u_1 x_1 + \ldots + u_k x_k$$

for some integers $u_1, \ldots, u_k$. If x is so expressed, then the value of t which corresponds to x in (18) is given by

$$t = u_1 t_1 + \ldots + u_k t_k.$$

Since t can take all integral values, we must have $(t_1, \ldots, t_k) = 1$ and so *a fortiori*, $\tau_k = 1$.

Let W_i $(1 \leqslant i \leqslant k-1)$ be the subspace of V (the space of Λ and M) spanned by $x_1, x_2, \ldots, x_{k-i}$. Similarly let $\Lambda_i = W_i \cap \Lambda$ and $\mathsf{M}_i = W_i \cap \mathsf{M}$, be the corresponding $k-i$ dimensional lattices. Let

$$\hat{W}_i = \{\hat{w} \in V^* \mid (\hat{w}, w) = 0 \ \ \forall w \in W_i\}$$

hence by (13) $\hat{W}_i$ is spanned by $x_k^*, x_{k-1}^*, \ldots, x_{k+1-i}^*$. If $\hat{\Lambda}_i = \hat{W}_i \cap \Lambda^*$ and $\hat{\mathsf{M}}_i = \hat{W}_i \cap \mathsf{M}^*$ we have the following corollary to Lemma 1.

Corollary 1. *For* $1 \leqslant i \leqslant k-1$

$$(21)\qquad [\hat{\mathsf{M}}_i : \hat{\Lambda}_i] = \tau_{k-i}$$

where the τ_{k-i} *are defined by* (20).

Proof. Clearly, from (19),

$$[W_i \cap \Lambda : W_i \cap \mathsf{M}] = q/(t_1, \ldots, t_{k-i}, q) = q/\tau_{k-i}.$$

Since $[\Lambda : \mathsf{M}] = q$ we deduce from Lemma 1 that

$$[\hat{W}_i \cap \mathsf{M}^* : \hat{W}_i \cap \Lambda^*] = [\hat{\mathsf{M}}_i : \hat{\Lambda}_i] = \tau_{k-i}$$

as required.

We also have

Corollary 2. *If* $\dim W_D^* = r$ $(0 \leqslant r \leqslant k-1)$ [1] *and* $\Lambda_D^* = \mathsf{M}_D^*$ *then*

$$(22)\qquad \tau_k = \tau_{k-1} = \ldots = \tau_{k-r} = 1.$$

Proof. If $\dim W_D^* = 0$ we have only to show that $\tau_k = 1$ which we have already proved is always the case. Otherwise there are exactly r linearly independent points in $\mathscr{S}_D$. This means that

$$\mu_r < D \leqslant \mu_{r+1}$$

and so W_D^* is the space spanned by the successive minimal points $a_1^*, \ldots, a_r^*$. By the second condition on our choice of bases for Λ and Λ^* this space is the space spanned by $x_k^*, \ldots, x_{k+1-r}^*$ which is precisely $\hat{W}_r$. Hence $\Lambda_D^* = \hat{\Lambda}_r$ and $\mathsf{M}_D^* = \hat{\mathsf{M}}_r$ so that

$$\tau_{k-r} = [\hat{\mathsf{M}}_r : \hat{\Lambda}_r] = [\mathsf{M}_D^* : \Lambda_D^*] = 1$$

by (21) with $i = r$ and hypothesis. The conclusion is now immediate since by (20) $\tau_{k-1} | \tau_{k-2} | \ldots | \tau_{k-r} = 1$.

Lemma 2. *If* F^* *satisfies the condition* C *then*

$$(23)\qquad \tau_{k-i} \leqslant c(k)\mu_1\mu_2\ldots\mu_i \quad (1 \leqslant i \leqslant k-1),$$

where $c(k)$ *denotes a positive constant depending only on* k.

Proof. The points of $\hat{\mathsf{M}}_i$ are of the form

$$a_1 x_k^* + \ldots + a_i x_{k+1-i}^*,$$

where the $(a_1, \ldots, a_i)$ run over a lattice of determinant $d = \tau_{k-i}^{-1}$ by (21).

Consider the convex symmetric body in a-space, defined by

$$(24)\qquad |a_j| < 1/(ij\mu_j) \quad (1 \leqslant j \leqslant i).$$

If this body has volume v greater than $2^i d$ then, by Minkowski's "first" theorem, it must contain a point $(a_1, \ldots, a_i)$ of the lattice other than the origin. If

$$x^* = a_1 x_k^* + \ldots + a_i x_{k+1-i}^*$$

then as F^* is convex we have

$$F^*(x^*) \leqslant |a_1| F^*(x_k^*) + \ldots + |a_i| F^*(x_{k+1-i}^*),$$

[1] We agree to adopt the convention that $r = 0$ if $\mathscr{S}_D = \{0\} = W_D^*$.

whence by (24) and (14) $F^*(x^*) < 1$ for $x^* \in \mathsf{M}^*$, $x^* \neq \mathbf{0}$ which is contrary to the condition C.

Hence

$$v = \prod_{j=1}^{i} 1/(ij\mu_j) \leqslant 2^i d$$

so that

$$(i^i 2^i (i)!\,\mu_1 \ldots \mu_i)^{-1} \leqslant d = \tau_{k-i}^{-1},$$

whence

$$\tau_{k-i} \leqslant c(i)\,\mu_1 \ldots \mu_i \leqslant c(k)\,\mu_1 \ldots \mu_i$$

which concludes the proof of the lemma.

We next introduce a useful function. For any positive integer n define $g(n)$ to be the least integer g such that amongst any g consecutive integers, there is at least one that is coprime to n. This function was studied in some detail by Jacobsthal and references to his work, which is not strictly relevant to this paper, can be found in [3] or [4]. Clearly $g(n)$ depends only on the square-free part of n, if $m|n$ then $g(m) \leqslant g(n)$ and

$$g(1) = 1, \quad g(p) = 2 \quad \text{for any prime } p.$$

It was proved in Lemma 6 of [3] that

(25) $$g(n) < n 2^{\nu(n)}/\varphi(n),$$

where $\nu(n)$ denotes the number of distinct prime factors of n. Since

$$2^{\nu(n)} = O(n^{\varepsilon}), \quad n/\varphi(n) = O(n^{\varepsilon})$$

(25) clearly implies that

(26) $$g(n) \leqslant c(\varepsilon)\, n^{\varepsilon}$$

for any $\varepsilon > 0$.

4. The principal results. We are now in a position to prove

THEOREM 2. *Suppose that F^* satisfies condition* C, $\Lambda_D^* = \mathsf{M}_D^*$ *and that* $\dim W_D^* = r$. *Let* $[\Lambda : \mathsf{M}] = q > 1$. *Then* $0 \leqslant r \leqslant k-1$ *and given any* $\varepsilon > 0$ *there is a point* $x \in \Lambda$ *which generates* Λ *over* M *and satisfies one of the following inequalities*

(27) $$F(x) \leqslant c(k, \varepsilon) D^{-1+\varepsilon} \quad \text{if} \quad 0 \leqslant r \leqslant k-3 \ (k \geqslant 3),$$

(28) $$F(x) \leqslant c(k, \varepsilon) q^{\varepsilon} \min\{2(V_F q)^{-1/k},\ k!\,D^{-1}\} + c(k) D^{-1},$$

where V_F *is the volume of the body* $\mathcal{K} = \{x | F(x) < 1\}$, *if* $r = k-2$ $(k \geqslant 2)$, *or*

(29) $$F(x) \leqslant c(k) \min\{2(V_F q)^{-1/k},\ k!\,D^{-1}\}$$

if $r = k-1$ $(k \geqslant 1)$.

Here $c(k)$ (or $c(k, \varepsilon)$) represents a positive constant, depending only on k (or k and ε), which is not necessarily the same on each appearance.

We note in passing that condition C on F^* implies that $V_F^{-1} \leqslant c(k)$. For by Minkowski's "first" theorem condition C implies $V_{F^*} \leqslant 2^k d(\mathsf{M}^*)$ where V_{F^*} denotes the volume of the body $\mathcal{K}^* = \{x^* | F^*(x^*) < 1\}$ dual to $\mathcal{K}$. Now $d(\mathsf{M}^*) = d(\mathsf{M}) = 1$, hence $V_F^{-1} \leqslant c(k)$ since

$$c(k) \leqslant V_F V_{F^*} \leqslant c(k)$$

(see for example Cassels [1], IV, Theorem VI). A consequence of this fact is that (29) implies an upper bound for $F(x)$ of the form $c(k) q^{-1/k}$, and if we choose $\varepsilon = 1/(k+1)$ (say) then (28) gives a bound of the form $c(k) D^{-1}$.

Proof. We first deal with the dimension of W_D^*. If $r = k$ then W_D^* is the whole dual space and so by (3) and the hypothesis of the theorem we have $\Lambda^* = \Lambda_D^* = \mathsf{M}_D^* = \mathsf{M}^*$, an obvious contradiction since $[\Lambda : \mathsf{M}] = [\mathsf{M}^* : \Lambda^*] = q > 1$. Hence $0 \leqslant r \leqslant k-1$.

We shall construct a point x of Λ which generates Λ over M and satisfies one of the inequalities (27), (28) or (29) according to the value of r.

If x is any point of Λ expressed in the usual form

$$x = m + ta \quad (m \in \mathsf{M},\ t \in \mathbf{Z})$$

then recalling the discussion in § 2 concerning the classes in Λ with respect to M we make the following observation. *The point x will itself be a generating point of Λ over M if and only if $(t, q) = 1$.*

Consider the point

(30) $$x = u_1 x_1 + \ldots + u_{k-r-1} x_{k-r-1} + x_{k-r}$$

which has

(31) $$t = u_1 t_1 + \ldots + u_{k-r-1} t_{k-r-1} + t_{k-r}.$$

By Lemma 1 Corollary 2

(32) $$\tau_{k-r} = (t_1, \ldots, t_{k-r}, q) = 1.$$

We shall choose the integers $u_{k-r-1}, \ldots, u_1$ (in that order) so that $(t, q) = 1$.

Divide the primes p which divide q into $k-r-1$ disjoint sets defined as follows. Let

$$S_1 = \{p |\ p | q,\ p \nmid t_1\}$$

and for $2 \leqslant i \leqslant k-r-1$

$$S_i = \{p |\ p | q,\ p | t_1, \ldots, p | t_{i-1},\ p \nmid t_i\}.$$

Firstly choose u_{k-r-1}. If $p_1 \in S_{k-r-1}$ and $p_1 | t_{k-r}$ we require that

$$u_{k-r-1} \not\equiv 0 \ (\text{mod } p_1).$$

If $p_2 \in S_{k-r-1}$ and $p_2 \nmid t_{k-r}$ we require that

$$u_{k-r-1}t_{k-r-1}+t_{k-r} \not\equiv 0 \pmod{p_2}.$$

By the Chinese Remainder Theorem and the definition of Jacobsthal's function we can find an integer u_{k-r-1} to satisfy these conditiosn such that

$$|u_{k-r-1}| \leqslant \tfrac{1}{2} g\Big(\prod p_1 \prod p_2\Big),$$

where the products are taken over all primes with the appropriate properties. It follows from (26) that for any given $\varepsilon > 0$

$$|u_{k-r-1}| \leqslant c(\varepsilon)\Big(\prod p_1 \prod p_2\Big)^{\varepsilon} \leqslant c(\varepsilon)\tau_{k-r-2}^{\varepsilon},$$

where the last inequality follows from (20) and the definition of S_{k-r-1}.

In general having chosen u_{i+1} we choose u_i as follows. If $p_1 \in S_i$ and $p_1 | (u_{i+1}t_{i+1}+\ldots+u_{k-r-1}t_{k-r-1}+t_{k-r})$ we require that

$$u_i \not\equiv 0 \pmod{p_1}.$$

If $p_2 \in S_i$ and $p_2 \nmid (u_{i+1}t_{i+1}+\ldots+u_{k-r-1}t_{k-r-1}+t_{k-r})$ we require that

$$u_i t_i + (u_{i+1}t_{i+1}+\ldots+u_{k-r-1}t_{k-r-1}+t_{k-r}) \not\equiv 0 \pmod{p_2}.$$

As before we can choose u_i to satisfy these conditions and also

$$|u_i| \leqslant c(\varepsilon)\Big(\prod p_1 \prod p_2\Big)^{\varepsilon} \leqslant c(\varepsilon)\tau_{i-1}^{\varepsilon}$$

provided $i \geqslant 2$. For $i = 1$ we follow the same procedure except that then the primes to be considered are in S_1 and so the final bound on u_1 is

$$|u_1| \leqslant c(\varepsilon)\Big(\prod p_1 \prod p_2\Big)^{\varepsilon} \leqslant c(\varepsilon) q^{\varepsilon}.$$

This choice procedure is to be used for $0 \leqslant r \leqslant k-2$ and for these choices of the u_i the t given by (31) has $(t, q) = 1$. If $r = k-1$ we have from (32) $\tau_1 = (t_1, q) = 1$ and so in this case we simply take $u_1 = 1$ and $\boldsymbol{x} = \boldsymbol{x}_1$.

From (30) and the convexity of F we have

(33) $$F(\boldsymbol{x}) \leqslant |u_1| F(\boldsymbol{x}_1)+\ldots+|u_{k-r-1}| F(\boldsymbol{x}_{k-r-1})+F(\boldsymbol{x}_{k-r}).$$

From (10) and the right-hand inequality in (11) we have

$$\lambda_1 \leqslant 2\big(V_F^{-1} d(\Lambda)\big)^{1/k}$$

which by (1) gives

(34) $$\lambda_1 \leqslant 2(V_F q)^{-1/k}.$$

Also because $\dim W_D^* = r$ we have

$$\mu_j \geqslant D \quad \text{for} \quad j \geqslant r+1 \quad (0 \leqslant r \leqslant k-1).$$

Hence by the right-hand inequality in (12)

(35) $$\lambda_i \leqslant k!\,D^{-1} \quad (1 \leqslant i \leqslant k-r).$$

Applying (17), (34) and (35) with $i = 1$ to (33) and using the bounds for the $|u_i|$ $(1 \leqslant i \leqslant k-r-1)$ we have in the case $0 \leqslant r \leqslant k-2$

(36) $F(\boldsymbol{x})$

$$\leqslant c(k, \varepsilon)\big(q^{\varepsilon}\min\{2(V_F q)^{-1/k}, k!\,D^{-1}\}+\tau_1^{\varepsilon}\lambda_2+\ldots+\tau_{k-r-2}^{\varepsilon}\lambda_{k-r-1}\big)+c(k)\lambda_{k-r}.$$

To estimate the terms $\tau_i^{\varepsilon}\lambda_{i+1}$ we write

$$\tau_i^{\varepsilon}\lambda_{i+1} \leqslant \big(c(k)\mu_1\mu_2\ldots\mu_{k-i}\big)^{\varepsilon}\lambda_{i+1}$$

by (23). Thus

$$\tau_i^{\varepsilon}\lambda_{i+1} \leqslant c(k, \varepsilon)\lambda_{i+1}/(\lambda_k\lambda_{k-1}\ldots\lambda_{i+1})^{\varepsilon}$$

by the right-hand inequality in (12). Now since $\lambda_k \geqslant \lambda_{k-1} \geqslant \ldots \geqslant \lambda_{i+1}$ we have

$$\tau_i^{\varepsilon}\lambda_{i+1} \leqslant c(k, \varepsilon)\lambda_{i+1}^{1-(k-i)\varepsilon}$$

for $1 \leqslant i \leqslant k-r-2$. Hence by (35) with $2 \leqslant i \leqslant k-r$, (36) and the remark that $V_F^{-1} \leqslant c(k)$ made earlier we have

$$F(\boldsymbol{x}) \leqslant c(k, \varepsilon) D^{-1+\varepsilon} \quad (\varepsilon_{\text{new}} = (k-1)\varepsilon_{\text{old}})$$

if $0 \leqslant r \leqslant k-3$. If $r = k-2$ we have

$$F(\boldsymbol{x}) \leqslant c(k, \varepsilon) q^{\varepsilon}\min\{2(V_F q)^{-1/k}, k!\,D^{-1}\}+c(k)D^{-1}.$$

Finally if $r = k-1$ so that $\boldsymbol{x} = \boldsymbol{x}_1$

$$F(\boldsymbol{x}) \leqslant c(k)\lambda_1 \leqslant c(k)\min\{2(V_F q)^{-1/k}, k!\,D^{-1}\}$$

which concludes the proof of the theorem.

As a final exercise in cyclic overlattices we shall prove

THEOREM 3. *Suppose that F^* satisfies condition C, $\Lambda_D^* \neq \mathsf{M}_D^*$ and that $\dim W_D^* = r$. Then $1 \leqslant r \leqslant k$ and there is a point $\boldsymbol{z}^* \in \Lambda_D^*$ which is primitive in Λ^* but not primitive in M^* such that*

(37) $$F^*(\boldsymbol{z}^*) \leqslant c(k) D^r.$$

Furthermore if $[\mathsf{M}^*:\Lambda^*] = q$ then $1 \leqslant r \leqslant k-1$ provided $q > c(k)D^k$.

Proof. Λ_D^* is spanned as a vector space by the vectors of $\mathscr{S}_D$ and so has a basis $\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_r^*$ with

(38) $$F(\boldsymbol{b}_j^*) \leqslant c(k) D \quad (1 \leqslant j \leqslant r).$$

Let Q be the index of Λ_D^* in M_D^*. Then the points of M_D^* are of the form

$$a_1\boldsymbol{b}_1^*+\ldots+a_r\boldsymbol{b}_r^*$$

where $(a_1, \ldots, a_r)$ runs through a lattice of determinant Q^{-1}. Hence by Minkowski's "first" theorem we can find a point $(a_1, \ldots, a_r)$ of this lattice, other than the origin, for which

$$|a_j| \leqslant 2Q^{-1/r} \quad (1 \leqslant j \leqslant r). \tag{39}$$

If

$$\boldsymbol{w}^* = a_1 \boldsymbol{b}_1^* + \ldots + a_r \boldsymbol{b}_r^*$$

we have

$$F^*(\boldsymbol{w}^*) \leqslant |a_1| F^*(\boldsymbol{b}_1^*) + \ldots + |a_r| F^*(\boldsymbol{b}_r^*) \leqslant c(k) D Q^{-1/r}$$

by (38) and (39). But $F^*(\boldsymbol{w}^*) \geqslant 1$ by condition C, and so

$$Q \leqslant c(k) D^r. \tag{40}$$

We may suppose $\boldsymbol{w}^*$ is primitive in M_D^* and furthermore $\boldsymbol{w}^* \notin \Lambda_D^*$ since the $\boldsymbol{b}_j^*$ span Λ_D^* and the a_j are clearly not all integers. Let s be the least positive integer such that $s\boldsymbol{w}^* \in \Lambda_D^*$. Then $s | Q$. Put $\boldsymbol{z}^* = s\boldsymbol{w}^*$. Then

$$F^*(\boldsymbol{z}^*) = sF^*(\boldsymbol{w}^*) \leqslant QF^*(\boldsymbol{w}^*) \leqslant c(k) Q^{1-1/r} D \leqslant c(k) D^r$$

as required.

To obtain the last assertion of the enunciation we observe that if $r = k$ then $\Lambda_D^* = \Lambda$ and $\mathsf{M}_D^* = \mathsf{M}$ so that

$$Q = [\mathsf{M}_D^* : \Lambda_D^*] = [\mathsf{M}^* : \Lambda^*] = q.$$

In which case we have a contradiction to (40) if $q > c(k) D^k$.

References

[1] J. W. S. Cassels, *Introduction to the Geometry of Numbers*, Springer-Verlag, 1959.

[2] H. Davenport and A. Schinzel, *Diophantine approximation and sums of roots of unity*, Math. Ann. 169 (1967), pp. 118–135.

[3] A. J. Jones, *Sums of three roots of unity*, Proc. Camb. Phil. Soc. 64 (1968), pp. 673–682.

[4] — *Sums of three roots of unity II*, Proc. Camb. Phil. Soc. 66 (1969), pp. 43–59.

[5] R. M. Robinson, *Some conjectures about cyclotomic integers*, Math. Comp. 19 (1965), pp. 210–217.

TRINITY COLLEGE
Cambridge, England

Received on 28. 10. 1969