ON GENERATING POINTS OF A LATTICE IN THE REGION
$| x_1^2 + x_2^2 - x_3^2 | \leqq 1$

by D. M. E. FOSTER

(Received 23 April, 1963)

1. A lattice Λ_n in n-dimensional Euclidean space E_n consists of the aggregate of all points with coordinates $(x_1, \ldots, x_n)$, where

$$x_r = \sum_{s=1}^{n} \alpha_{rs} u_s \quad (r = 1, \ldots, n), \quad u_1, \ldots, u_n = 0, \pm 1, \pm 2, \ldots,$$

for some real α_{rs} $(r, s = 1, \ldots, n)$, subject to the condition $\| \alpha_{rs} \|_{nn} \neq 0$. The determinant Δ_n of Λ_n is defined by the relation $\Delta_n = \pm \| \alpha_{rs} \|_{nn}$, the sign being chosen to ensure that $\Delta_n > 0$. If $A_1, \ldots, A_n$ are the n points of Λ_n having coordinates $(\alpha_{11}, \alpha_{21}, \ldots, \alpha_{n1}), \ldots, (\alpha_{1n}, \alpha_{2n}, \ldots, \alpha_{nn})$, respectively, then every point of Λ_n may be expressed in the form

$$u_1 A_1 + \ldots + u_n A_n,$$

and $A_1, \ldots, A_n$, together with the origin O, are said to generate Λ_n. This particular set of generating points is not unique; it may be proved that a necessary and sufficient condition that n points of Λ_n should generate the lattice is that the $n \times n$ determinant formed by their x-coordinates should be $\pm \Delta_n$, or, equivalently, that the $n \times n$ determinant formed by their corresponding u-coordinates should be ± 1.

The problem of finding infinite regions in E_n which contain the origin and n further generating points of Λ_n has already been considered by Minkowski. In particular, Minkowski [13] proved by simple geometrical arguments that the region

$$| x_1 x_2 | \leqq \tfrac{1}{2} \Delta_2$$

always contains two generating points of Λ_2. Chalk [3] obtained a generalisation of this result, and later suggested the following conjecture [4] which he proved for $n = 3$ and 4.

CONJECTURE. *There exist n lattice points generating Λ_n in the region*

$$| x_1 x_2 \ldots x_n | \leqq \frac{1}{2^{n-1}} \Delta_n .$$

Clearly the conjectured inequality, if true for general n, would be best possible when the lattice Λ_n is of the form

$$x_i = u_i + \tfrac{1}{2} u_n \quad (i = 1, \ldots, n-1), \quad x_n = u_n.$$

Further results of a slightly different nature concerning generating points of E_2 and E_3 have also been obtained by Chalk and Rogers [6], Barnes [1] and Oppenheim [15].

Our object is to prove the following two theorems, which yield information about sets of generating points of Λ_3 in the three dimensional region

$$|x_1^2+x_2^2-x_3^2| \leqq 1.$$

THEOREM 1. *If Λ_3 has a point, other than the origin, on the surface $x_1^2+x_2^2-x_3^2=0$, then the region*

$$|x_1^2+x_2^2-x_3^2| \leqq \Delta_3^{2/3} \tag{1}$$

contains a set of generating points of Λ_3.

THEOREM 2. *If Λ_3 has no point, other than the origin, on the surface $x_1^2+x_2^2-x_3^2=0$, then the region*

$$|x_1^2+x_2^2-x_3^2| \leqq \left(\frac{27}{25}\Delta_3^2\right)^{1/3} \tag{2}$$

contains a set of generating points of Λ_3.

We shall show that the inequalities (1) and (2) are best possible. Before doing so, however, it is convenient to restate Theorems 1 and 2 in terms of indefinite quadratic forms in three variables. For, if Λ_3 is given by equations of the form

$$x_r = \sum_{s=1}^{3} \alpha_{rs} u_s \quad (r = 1, 2, 3),$$

where $\Delta_3 = \pm \| \alpha_{rs} \|_{33}$, then clearly $x_1^2+x_2^2-x_3^2$ may be expressed as an indefinite quadratic form

$$q(u_1, u_2, u_3) = \sum_{r=1}^{3} \sum_{s=1}^{3} a_{rs} u_r u_s \quad (a_{rs} = a_{sr})$$

for appropriate a_{rs} $(r, s = 1, 2, 3)$, with determinant $D_3 = \| a_{rs} \|_{33}$. On comparison of determinants we see that

$$D_3 = -\Delta_3^2 < 0.$$

Two quadratic forms $q(u_1, \ldots, u_n)$, $Q(U_1, \ldots, U_n)$ are said to be equivalent, and we write $q \sim Q$, if q can be transformed into Q by an integral unimodular substitution of the form

$$u_r = \sum_{s=1}^{n} p_{rs} U_s \quad (r = 1, \ldots, n),$$

where the p_{rs} are integers with determinant $\| p_{rs} \| = \pm 1$. The following Theorems 1* and 2*, which are expressed in terms of quadratic forms, contain the assertions of Theorems 1 and 2, respectively, and we prove them in this form.

THEOREM 1*. *If $q(u_1, u_2, u_3)$ represents zero non-trivially, then it is equivalent to a form for which*

$$|a_{ii}| \leqq |D_3|^{1/3} \quad (i = 1, 2, 3), \tag{1*}$$

with strict inequality unless $q \sim \lambda q_0$ or λq_1, where

$$q_0(u_1, u_2, u_3) = 2u_1u_2+u_3^2$$

and

$$q_1(u_1, u_2, u_3) = 2u_1u_2+u_2^2+u_2u_3+u_3^2.$$

THEOREM 2*. *If $q(u_1, u_2, u_3)$ does not represent zero non-trivially, then it is equivalent to a form for which*

$$|a_{ii}| \leqq \left(\frac{27}{25}|D_3|\right)^{1/3} \quad (i = 1, 2, 3), \tag{2*}$$

with strict inequality unless $q \sim \lambda q_2$, where

$$q_2(u_1, u_2, u_3) = u_1^2+u_1u_2-u_2^2+\tfrac{5}{2}u_3^2.$$

In a recent paper [5], Dr J. H. H. Chalk has obtained a striking result for a certain class of quadratic forms in an even number of variables. He has shown that if

$$q(u_1, \ldots, u_{2m}) = \sum_{r=1}^{2m} \sum_{s=1}^{2m} a_{rs}u_ru_s \quad (a_{rs} = a_{sr})$$

is an indefinite form in $u_1, \ldots, u_{2m}$ of signature zero and determinant $D_{2m} = \| a_{rs} \|_{2m,\,2m} \neq 0$, then it is equivalent to a form for which

$$|a_{ii}| \leqq |D_{2m}|^{1/2m} \quad (i = 1, \ldots, 2m),$$

with equality when

$$q(u_1, \ldots, u_{2m}) = \sum_{r=1}^{m-1} (u_{2r-1}^2 - u_{2r}^2) + 2u_{2m-1}u_{2m}.$$

The proof of Theorem 1* in §2 divides into two cases, in one of which we use an elementary result in the theory of continued fractions (Lemma 1) to replace the inequalities (1)* by

$$|a_{ii}| < \varepsilon \quad (i = 1, 2, 3)$$

for any $\varepsilon > 0$. The other case is less trivial and the proof depends upon Lemma 2, which gives a useful inequality for a quadratic in a single integral variable. The lemma is not new and is a corollary of Lemma 5 of Davenport [7], but a proof is given for convenience. The use of this lemma could be avoided by a direct appeal to a theorem of Macbeath [11] on a quadratic polynomial in two variables.

The proof of Theorem 2* is rather different and is based upon Lemma 2 and three further lemmas. Lemma 3, which is needed as a starting point for the proof of the theorem, is classical and gives the first " minimum " for an indefinite quadratic form in three variables. Lemma 4

https://doi.org/10.1017/S2040618500034912 Published online by Cambridge University Press

is a straightforward extension, to a two-dimensional asymmetric hyperbolic region, of Minkowski's original theorem on generating points of Λ_2. The result stated in Lemma 5 is a special case of a recent theorem of Watson on values of a non-zero binary quadratic form.

I am very grateful to Dr J. H. H. Chalk for suggesting this problem to me and for his valuable help and advice during my work on it. I should also like to thank Dr G. L. Watson for his helpful suggestions in improving the presentation.

2. For the proof of Theorem 1* we require the following two lemmas.

LEMMA 1. *If α is a given positive irrational number and $\varepsilon > 0$, then the inequalities*

$$0 < | q_n\alpha - p_n | < \varepsilon \quad \textit{and} \quad 0 < | q_{n+1}\alpha - p_{n+1} | < \varepsilon$$

are always soluble in integer pairs (p_n, q_n) and (p_{n+1}, q_{n+1}) with $p_n q_{n+1} - p_{n+1} q_n = 1$.

Proof. Take p_n/q_n and p_{n+1}/q_{n+1} to be successive convergents to the continued fraction for α with n odd and sufficiently large.

LEMMA 2. *If a, α, t are any constants satisfying*

$$0 < a < 1, \tag{3}$$

$$0 \leqq t^2 < 1 + \tfrac{1}{4}a^2, \tag{4}$$

then the inequalities

$$| a(u+\alpha)^2 - a^{-1}t^2 | < 1 \tag{5}$$

are always soluble for an integer u.

Proof. We write

$$f(u) = a(u+\alpha)^2 - a^{-1}t^2$$

for convenience. If $t^2 < a$, we choose an integer u satisfying

$$| u+\alpha | < a^{-1}(t^2+a)^{1/2},$$

which is possible since

$$a^{-1}(t^2+a)^{1/2} > a^{-1/2} > 1,$$

by (3) and (4). With this value of u we have

$$-1 < -a^{-1}t^2 < f(u) < 1.$$

If $t^2 \geqq a$, let u denote the integer for which

$$a^{-1}(t^2+a)^{1/2} - 1 \leqq u+\alpha < a^{-1}(t^2+a)^{1/2}. \tag{6}$$

We have, successively,

$$\begin{aligned} t^2 &< 1+\tfrac{1}{4}a^2, \\ 4(t^4-a^2) &< 4t^4-4t^2a^2+a^4, \\ 2(t^4-a^2)^{1/2} &< 2t^2-a^2, \\ a^2 &< 2t^2-2(t^4-a^2)^{1/2}, \\ 1 &< a^{-1}(t^2+a)^{1/2}-a^{-1}(t^2-a)^{1/2}. \end{aligned} \tag{7}$$

By (6) and (7) we see that u satisfies

$$a^{-1}(t^2-a)^{1/2} < u+\alpha < a^{-1}(t^2+a)^{1/2},$$

and (5) now follows.

Proof of Theorem 1*. By considering a positive multiple of $q = q(u_1, u_2, u_3)$ in place of q, if necessary, we may assume that $|D_3| = 1$. Then it suffices to prove that, unless $q \sim \lambda q_0$ or λq_1, the inequalities

$$|q(u_{1s}, u_{2s}, u_{3s})| < 1 \quad (s = 1, 2, 3) \tag{8}$$

are soluble in integers (u_{1s}, u_{2s}, u_{3s}), with $\| u_{rs} \|_{33} = 1$, since the integral unimodular substitution

$$u_r = \sum_{s=1}^{3} u_{rs} U_s \quad (r = 1, 2, 3)$$

will transform q into a form each of whose diagonal coefficients is less than 1 in absolute value.

As q represents zero non-trivially, we may suppose, after applying an integral unimodular substitution to the variables, that $a_{11} = 0$, and q now takes the form

$$q(u_1, u_2, u_3) = 2(a_{12}u_2+a_{13}u_3)u_1+a_{22}u_2^2+2a_{23}u_2u_3+a_{33}u_3^2.$$

Since $|D_3| \neq 0$, the coefficients a_{12}, a_{13} cannot both be zero. By interchanging u_2, u_3, if necessary, we may suppose that $a_{12} \neq 0$. Two cases now arise, according as the ratio a_{13}/a_{12} is irrational or rational.

Suppose first that a_{13}/a_{12} is irrational and let $\varepsilon > 0$. By changing the signs of u_2, u_3, if necessary, we may assume that $a_{12} > 0$, $a_{13} < 0$.

Choose $(u_{11}, u_{21}, u_{31}) = (1, 0, 0)$. By Lemma 1, since $(\varepsilon/a_{12}) > 0$, there exist integer pairs (u_{22}, u_{32}) and (u_{23}, u_{33}), with $u_{22}u_{33}-u_{23}u_{32} = 1$, satisfying

$$0 < \left| u_{2s}+\frac{a_{13}}{a_{12}}u_{3s} \right| < \frac{\varepsilon}{a_{12}} \quad (s = 2, 3).$$

For each pair (u_{2s}, u_{3s}) $(s = 2, 3)$, we can always choose a corresponding integer $u_1 = u_{1s}$ $(s = 2, 3)$ satisfying

$$|q(u_{1s}, u_{2s}, u_{3s})| \leqq \varepsilon,$$

https://doi.org/10.1017/S2040618500034912 Published online by Cambridge University Press

and (8) follows with the triads $(1, 0, 0)$, (u_{12}, u_{22}, u_{32}) and (u_{13}, u_{23}, u_{33}), since ε may be arbitrarily small.

Now suppose that $a_{13}/a_{12} = q/p$ where p, q are integers with $(p, q) = 1$ and $q \neq 0$ (i.e. $a_{13} \neq 0$). It is known that there exist integers p', q', with $(p', q') = 1$, satisfying $pq' - p'q = 1$. Then the integral unimodular substitution given by

$$u_1' = u_1, \quad u_2' = pu_2 + qu_3, \quad u_3' = p'u_2 + q'u_3$$

will reduce q to the form

$$q(u_1, u_2, u_3) = 2b_{12}u_1u_2 + b_{22}u_2^2 + 2b_{23}u_2u_3 + b_{33}u_3^2,$$

for appropriate $b_{12}, \ldots, b_{33}$. If $a_{13} = 0$, the above substitution is not required. Comparing determinants we see that

$$b_{12}^2 \mid b_{33} \mid = \mid D_3 \mid = 1. \tag{9}$$

If $\mid b_{12} \mid < 1$, the result is easily proved, by choosing the triads $(1, 0, 0)$, $(u_{12}, 1, 0)$ and $(u_{13}, 1, 1)$, where u_{12}, u_{13} are the integers satisfying

$$\mid 2b_{12}u_{12} + b_{22} \mid \leqq \mid b_{12} \mid < 1$$

and

$$\mid 2b_{12}u_{13} + b_{22} + 2b_{23} + b_{33} \mid \leqq \mid b_{12} \mid < 1.$$

Now suppose that $\mid b_{12} \mid > 1$ and hence $\mid b_{33} \mid < 1$, by (9). We first choose the triads $(1, 0, 0)$ and $(0, 0, -1)$. Then taking $u_2 = u_{23} = 1$, we have, on re-arranging,

$$q(u_1, 1, u_3) = b_{33}\left(u_3 + \frac{b_{23}}{b_{33}}\right)^2 + 2b_{12}u_1 + b_{22} - \frac{b_{23}^2}{b_{33}}.$$

By considering $-q\,(u_1, 1, u_3)$, if necessary, we may suppose that

$$0 < b_{33} < 1. \tag{10}$$

Let $u_1 = u_{13}$ be the integer satisfying

$$1 - \tfrac{1}{4}b_{33} - 2b_{12} \leqq 2b_{12}u_{13} + b_{22} - \frac{b_{23}^2}{b_{33}} < 1 - \tfrac{1}{4}b_{33}.$$

If

$$0 \leqq 2b_{12}u_{13} + b_{22} - \frac{b_{23}^2}{b_{33}} < 1 - \tfrac{1}{4}b_{33},$$

we choose an integer $u_3 = u_{33}$ satisfying

$$\left| u_{33} + \frac{b_{23}}{b_{33}} \right| \leqq \tfrac{1}{2},$$

and then (8) follows. Thus we are left to consider the case in which

$$q(u_{13}, 1, u_3) = b_{33}\left(u_3 + \frac{b_{23}}{b_{33}}\right)^2 - \lambda,$$

https://doi.org/10.1017/S2040618500034912 Published online by Cambridge University Press

where

$$0 < b_{33}\lambda \leqq \tfrac{1}{4}b_{33}^2 - b_{33} + 2b_{33}^{1/2},$$

and hence, since $0 < b_{33} < 1$, we have

$$0 < b_{33}\lambda < \tfrac{1}{4}b_{33}^2 + 1.$$

By Lemma 2, with $a = b_{33}$, $\alpha = b_{23}/b_{33}$, $t^2 = b_{33}\lambda$, it follows that there is an integer $u_3 = u_{33}$ satisfying

$$| q(u_{13}, 1, u_{33}) | < 1.$$

It remains to consider the case in which $| b_{12} | = 1$, $| b_{33} | = 1$. By changing, if necessary, the sign of q or the sign of u_1 or both we may suppose that

$$q(u_1, u_2, u_3) = 2u_1u_2 + b_{22}u_2^2 + 2b_{23}u_2u_3 + u_3^2.$$

Further, by absorbing integral multiples of u_2, u_3 into u_1 and changing the sign of u_3, if necessary, we may suppose that

$$| b_{22} | \leqq 1 \quad \text{and} \quad 0 \leqq 2b_{23} \leqq 1.$$

If $| b_{22} | < 1$, the congruences

$$b_{22} \pm 2b_{23} \equiv 0 \pmod 2$$

together imply that $b_{22} = b_{23} = 0$. Thus if u_{13}, u'_{13} are integers satisfying

$$| 2u_{13} + b_{22} + 2b_{23} + 1 | \leqq 1$$

and

$$| 2u'_{13} - b_{22} + 2b_{23} - 1 | \leqq 1,$$

respectively, then it follows that $| q | < 1$ for the triads $(1, 0, 0)$, $(0, 1, 0)$ and $(u_{13}, 1, 1)$ or $(u'_{13}, -1, 1)$, unless

$$q = q_0 = 2u_1u_2 + u_3^2.$$

If $| b_{22} | = 1$, then q is equivalent to the form

$$q(u_1, u_2, u_3) = 2u_1u_2 + u_2^2 + 2b_{23}u_2u_3 + u_3^2.$$

Let u_{13} be an integer satisfying

$$| u_{13} + b_{23} - 1 | \leqq \tfrac{1}{2}.$$

Then $| q | < 1$ for the triads $(1, 0, 0)$, $(-1, 2, -1)$ and $(u_{13}, -1, 1)$, unless $2b_{23} = 1$, in which case

$$q = q_1 = 2u_1u_2 + u_2^2 + u_2u_3 + u_3^2.$$

3. In this section we prove Theorem 2*. The proof is independent of Theorem 1* and use is made of the following three lemmas.

LEMMA 3. *The inequalities*

$$|\, q(u_1, u_2, u_3) \,| \leqq (\tfrac{2}{3} \,|\, D_3 \,|)^{1/3}$$

are always soluble in integers $(u_1, u_2, u_3) \neq (0, 0, 0)$.

For a proof of this classical result, which is the first of a sequence of minima of an indefinite quadratic form in three variables, see [10]. We observe, in passing, that the particular form relating to the fourth minimum arises as the critical form $q_2(u_1, u_2, u_3)$ in Theorem 2*.

LEMMA 4. *For any* $\Gamma > 0$, *the region*

$$-\Gamma\Delta_2 \leqq x_1 x_2 \leqq \frac{1}{4\Gamma}\Delta_2$$

always contains two generating points of Λ_2.

Proof. Consider the tangent parallelogram Π_t defined by

$$|\, t^{-1}x_1 + t x_2 \,| \leqq \sqrt{(\Delta_2/\Gamma)}, \quad |\, t^{-1}x_1 - t x_2 \,| \leqq 2\sqrt{(\Gamma\Delta_2)}.$$

Clearly Π_t is symmetrical about the origin, and since it may be transformed by a linear substitution of determinant 2 into a rectangle having area $8\Delta_2$, its area is $4\Delta_2$. By Minkowski's fundamental theorem, Π_t contains a point of Λ_2 other than the origin O. Further, by varying t continuously, we can obtain a parallelogram $\Pi_{t'}$, which contains two *independent* points P, Q, say, of Λ_2, other than O. Let P', Q' be the reflections of P, Q respectively in O. If the parallelogram $PQP'Q'$ contains points of Λ_2 other than O, we simply replace it by a smaller parallelogram. Thus we assume that $PQP'Q'$ does not contain any point of Λ_2 other than O.

Since P, Q are lattice points, it follows that the area of the parallelogram with sides OP, OQ is an integral multiple of Δ_2, say $m\Delta_2$. The area of the parallelogram $PQP'Q'$ is $2m\Delta_2$, and $2m\Delta_2 \leqq 4\Delta_2$; consequently two possibilities arise according as $m = 1$ or 2. If $m = 1$, the parallelogram with sides OP, OQ has area Δ_2, and hence P, Q, together with O, generate Λ_2. If $m = 2$, the parallelogram $PQP'Q'$ coincides with the original tangent parallelogram Π_t, and Q and $\frac{1}{2}(P+Q)$, together with O, generate Λ_2.

We observe that the two generating points obtained lie entirely *inside* the region considered if there is no point of Λ_2 on either bounding hyperbola. However, if there is a point of Λ_2 on one of these hyperbolae, the tangent parallelogram Π_t, for suitable t, through that point will have on its boundary two basis points lying inside the region, unless there is a primitive point of Λ_2 on the other hyperbola. In this case Λ_2 is of the form

$$x_1 = \frac{t}{2}\sqrt{\left(\frac{\Delta_2}{\Gamma}\right)}u_1 - t\sqrt{(\Gamma\Delta_2)}u_2,$$

$$x_2 = \frac{1}{2t}\sqrt{\left(\frac{\Delta_2}{\Gamma}\right)}u_1 + t^{-1}\sqrt{(\Gamma\Delta_2)}u_2.$$

Restating the result with $\mu = 1/(2\Gamma)$, we obtain the following corollary.

Corollary. *If $\mu > 0$ and if $q(u_1, u_2) = (\alpha u_1 + \beta u_2)(\gamma u_1 + \delta u_2)$ is an indefinite quadratic form in u_1, u_2 of determinant $d = -\frac{1}{4}(\alpha\delta - \beta\gamma)^2$, then the inequalities*

$$-\frac{1}{\mu} \mid d \mid^{1/2} < q(u_{1s}, u_{2s}) < \mu \mid d \mid^{1/2} \quad (s = 1, 2)$$

are always soluble in integers (u_{1s}, u_{2s}) $(s = 1, 2)$ with $\| u_{rs} \| = 1$, unless

$$q(u_1, u_2) \sim \sqrt{(\mid d \mid)}(\mu u_1^2 - \mu^{-1} u_2^2).$$

A proof of the next lemma, due to Watson, is given for convenience as his has not been published. Let

$$q = q(u_1, u_2) = au_1^2 + 2bu_1u_2 + cu_2^2$$

denote an indefinite quadratic form in u_1, u_2 which does not represent zero non-trivially and has determinant

$$d = ac - b^2 < 0.$$

Denote by P, N the lower bounds of the positive values of q, $-q$, respectively, for all integers $(u_1, u_2) \neq (0, 0)$.

Lemma 5.

$$PN \leqq \tfrac{4}{5} \mid d \mid,$$

with equality when

$$q(u_1, u_2) = \lambda(u_1^2 + u_1u_2 - u_2^2).$$

Proof.† We suppose $PN \neq 0$, for otherwise the result is obvious. Also if $P = N$ the result is well known [12], since

$$P = N \leqq \sqrt{(\tfrac{4}{5} \mid d \mid)}.$$

By changing the sign of q, if necessary, we may suppose that

$$N < P.$$

Hence

$$N \leqq \sqrt{(\tfrac{4}{5} \mid d \mid)}. \tag{11}$$

If we consider a suitable multiple of q instead of q, we may take $P = 1$, and it now suffices to prove that

$$N \leqq \tfrac{4}{5} \mid d \mid. \tag{12}$$

Let $\varepsilon > 0$. After applying an appropriate unimodular substitution to the variables u_1, u_2, we may assume that

$$1 \leqq a < 1 + \varepsilon, \quad \tfrac{1}{2}a \leqq b \leqq a. \tag{13}$$

† The proof given here is an adaptation of that of Dr Watson, who has very kindly let me reproduce it.

L

By our hypothesis concerning P and N, it follows that either $q \leqq -N$ or $q \geqq 1$ for all integers $(u_1, u_2) \neq (0, 0)$.

The inequality (12) follows easily if $|d| \geqq \frac{5}{4}$. For in this case we have

$$N \leqq \sqrt{(\tfrac{4}{5}|d|)} \leqq \tfrac{4}{5}|d|,$$

by (11). Thus suppose now that

$$|d| < \tfrac{5}{4}. \tag{14}$$

Since

$$ac - b^2 = d < 0$$

we have

$$ac < b^2 \leqq a^2,$$

by (13), and hence

$$c < a. \tag{15}$$

Thus either (i) $1 \leqq c < 1+\varepsilon$, or (ii) $c < 0$.

In the first case

$$q(-1, 1) = a - 2b + c,$$

and by (13), (15) and the choice of c, we have

$$1 - 2(1+\varepsilon) + 1 < q(-1, 1) < 1 + \varepsilon - 2 + 1 + \varepsilon,$$

since, using (13), $b \geqq \frac{1}{2}a > 0$ and $(1+\varepsilon)^2 > b^2 > ac \geqq 1$. Thus

$$-2\varepsilon < q(-1, 1) < 2\varepsilon,$$

which is impossible if ε is sufficiently small. Hence only the second case can arise, and we have therefore

$$c \leqq -N. \tag{16}$$

Now

$$|d| = a|c| + b^2 \geqq aN + \tfrac{1}{4}a^2, \quad \text{by (16)},$$
$$\geqq N + \tfrac{1}{4}, \quad \text{by (13)},$$

so that

$$N \leqq |d| - \tfrac{1}{4}$$
$$< \tfrac{4}{5}|d|, \quad \text{by (14)}.$$

Proof of Theorem 2*. By considering a suitable positive multiple of $q = q\ (u_1, u_2, u_3)$ in place of q, if necessary, we can take $D_3 = -25/27$. Then, as in the proof of Theorem 1*, it suffices to prove that, unless $q \sim \lambda q_2$, the inequalities

$$|q(u_{1s}, u_{2s}, u_{3s})| < 1 \quad (s = 1, 2, 3) \tag{17}$$

are always soluble in integers (u_{1s}, u_{2s}, u_{3s}) $(s = 1, 2, 3)$, with $\|u_{rs}\|_{33} = 1$.

https://doi.org/10.1017/S2040618500034912 Published online by Cambridge University Press

If M denotes the lower bound of $|q(u_1, u_2, u_3)|$ over all integer triads $(u_1, u_2, u_3) \neq (0, 0, 0)$, then, by a weaker form of Lemma 3, we have

$$0 \leqq M < 9/10.$$

Suppose first that $M = 0$. Then, for any $\varepsilon > 0$, the inequalities

$$0 < |q(u_1, u_2, u_3)| < \varepsilon$$

are always soluble in integers u_1, u_2, u_3, and it follows that the inequalities

$$0 < q(u_1, u_2, u_3) < \varepsilon$$

are also soluble for any $\varepsilon > 0$, by a theorem of Oppenheim [**14**].

Now suppose that $M \neq 0$, and choose ε so that

$$0 \leqq \varepsilon < 1/81.$$

By the definition of M, there are coprime integers u_1, u_2, u_3 satisfying

$$0 < M \leqq |q| < M/(1-\varepsilon) < 1.$$

Thus, if the inequalities $0 < q < 1$ are insoluble in integers u_1, u_2, u_3, then the inequalities $0 < -q < 1$ are soluble in integers u_1, u_2, u_3.

In either case, therefore, after applying a suitable unimodular substitution to the variables u_1, u_2, u_3, we may ensure that either

$$\text{(i) } 0 < a_{11} < 1$$

or

$$\text{(ii) } 0 < -a_{11} < M/(1-\varepsilon) < 1,$$

and in case (ii) the inequalities $0 < q < 1$ are insoluble in integers u_1, u_2, u_3.

Case (i). We may write

$$q(u_1, u_2, u_3) = a_{11}(u_1 + c_2u_2 + c_3u_3)^2 + q_1(u_2, u_3),$$

for suitable constants c_2, c_3 and $q_1(u_2, u_3)$, which is an indefinite quadratic form in u_2, u_3 of determinant $-25/(27a_{11})$. By the corollary to Lemma 4, with $\mu = \{(4-a_{11})(27a_{11})^{\frac{1}{2}}\}/20$, there exist integer pairs (u_{22}, u_{32}) and (u_{23}, u_{33}), with $u_{22}u_{33} - u_{23}u_{32} = 1$, satisfying

$$-\frac{100}{(4-a_{11})27a_{11}} < q_1(u_{2s}, u_{3s}) < \frac{4-a_{11}}{4} \quad (s = 2, 3), \tag{18}$$

unless

$$q_1(u_2, u_3) \sim (\mu u_2^2 - \mu^{-1}u_3^2)\{25/(27a_{11})\}^{\frac{1}{2}}.$$

If

$$0 \leqq q_1(u_{2s}, u_{3s}) < \frac{4-a_{11}}{4}$$

for some $s = 2, 3$, we choose an integer u_{1s} satisfying

$$|u_{1s}+c_2u_{2s}+c_3u_{3s}| \leqq \tfrac{1}{2},$$

and then

$$|q(u_{1s}, u_{2s}, u_{3s})| < \tfrac{1}{4}a_{11}+\tfrac{1}{4}(4-a_{11}) = 1.$$

Now suppose that $q_1(u_{2s}, u_{3s}) = -\lambda$ for some $s = 2, 3$, where

$$0 < \lambda < 100/\{27a_{11}(4-a_{11})\}, \text{ by (18)},$$

i.e.

$$0 < a_{11}\lambda < 100/\{27(4-a_{11})\}.$$

In this case we have

$$q(u_1, u_{2s}, u_{3s}) = a_{11}(u_1+c_2u_{2s}+c_3u_{3s})^2-a_{11}^{-1}(a_{11}\lambda).$$

Since $0 < a_{11} < 1$, we have, successively,

$$(3a_{11}-2)^2(3a_{11}-8) \leqq 0,$$

$$27a_{11}^3-108a_{11}^2+108a_{11}-32 \leqq 0,$$

$$400-27(4-a_{11})(4+a_{11}^2) \leqq 0,$$

$$100/\{27(4-a_{11})\} \leqq (4+a_{11}^2)/4.$$

By Lemma 2, with $a = a_{11}$, $t^2 = a_{11}\lambda$, there is an integer u_{1s} satisfying

$$|q(u_{1s}, u_{2s}, u_{3s})| < 1.$$

Thus the inequalities (17) follow, with the triads $(1, 0, 0)$, (u_{12}, u_{22}, u_{32}) and (u_{13}, u_{23}, u_{33}).

It remains to consider the case in which

$$q_1(u_2, u_3) = (\mu u_2^2-\mu^{-1}u_3^2)\{25/(27a_{11})\}^{\frac{1}{2}},$$

where $\mu = \{(4-a_{11})(27a_{11})^{\frac{1}{2}}\}/20$. If we choose $(u_{22}, u_{32}) = (0, -1)$ and $(u_{23}, u_{33}) = (1, 1)$, then

$$-\frac{100}{(4-a_{11})27a_{11}} \leqq q_1(u_{2s}, u_{3s}) < \frac{4-a_{11}}{4} \quad (s = 2, 3),$$

and (17) again follows, with the triads $(1, 0, 0)$, $(u_{12}, 0, -1)$ and $(u_{13}, 1, 1)$, unless $a_{11} = 2/3$. In this case $\mu = 1/\sqrt{2}$, and q is equivalent to

$$q(u_1, u_2, u_3) = \tfrac{2}{3}(u_1+c_2'u_2+c_3'u_3)^2+\tfrac{5}{6}(u_2^2-2u_3^2)$$

for some constants c_2', c_3'. By absorbing integral multiples of u_2, u_3 into u_1 and changing the sign of u_2, if necessary, we may assume that

$$0 \leqq c_2' \leqq \tfrac{1}{2} \quad \text{and} \quad 0 \leqq c_3' < 1.$$

We shall show that there are three triads of determinant 1 for which $|q| < 1$, unless $c_2' = \frac{1}{2}$ and $c_3' = 0$.

If $c_2' \neq \frac{1}{2}$ and $c_3' \neq 0$, we choose the triads (1, 0, 0), (0, 1, 0) and (1, 0, 1); if $c_2' = \frac{1}{2}$ and $c_3' \neq 0$, we choose the triads (1, 0, 0), (1, 1, −1) and (1, 0, 1); finally, if $c_2' \neq \frac{1}{2}$, $c_3' = 0$, we choose the triads (1, 0, 0), (1, 1, −1) and (0, 1, 0).

In the remaining case, when $(c_2', c_3') = (\frac{1}{2}, 0)$, the unimodular substitution

$$u_1 = U_1 + U_3, \quad u_2 = U_2 - 2U_3, \quad u_3 = U_2 - U_3$$

will transform q into the equivalent form $Q = Q(U_1, U_2, U_3)$, where

$$\tfrac{3}{2}Q(U_1, U_2, U_3) = U_1^2 + U_1U_2 - U_2^2 + \tfrac{5}{2}U_3^2.$$

It may be verified that $\frac{3}{2}Q$ does not represent zero, and that it has absolute minimum 1, attained only when $U_2 \equiv 0 \pmod 2$.

Before going on to the alternative case, we observe that, if $M = 0$, we can ensure that $0 < a_{11} < \varepsilon$, and a slight modification of the foregoing proof will yield a result of the type

$$| q(u_{1s}, u_{2s}, u_{3s}) | < \varepsilon \quad (s = 1, 2, 3)$$

with $\| u_{rs} \|_{33} = 1$.

Case (ii). In this case we write

$$q(u_1, u_2, u_3) = -| a_{11} | (u_1 + d_2u_2 + d_3u_3)^2 + q_2(u_2, u_3),$$

for suitable constants d_2, d_3 and $q_2(u_2, u_3)$, which is a positive definite quadratic form in u_2, u_3 of determinant $25/(27 | a_{11} |)$, and

$$0 < | a_{11} | < 1.$$

After applying an integral unimodular substitution to the variables u_2, u_3, it is known [8, Theorem 51] that we can ensure that

$$q_2(u_2, u_3) = Au_2^2 + 2Bu_2u_3 + Cu_3^2,$$

where

$$AC - B^2 = \frac{25}{27 | a_{11} |}, \quad | 2B | \leqq A \quad \text{and} \quad 0 < A \leqq \min\left\{C, \sqrt{\frac{4}{3} \cdot \frac{25}{27 | a_{11} |}} = \sqrt{\frac{100}{81 | a_{11} |}}\right\}. \tag{19}$$

We again choose $(u_{11}, u_{21}, u_{31}) = (1, 0, 0)$. We next choose $(u_{22}, u_{32}) = (1, 0)$, so that

$$-q(u_1, 1, 0) = | a_{11} | (u_1 + d_2')^2 - | a_{11} |^{-1}(| a_{11} | A)$$

for appropriate d_2', where

$$0 < | a_{11} | A < \sqrt{(\tfrac{5}{4} | a_{11} |)}, \quad \text{by (19)},$$
$$< \tfrac{5}{8} + \tfrac{1}{2} | a_{11} |,$$

by the inequality of the arithmetic and geometric means. Since $0 < | a_{11} | < 1$, we have

$$| a_{11} | (2 - | a_{11} |) < \tfrac{3}{2},$$

i.e.

$$\tfrac{5}{8} + \tfrac{1}{2} | a_{11} | < 1 + \tfrac{1}{4}a_{11}^2,$$

and hence
$$0 < | a_{11} | A < 1 + \tfrac{1}{4} a_{11}^2 .$$

By Lemma 2, with $a = | a_{11} |$, $t^2 = | a_{11} | A$, we can always choose an integer u_{12} satisfying
$$| q(u_{12}, 1, 0) | < 1.$$

Finally, we take $(u_{23}, u_{33}) = (0, 1)$, so that
$$-q(u_1, 0, 1) = | a_{11} | (u_1 + d_3')^2 - | a_{11} |^{-1} (| a_{11} | C),$$

for some constant d_3'. We now show, with the help of Lemma 5, that A cannot be too small, and then deduce that $| a_{11} | C$ is bounded above in terms of $| a_{11} |$.

Consider the quadratic section
$$q(u_1, u_2, 0) = -| a_{11} | (u_1 + d_2' u_2)^2 + A u_2^2$$

of $q(u_1, u_2, u_3)$. This is an indefinite quadratic form in u_1, u_2 of determinant $-| a_{11} | A$, which does not represent zero non-trivially. Thus if P, N denote the lower bounds of the positive values of $q(u_1, u_2, 0)$, $-q(u_1, u_2, 0)$, respectively, it follows, by Lemma 5, that
$$PN \leqq \tfrac{4}{5} | a_{11} | A. \tag{20}$$

By hypothesis,
$$P \geqq 1 \quad \text{and} \quad N \geqq M > | a_{11} | (1 - \varepsilon). \tag{21}$$

Thus by (20), (21) we have
$$| a_{11} | (1 - \varepsilon) < M \leqq N \leqq PN \leqq \tfrac{4}{5} | a_{11} | A,$$

and hence
$$A > \tfrac{5}{4} (1 - \varepsilon).$$

But since $| 2B | \leqq A \leqq C$, by (19), we have
$$\tfrac{3}{4} \cdot \tfrac{5}{4} (1 - \varepsilon) C < \tfrac{3}{4} AC \leqq AC - B^2 = \frac{25}{27 | a_{11} |},$$

which leads to
$$| a_{11} | C < \frac{80}{81 (1 - \varepsilon)} < 1 + \tfrac{1}{4} a_{11}^2 ,$$

since $\varepsilon < 1/81$. A final application of Lemma 5, with $a = | a_{11} |$ and $t^2 = | a_{11} | C$, shows that
$$| q(u_{13}, 0, 1) | < 1$$

for some integer u_{13}. The inequalities (17) now follow, with the triads $(1, 0, 0)$, $(u_{12}, 1, 0)$ and $(u_{13}, 0, 1)$.

https://doi.org/10.1017/S2040618500034912 Published online by Cambridge University Press

Note. If M' denotes the lower bound of the positive values of $q(u_1, u_2, u_3)$ taken over all integer triads $(u_1, u_2, u_3) \neq (0, 0, 0)$, then, by a theorem of Barnes [2], we have

$$M' \leqq \left(\frac{4}{3} \cdot \frac{25}{27}\right)^{1/3} = \left(\frac{100}{81}\right)^{1/3}.$$

It may be remarked that this is inadequate to ensure that $0 < a_{11} < 1$ and thereby exclude case (ii) of Theorem 2*.

REFERENCES

1. E. S. Barnes, The minimum of the product of two values of a quadratic form, I, II and III, *Proc. London Math. Soc.* (3) **1** (1951), 257–283, 385–414, 415–434.

2. E. S. Barnes, The non-negative values of quadratic forms, *Proc. London Math. Soc.* (3) **5** (1955), 185–196, Theorem 1.

3. J. H. H. Chalk, A theorem of Minkowski on the product of two linear forms, *Proc. Cambridge Phil. Soc.* **49** (1953), 413–420.

4. J. H. H. Chalk, On the product of *n* homogeneous linear forms, *Proc. London Math. Soc.* (3) **5** (1955), 449–473.

5. J. H. H. Chalk, Integral bases for quadratic forms, *Canad. J. Math.* **15** (1963), 412–421.

6. J. H. H. Chalk and C. A. Rogers, On the product of three homogeneous linear forms, *Proc. Cambridge Phil. Soc.* **47** (1951), 251–259.

7. H. Davenport, Non-homogeneous ternary quadratic forms, *Acta Math.* **80** (1948), 65–95; see also Barnes and Swinnerton-Dyer, Inhomogeneous minima of binary quadratic forms (I), *Acta Math.* **85** (1952), 259–323, especially §6.

8. L. E. Dickson, *Introduction to the theory of numbers* (Chicago, 1929).

9. L. E. Dickson, *Studies in the theory of numbers* (Chicago, 1930).

10. A. Korkine and G. Zolotareff, Sur les formes quadratiques, *Math. Ann.* **6** (1873), 366–389; see also [9], Theorem 83.

11. A. M. Macbeath, A new sequence of minima in the geometry of numbers, *Proc. Cambridge Phil. Soc.* **47** (1951), 266–273.

12. A. Markoff, Sur les formes quadratiques binaires indéfinies, *Math. Ann.* **15** (1879), 381–406; see also *Math. Ann.* **56** (1903), 233–251; see also [8], Theorem 119.

13. H. Minkowski, Ueber die Annäherung an eine reele Größe dursch rationale Zahlen, *Math. Ann.* **54** (1900), 91–124.

14. A. Oppenheim, Values of quadratic forms, I, *Quart. J. Math. Oxford Ser.* (2) **4** (1953), 54–59, Theorem 1.

15. A. Oppenheim, On indefinite binary quadratic forms, *Acta Math.* **91** (1954), 43–50.

St. Salvator's College
University of St. Andrews